

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zürich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7408>

Klaus Havelund · Gerard Holzmann
Rajeev Joshi (Eds.)

NASA Formal Methods

7th International Symposium, NFM 2015
Pasadena, CA, USA, April 27–29, 2015
Proceedings

Editors

Klaus Havelund
Jet Propulsion Laboratory
Pasadena, California
USA

Rajeev Joshi
Jet Propulsion Laboratory
Pasadena, California
USA

Gerard Holzmann
Jet Propulsion Laboratory
Pasadena, California
USA

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-319-17523-2

ISBN 978-3-319-17524-9 (eBook)

DOI 10.1007/978-3-319-17524-9

Library of Congress Control Number: 2015935615

LNCS Sublibrary: SL2 – Programming and Software Engineering

Springer Cham Heidelberg New York Dordrecht London

© Springer International Publishing Switzerland 2015

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.

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media
(www.springer.com)

Preface

This volume contains the papers presented at NFM 2015, the 7th NASA Formal Methods Symposium, held during April 27–29, 2015 in Pasadena. The NASA Formal Methods Symposium is a forum for anyone interested in the development and application of formal methods, both theoreticians and practitioners, from academia, industry, and government. The goal of the symposium is to identify challenges and provide solutions that can help us achieve greater reliability of mission- and safety-critical systems.

Within NASA, such systems include manned and unmanned spacecraft, orbiting satellites, and aircraft. Rapidly increasing code size and new software development paradigms, including the broad use of automatic code generation and code synthesis tools, static source code analysis techniques, and tool-based code review methods, all bring new challenges as well as new opportunities for improvement. Also gaining increasing importance in NASA applications is the use of more rigorous software test methods, often inspired by new theoretical insights.

The focus of the symposium is understandably on formal methods, their foundation, current capabilities, and limitations. The NASA Formal Methods Symposium is an annual event, which was created to highlight the state of the art in formal methods, both in theory and in practice. The series started as the Langley Formal Methods Workshop, and was held under that name in 1990, 1992, 1995, 1997, 2000, and 2008. In 2009 the first NASA Formal Methods Symposium was organized by NASA Ames Research Center, which also organized the 2013 symposium. In 2010 the symposium was organized in Washington DC by the Formal Methods Group of NASA Langley Research Center with the collaboration of NASA Goddard and NASA Headquarters; and in 2012 it was organized by NASA Langley Research Center in Norfolk, Virginia. In 2011 the organization was done by JPL's Laboratory for Reliable Software, in Pasadena, California. In 2014 it was organized by NASA's Johnson Space Center in collaboration with NASA Ames Research Center and Lero (Ireland), in Houston, Texas. Finally, the organization of the current 2015 symposium returned to JPL's Laboratory for Reliable Software in Pasadena, California.

The topics covered by the NASA Formal Methods Symposia include: theorem proving, logic model checking, automated testing and simulation, model-based engineering, real-time and stochastic systems, SAT and SMT solvers, symbolic execution, abstraction and abstraction refinement, compositional verification techniques, static and dynamic analysis techniques, fault protection, cyber security, specification formalisms, requirements analysis, and applications of formal techniques.

Two types of papers were considered: regular papers describing fully developed work and complete results or case studies, and short papers on tools, experience reports, or work in progress with preliminary results. The symposium received 108 submissions (77 regular papers and 31 short papers) out of which 33 were accepted (24 regular papers and 9 short papers), giving an acceptance rate of 30.6%. All submissions went through a rigorous reviewing process, where each paper was read by three reviewers.

In addition to the refereed papers, the symposium featured three invited presentations: by Dino Distefano from Facebook, USA, and Professor at Queen Mary University of London, UK, titled *Moving Fast with Software Verification*; by Viktor Kuncak, from the Laboratory for Automated Reasoning and Analysis at EPFL, in Lausanne, Switzerland, on *Developing Verified Software using Leon*; and by Rob Manning, from NASA's Jet Propulsion Laboratory, on *Complexity Tolerance: Dealing with Faults of Our Own Making*.

