Lecture Notes in Computer Science

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

Editorial Board

David Hutchison, UK Josef Kittler, UK Friedemann Mattern, Switzerland Moni Naor, Israel Bernhard Steffen, Germany Doug Tygar, USA Takeo Kanade, USA Jon M. Kleinberg, USA John C. Mitchell, USA C. Pandu Rangan, India Demetri Terzopoulos, USA Gerhard Weikum, Germany

Formal Methods

Subline of Lectures Notes in Computer Science

Subline Series Editors

Ana Cavalcanti, University of York, UK Marie-Claude Gaudel, Université de Paris-Sud, France

Subline Advisory Board

Manfred Broy, *TU Munich, Germany* Annabelle McIver, *Macquarie University, Sydney, NSW, Australia* Peter Müller, *ETH Zurich, Switzerland* Erik de Vink, *Eindhoven University of Technology, The Netherlands* Pamela Zave, *AT&T Laboratories Research, Bedminster, NJ, USA* 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



Editors Aaron Dutle NASA Langley Research Center Hampton, VA USA

César Muñoz NASA Langley Research Center Hampton, VA USA Anthony Narkawicz 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
 ISBN 978-3-319-77935-5
 (eBook)

Library of Congress Control Number: 2018937364

LNCS Sublibrary: SL2 - Programming and Software Engineering

© 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 publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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	University of Colorado Boulder, USA
Sankaranarayanan	
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 Michael Whalen Virginie Wiels German Aerospace Center, Germany University of Minnesota, USA 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

Incremental Construction of Realizable Choreographies Sarah Benyagoub, Meriem Ouederni, Yamine Aït-Ameur, and Atif Mashkoor	1
Formal Assurance for Cooperative Intelligent Autonomous Agents Siddhartha Bhattacharyya, Thomas C. Eskridge, Natasha A. Neogi, Marco Carvalho, and Milton Stafford	20
Ghosts for Lists: A Critical Module of Contiki Verified in Frama-C Allan Blanchard, Nikolai Kosmatov, and Frédéric Loulergue	37
An Executable Formal Framework for Safety-Critical Human Multitasking Giovanna Broccia, Paolo Milazzo, and Peter Csaba Ölveczky	54
Simpler Specifications and Easier Proofs of Distributed Algorithms Using History Variables Saksham Chand and Yanhong A. Liu	70
Don't Miss the End: Preventing Unsafe End-of-File Comparisons	87
An Efficient Rewriting Framework for Trace Coverage of Symmetric Systems	95
Verification of Fault-Tolerant Protocols with Sally Bruno Dutertre, Dejan Jovanović, and Jorge A. Navas	113
Output Range Analysis for Deep Feedforward Neural Networks	121
Formal Dynamic Fault Trees Analysis Using an Integration of Theorem Proving and Model Checking Yassmeen Elderhalli, Osman Hasan, Waqar Ahmad, and Sofiène Tahar	139
Twenty Percent and a Few Days – Optimising a Bitcoin Majority Attack Ansgar Fehnker and Kaylash Chaudhary	157
An Even Better Approach – Improving the B.A.T.M.A.N. Protocol Through Formal Modelling and Analysis	164

X Contents

Towards a Formal Safety Framework for Trajectories	179
Static Value Analysis of Python Programs by Abstract Interpretation Aymeric Fromherz, Abdelraouf Ouadjaout, and Antoine Miné	185
Model-Based Testing for General Stochastic Time	203
Strategy Synthesis for Autonomous Agents Using PRISM Ruben Giaquinta, Ruth Hoffmann, Murray Ireland, Alice Miller, and Gethin Norman	220
The Use of Automated Theory Formation in Support of Hazard Analysis Andrew Ireland, Maria Teresa Llano, and Simon Colton	237
Distributed Model Checking Using ProB Philipp Körner and Jens Bendisposto	244
Optimal Storage of Combinatorial State Spaces	261
Stubborn Transaction Reduction	280
Certified Foata Normalization for Generalized Traces	299
On the Timed Analysis of Big-Data Applications Francesco Marconi, Giovanni Quattrocchi, Luciano Baresi, Marcello M. Bersani, and Matteo Rossi	315
Tuning Permissiveness of Active Safety Monitorsfor Autonomous SystemsLola Masson, Jérémie Guiochet, Hélène Waeselynck,Kalou Cabrera, Sofia Cassel, and Martin Törngren	333
Sound Black-Box Checking in the LearnLib	349
Model-Checking Task Parallel Programs for Data-Race	367
Consistency of Property Specification Patterns with Boolean and Constrained Numerical Signals	383

Automatic Generation of DO-178 Test Procedures César Ochoa Escudero, Rémi Delmas, Thomas Bochot, Matthieu David, and Virginie Wiels	399
Using Test Ranges to Improve Symbolic Execution Rui Qiu, Sarfraz Khurshid, Corina S. Păsăreanu, Junye Wen, and Guowei Yang	416
Symbolic Execution and Reachability Analysis Using Rewriting Modulo SMT for Spatial Concurrent Constraint Systems with Extrusion	435
Experience Report: Application of Falsification Methods on the UxAS System <i>Cumhur Erkan Tuncali, Bardh Hoxha, Guohui Ding,</i> <i>Georgios Fainekos, and Sriram Sankaranarayanan</i>	452
MoDeS3: Model-Based Demonstrator for Smart and Safe Cyber-Physical Systems András Vörös, Márton Búr, István Ráth, Ákos Horváth, Zoltán Micskei, László Balogh, Bálint Hegyi, Benedek Horváth, Zsolt Mázló, and Dániel Varró	460
Author Index	469