Lecture Notes in Computer Science **9058**

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Springer

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

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