The organizers are grateful to the authors for submitting their work to NFM 2015 and to the invited speakers for sharing their insights. NFM 2015 would not have been possible without the collaboration of the outstanding Program Committee and external reviewers, the support of the Steering Committee, and the general support of the NASA Formal Methods community. The NFM 2015 website can be found at <http://nasaformalmethods.org>.

Support for the preparation of these proceedings was provided by the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

February 2015

Klaus Havelund
Gerard Holzmann
Rajeev Joshi

Organization

Program Committee

Erika Ábrahám	RWTH Aachen University, Germany
Julia Badger	NASA Johnson Space Center, USA
Christel Baier	Dresden University of Technology, Germany
Saddek Bensalem	VERIMAG/University Joseph Fourier, France
Dirk Beyer	University of Passau, Germany
Armin Biere	Johannes Kepler University, Austria
Nikolaj Bjørner	Microsoft Research, USA
Borzoo Bonakdarpour	McMaster University, Canada
Alessandro Cimatti	Fondazione Bruno Kessler, Italy
Leonardo De Moura	Microsoft Research, USA
Ewen Denney	NASA Ames Research Center, USA
Ben Di Vito	NASA Langley Research Center, USA
Dawson Engler	Stanford University, USA
Jean-Christophe Filliatre	Université Paris-Sud, France
Dimitra Giannakopoulou	NASA Ames Research Center, USA
Alwyn Goodloe	NASA Langley Research Center, USA
Susanne Graf	VERIMAG, France
Alex Groce	Oregon State University, USA
Radu Grosu	Vienna University of Technology, Austria
John Harrison	Intel Corporation, USA
Mike Hinchey	University of Limerick/Lero, Ireland
Bart Jacobs	Katholieke Universiteit Leuven, Belgium
Sarfraz Khurshid	University of Texas at Austin, USA
Gerwin Klein	NICTA and University of New South Wales, Australia
Daniel Kroening	University of Oxford, UK
Orna Kupferman	Hebrew University Jerusalem, Israel
Kim Larsen	Aalborg University, Denmark
Rustan Leino	Microsoft Research, USA
Martin Leucker	University of Lübeck, Germany
Rupak Majumdar	Max Planck Institute, Germany
Panagiotis Manolios	Northeastern University, USA
Peter Müller	ETH Zürich, Switzerland
Kedar Namjoshi	Bell Laboratories/Alcatel-Lucent, USA

Corina Pasareanu	NASA Ames Research Center, USA
Doron Peled	Bar-Ilan University, Israel
Suzette Person	NASA Langley Research Center, USA
Andreas Podelski	University of Freiburg, Germany
Grigore Rosu	University of Illinois at Urbana-Champaign, USA
Kristin Yvonne Rozier	NASA Ames Research Center, USA
Natarajan Shankar	SRI International, USA
Natasha Sharygina	University of Lugano, Switzerland
Scott Smolka	Stony Brook University, USA
Willem Visser	Stellenbosch University, South Africa
Mahesh Viswanathan	University of Illinois at Urbana-Champaign, USA
Michael Whalen	University of Minnesota, USA
Jim Woodcock	University of York, UK

