Lecture Notes in Computer Science **10811**

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

Formal Methods

Subline of Lectures Notes in Computer Science

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

Aaron Dutle · César Muñoz
Anthony Narkawicz (Eds.)

NASA Formal Methods

10th International Symposium, NFM 2018
Newport News, VA, USA, April 17–19, 2018
Proceedings

Springer

Editors
Aaron Dutle
NASA Langley Research Center
Hampton, VA
USA

Anthony Narkawicz
NASA Langley Research Center
Hampton, VA
USA

César Muñoz
NASA Langley Research Center
Hampton, VA
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-77934-8 ISBN 978-3-319-77935-5 (eBook)
https://doi.org/10.1007/978-3-319-77935-5

Library of Congress Control Number: 2018937364

LNCS Sublibrary: SL2 – Programming and Software Engineering

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

Preface

The NASA Formal Methods (NFM) Symposium is a forum to foster collaboration between theoreticians and practitioners from NASA, academia, and industry, with the goal of identifying challenges and providing solutions to achieving assurance in mission- and safety-critical systems. Examples of such systems include advanced separation assurance algorithms for aircraft, next-generation air transportation, autonomous rendezvous and docking for spacecraft, autonomous on-board software for unmanned aerial systems (UAS), UAS traffic management, autonomous robots, and systems for fault detection, diagnosis, and prognostics. The topics covered by the NASA Formal Methods Symposia include:

- Formal verification, including theorem proving, model checking, and static analysis
- Advances in automated theorem proving including SAT and SMT solving
- Use of formal methods in software and system testing
- Run-time verification
- Techniques and algorithms for scaling formal methods such as abstraction and symbolic methods, compositional techniques, as well as parallel and/or distributed techniques
- Code generation from formally verified models
- Safety cases and system safety
- Formal approaches to fault tolerance
- Theoretical advances and empirical evaluations of formal methods techniques for safety-critical systems, including hybrid and embedded systems
- Formal methods in systems engineering and model-based development
- Formalization of mathematics and physics

This volume contains the papers presented at NFM 2018, the 10th NASA Formal Methods Symposium, held during April 17–19, 2018 in Newport News, VA. NFM 2018 celebrated 30 years of formal methods research at NASA. Previous symposia were held in Moffett Field, CA (2017), Minneapolis, MN (2016), Pasadena, CA (2015), Houston, TX (2014), Moffett Field, CA (2013), Norfolk, VA (2012), Pasadena, CA (2011), Washington, DC (2010), and Moffett Field, CA (2009). The series started as the Langley Formal Methods Workshop, and was held under that name in 1990, 1992, 1995, 1997, 2000, and 2008.

Papers were solicited for NFM 2018 under two categories: regular papers describing fully developed work and complete results, and short papers describing tools, experience reports, or work in progress with preliminary results. The symposium received 92 submissions for review out of which 31 were accepted for publication. These submissions went through a rigorous reviewing process, where each paper was first independently reviewed by at least three reviewers and then subsequently discussed by the Program Committee. In addition to the refereed papers, the symposium featured

two invited presentations, one by Rick Butler of NASA Langley Research Center, USA, and one by Gilles Dowek of Inria, CNRS, and ENS Cachan, France.

The organizers are grateful to the authors for submitting their work to NFM 2018 and to the invited speakers for sharing their insights. NFM 2018 would not have been possible without the collaboration of the outstanding Program Committee and additional reviewers, the support of the Steering Committee, the efforts of the staff at the NASA Langley Research Center, and the general support of the NASA Formal Methods community. The NFM 2018 website can be found at: https://shemesh.larc.nasa.gov/NFM2018.

April 2018

Aaron Dutle
César Muñoz
Anthony Narkawicz

Organization

Program Committee

Erika Ábrahám	RWTH Aachen University, Germany
Mauricio Ayala-Rincon	Universidade de Brasilia, Brazil
Julia Badger	NASA, USA
Dirk Beyer	LMU Munich, Germany
Nikolaj Bjørner	Microsoft, USA
Jasmin Blanchette	Vrije Universiteit Amsterdam, The Netherlands
Sylvie Boldo	Inria, France
Kalou Cabrera Castillos	LAAS-CNRS, France
Misty Davies	NASA, USA
Catherine Dubois	ENSIIE-Samovar, France
Aaron Dutle	NASA, USA
Stefania Gnesi	ISTI-CNR, Italy
Alberto Griggio	Fondazione Bruno Kessler, Italy
George Hagen	NASA, USA
John Harrison	Intel, USA
Klaus Havelund	NASA Jet Propulsion Laboratory, USA
Ashlie Hocking	Dependable Computing, USA
Susmit Jha	SRI International, USA
Rajeev Joshi	NASA Jet Propulsion Laboratory, USA
Laura Kovacs	Vienna University of Technology, Austria
Michael Lowry	NASA, USA
Panagiotis Manolios	Northeastern University, USA
Shaun McWherter	NASA, USA
César Muñoz	NASA, USA
Anthony Narkawicz	NASA, USA
Natasha Neogi	NASA, USA
Lee Pike	Groq, USA
Murali Rangarajan	The Boeing Company, USA
Elvinia Riccobene	University of Milan, Italy
Camilo Rocha	Pontificia Universidad Javeriana Cali, Colombia
Kristin Yvonne Rozier	Iowa State University, USA
Sriram Sankaranarayanan	University of Colorado Boulder, USA
Johann Schumann	SGT, USA
Konrad Slind	Rockwell Collins, USA
Cesare Tinelli	The University of Iowa, USA
Laura Titolo	National Institute of Aerospace, USA

Christoph Torens	German Aerospace Center, Germany
Michael Whalen	University of Minnesota, USA
Virginie Wiels	ONERA, France

Additional Reviewers

Alves, Vander
Arcaini, Paolo
Basile, Davide
Bozzano, Marco
Braghin, Chiara
Brotherston, James
Byun, Taejoon
Chakarov, Aleksandar
Champion, Adrien
Chen, Xin
Chowdhury, Omar
Cohen, Cyril
Cox, Arlen
Cruanes, Simon
Dangl, Matthias
Dodds, Mike
Dureja, Rohit
Fainekos, Georgios
Fantechi, Alessandro
Feliú Gabaldon, Marco
Ferrari, Alessio
Fleury, Mathias
Fokkink, Wan
Friedberger, Karlheinz
Gallois-Wong, Diane
Ghassabani, Elaheh
Goodloe, Alwyn
Hoxha, Bardh
Hussein, Soha
Jakobs, Marie-Christine
Jones, Benjamin
Katis, Andreas
Katz, Guy
Kremer, Gereon
Lammich, Peter
Larraz, Daniel
Lemberger, Thomas
Li, Jianwen
Lüdtke, Daniel
Marché, Claude
Marechal, Alexandre
Mazzanti, Franco
Meel, Kuldeep S.
Merz, Stephan
Moscato, Mariano
Nantes-Sobrinho, Daniele
Nigam, Vivek
Panizo, Laura
Paskevich, Andrei
Pérez, Jorge A.
Ravitch, Tristian
Rioboo, Renaud
Roveri, Marco
Schirmer, Sebastian
Schopferer, Simon
Schupp, Stefan
Stewart, Danielle
Strub, Pierre-Yves
Tian, Chun
Traytel, Dmitriy
Weaver, Sean
Wendler, Philipp
Weps, Benjamin

Contents