Additional Reviewers

Alberti, Francesco	Hyvärinen, Antti
Alt, Leonardo	Isakovic, Haris
Arlt, Stephan	Jain, Mitesh
Astefanoaei, Lacramioara	Jovanović, Dejan
Bartocci, Ezio	Juhasz, Uri
Bourke, Timothy	Kahsai, Temesghen
Bozga, Marius	Kandl, Susanne
Bozzano, Marco	Katz, Guy
Cattaruzza, Dario	Kesseli, Pascal
Chamarthi, Harsh Raju	Kim, Chang Hwan Peter
Chang, Yen Jung	Li, Wenchao
Cholewa, Andrew	Li, Yilong
Christ, Juergen	Luckow, Kasper
Corzilius, Florian	Luo, Qingzhou
Dangl, Matthias	Löwe, Stefan
David, Cristina	Mahboubi, Assia
Decker, Normann	Markin, Grigory
Duan, Lian	Mehta, Farhad
Duggirala, Parasara Sridhar	Melnychenko, Oleksandr
Dutertre, Bruno	Melquiond, Guillaume
Farkash, Monica	Mentis, Anakreon
Fedyukovich, Grigory	Mery, Dominique
Ferrara, Pietro	Miyazawa, Alvaro
Fiadeiro, José Luiz	Moore, Brandon
Frömel, Bernhard	Moy, Yannick
Ghassabani, Elaheh	Munoz, Cesar
Greenaway, David	Murali, Rajiv
Griggio, Alberto	Narkawicz, Anthony
Harder, Jannis	Neogi, Natasha

Neville, Daniel
Nouri, Ayoub
Olivo, Oswaldo
Owre, Sam
Pais, Jorge
Papavasileiou, Vasilis
Prokesch, Daniel
Radoi, Cosmin
Ratasich, Denise
Rodriguez-Navas, Guillermo
Rozier, Eric
Scheffel, Torben
Schrammel, Peter
Schupp, Stefan
Schönfelder, René

Selyunin, Konstantin
Stefanescu, Andrei
Sticksel, Christoph
Stümpel, Annette
Taha, Walid
Thoma, Daniel
Tixeuil, Sebastien
Van Glabbeek, Rob
Vizel, Yakir
Wachter, Björn
Weissenbacher, Georg
Wendler, Philipp
Westphal, Bernd
Yang, Junxing
Zalinescu, Eugen

Contents

Invited Papers

Moving Fast with Software Verification	3
<i>Cristiano Calcagno, Dino Distefano, Jeremy Dubreil, Dominik Gabi, Pieter Hooimeijer, Martino Luca, Peter O’Hearn, Irene Papakonstantinou, Jim Purbrick, and Dulma Rodriguez</i>	
Developing Verified Software Using Leon.	12
<i>Viktor Kuncak</i>	

Regular Papers

Timely Rollback: Specification and Verification.	19
<i>Martín Abadi and Michael Isard</i>	
Sum of Abstract Domains	35
<i>Gianluca Amato, Simone Di Nardo Di Maio, and Francesca Scozzari</i>	
Reachability Preservation Based Parameter Synthesis for Timed Automata . . .	50
<i>Étienne André, Giuseppe Lipari, Hoang Gia Nguyen, and Youcheng Sun</i>	
Compositional Verification of Parameterised Timed Systems.	66
<i>Lăcrămioara Aștefănoaei, Souha Ben Rayana, Saddek Bensalem, Marius Bozga, and Jacques Combaz</i>	
Requirements Analysis of a Quad-Redundant Flight Control System.	82
<i>John Backes, Darren Cofer, Steven Miller, and Michael W. Whalen</i>	
Partial Order Reduction and Symmetry with Multiple Representatives	97
<i>Dragan Bošnački and Mark Scheffer</i>	
Statistical Model Checking of Ad Hoc Routing Protocols in Lossy Grid Networks.	112
<i>Alice Dal Corso, Damiano Macedonio, and Massimo Merro</i>	
Efficient Guiding Strategies for Testing of Temporal Properties of Hybrid Systems	127
<i>Tommaso Dreossi, Thao Dang, Alexandre Donzé, James Kapinski, Xiaoqing Jin, and Jyotirmoy V. Deshmukh</i>	

First-Order Transitive Closure Axiomatization via Iterative Invariant Injections	143
<i>Aboubakr Achraf El Ghazi, Mana Taghdiri, and Mihai Herda</i>	
Reachability Analysis Using Extremal Rates	158
<i>Andrew N. Fisher, Chris J. Myers, and Peng Li</i>	
Towards Realizability Checking of Contracts Using Theories	173
<i>Andrew Gacek, Andreas Katis, Michael W. Whalen, John Backes, and Darren Cofer</i>	
Practical Partial Order Reduction for CSP	188
<i>Thomas Gibson-Robinson, Henri Hansen, A.W. Roscoe, and Xu Wang</i>	
A Little Language for Testing	204
<i>Alex Groce and Jervis Pinto</i>	
Detecting MPI Zero Buffer Incompatibility by SMT Encoding	219
<i>Yu Huang and Eric Mercer</i>	
A Falsification View of Success Typing	234
<i>Robert Jakob and Peter Thiemann</i>	
Verified ROS-Based Deployment of Platform-Independent Control Systems	248
<i>Wenrui Meng, Junkil Park, Oleg Sokolsky, Stephanie Weirich, and Insup Lee</i>	
A Rigorous Approach to Combining Use Case Modelling and Accident Scenarios	263
<i>Rajiv Murali, Andrew Ireland, and Gudmund Grov</i>	
Are We There Yet? Determining the Adequacy of Formalized Requirements and Test Suites	279
<i>Anitha Murugesan, Michael W. Whalen, Neha Rungta, Oksana Tkachuk, Suzette Person, Mats P.E. Heimdahl, and Dongjiang You</i>	
A Greedy Approach for the Efficient Repair of Stochastic Models	295
<i>Shashank Pathak, Erika Ábrahám, Nils Jansen, Armando Tacchella, and Joost-Pieter Katoen</i>	
Integrating SMT with Theorem Proving for Analog/Mixed-Signal Circuit Verification	310
<i>Yan Peng and Mark Greenstreet</i>	
Conflict-Directed Graph Coverage	327
<i>Daniel Schwartz-Narbonne, Martin Schäfer, Dejan Jovanović, Philipp Rümmer, and Thomas Wies</i>	

Shape Analysis with Connectors	343
<i>Holger Siegel and Axel Simon</i>	
Automated Conflict-Free Concurrent Implementation of Timed Component-Based Models	359
<i>Ahlem Triki, Borzoo Bonakdarpour, Jacques Combaz, and Saddek Bensalem</i>	
Formal API Specification of the PikeOS Separation Kernel	375
<i>Freek Verbeek, Oto Havle, Julien Schmaltz, Sergey Tverdyshev, Holger Blasum, Bruno Langenstein, Werner Stephan, Burkhart Wolff, and Yakoub Nemouchi</i>	
Short Papers	
Data Model Bugs	393
<i>Ivan Bocić and Tevfik Bultan</i>	
Predicting and Witnessing Data Races Using CSP	400
<i>Luis M. Carril and Walter F. Tichy</i>	
A Benchmark Suite for Hybrid Systems Reachability Analysis	408
<i>Xin Chen, Stefan Schupp, Ibtissem Ben Makhlof, Erika Ábrahám, Goran Frehse, and Stefan Kowalewski</i>	
Generalizing a Mathematical Analysis Library in Isabelle/HOL	415
<i>Jesús Aransay and Jose Divasón</i>	
A Tool for Intersecting Context-Free Grammars and Its Applications	422
<i>Graeme Gange, Jorge A. Navas, Peter Schachte, Harald Søndergaard, and Peter J. Stuckey</i>	
UFIT: A Tool for Modeling Faults in UPPAAL Timed Automata	429
<i>Reza Hajisheykhi, Ali Ebneenasir, and Sandeep S. Kulkarni</i>	
Blocked Literals Are Universal.	436
<i>Marijn J.H. Heule, Martina Seidl, and Armin Biere</i>	
Practical Formal Verification of Domain-Specific Language Applications . . .	443
<i>Greg Eakman, Howard Reubenstein, Tom Hawkins, Mitesh Jain, and Panagiotis Manolios</i>	
Reporting Races in Dynamic Partial Order Reduction	450
<i>Olli Saarikivi and Keijo Heljanko</i>	
Author Index	457