Lecture Notes in Computer Science 10227

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

Clark Barrett · Misty Davies
Temesghen Kahsai (Eds.)

NASA Formal Methods

9th International Symposium, NFM 2017
Moffett Field, CA, USA, May 16–18, 2017
Proceedings

Springer

Editors
Clark Barrett
Stanford University
Palo Alto, CA
USA

Misty Davies
NASA Ames Research Center
Moffett Field, CA
USA

Temesghen Kahsai
NASA Ames Research Center
Moffett Field, CA
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-57287-1 ISBN 978-3-319-57288-8 (eBook)
DOI 10.1007/978-3-319-57288-8

Library of Congress Control Number: 2017937299

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer International Publishing AG 2017
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 Springer Nature
The registered company is Springer International Publishing AG
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: model checking, theorem proving, SAT and SMT solving, symbolic execution, automated testing and verification, static and dynamic analysis, model-based development, runtime verification, software and system testing, safety assurance, fault tolerance, compositional verification, security and intrusion detection, design for verification and correct-by-design techniques, techniques for scaling formal methods, formal methods for multi-core GPU-based implementations, generation, specification, and validation of requirements, human–machine interaction analysis, certification, and applications of formal methods in systems development.

This volume contains the papers presented at NFM 2017, the 9th NASA Formal Methods Symposium, held at the NASA Ames Research Center, Moffett Field, CA, during May 16–18, 2017. Previous symposia were held in 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 2017 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 77 submissions for review (60 regular papers and 17 short papers) out of which 31 were accepted for publication (23 regular papers and eight short papers). 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 five invited presentations: "Formal Methods for the Informal World," by Michael Wagner, Senior Commercialization Specialist at the Robotics Institute at Carnegie Mellon University, Pittsburgh, PA; "Agile Aerospace at Planet," by Ben Haldeman, Technologist and Program Manager at Planet, San Francisco, CA; "Moving Fast with High Reliability: Static Analysis at Uber," by Manu Sridharan, Senior Software Engineer at Uber, Palo Alto, CA; "Challenges in Designing for the Next Era of Human Space Exploration," by Jason Crusan, Director of the Advanced Exploration Systems Division within the Human Exploration and Operations Mission Directorate at NASA, Washington, DC; and "A Tour of Formal Methods in Support of Aerospace Products Development," by

Alexandre Arnold, Research Engineer at Airbus. The symposium also featured a panel that discussed how to make more real problems and case studies from NASA and the aerospace industry available to researchers.

The organizers are grateful to the authors for submitting their work to NFM 2017 and to the invited speakers for sharing their insights. NFM 2017 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 Ames Research Center, and the general support of the NASA Formal Methods community. The NFM 2017 website can be found at: https://ti.arc.nasa.gov/events/nfm-2017.

May 2017

Clark Barrett
Misty Davies
Temesghen Kahsai

Organization

Program Committee

Ella Atkins	University of Michigan, USA
Domagoj Babic	Google, USA
Julia Badger	NASA Johnson Space Center, USA
Clark Barrett	Stanford University, USA
Kirstie Bellman	The Aerospace Corporation, USA
Dirk Beyer	LMU Munich, Germany
Nikolaj Bjorner	Microsoft Research, USA
Kalou Cabrera Castillos	LAAS-CNRS, France
Alessandro Cimatti	FBK-IRST, Italy
Misty Davies	NASA Ames Research Center, USA
Ewen Denney	Stinger Ghaffarian Technologies and NASA Ames Research Center, USA
Dino Distefano	Facebook, UK
Eric Feron	Georgia Institute of Technology, USA
Pierre-Loic Garoche	ONERA, France
Patrice Godefroid	Microsoft Research, USA
Alwyn Goodloe	NASA Langley Research Center, USA
Alberto Griggio	FBK-IRST, Italy
Aarti Gupta	Princeton University, USA
Arie Gurfinkel	University of Waterloo, Canada
John Harrison	Intel Corporation, USA
Klaus Havelund	Jet Propulsion Laboratory, California Institute of Technology, USA
Kelly Hayhurst	NASA Langley Research Center, USA
Mats Heimdahl	University of Minnesota, USA
Mike Hinchey	Lero-the Irish Software Engineering Research Centre, Ireland
Susmit Jha	SRI International, USA
Rajeev Joshi	Laboratory for Reliable Software, Jet Propulsion Laboratory, USA
Dejan Jovanović	SRI International, USA
Temesghen Kahsai	NASA Ames Research Center/CMU, USA
Gerwin Klein	Data61, CSIRO, Australia
Daniel Kroening	University of Oxford, UK
Wenchao Li	Boston University, USA
Lowry Michael	NASA Ames Research Center, USA
Jorge A Navas	SRI International, USA
Natasha Neogi	NASA Langley Research Center, USA
Meeko Oishi	University of New Mexico, USA

Lee Pike	Galois, Inc., USA
Zvonimir Rakamaric	University of Utah, USA
Murali Rangarajan	The Boeing Company, USA
Kristin Yvonne Rozier	Iowa State University, USA
Lael Rudd	Draper, USA
Philipp Ruemmer	Uppsala University, Sweden
Neha Rungta	Amazon Web Services, USA
John Rushby	SRI International, USA
Sriram Sankaranarayanan	University of Colorado, Boulder, USA
Martin Schäf	SRI International, USA
Cesare Tinelli	The University of Iowa, USA
Christoph Torens	German Aerospace Center, Institute of Flight Systems, Germany
Virginie Wiels	ONERA/DTIM, France

Additional Reviewers

Backeman, Peter
Backes, John
Bittner, Benjamin
Blackshear, Sam
Calderón Trilla, José Manuel
Cattaruzza, Dario
Chowdhury, Omar
Cohen, Raphael
Dangl, Matthias
Dimjasevic, Marko
Elliott, Trevor
Erkok, Levent
Galea, John
Gay, David
Gross, Kerianne
Hamon, Arnaud
He, Shaobo
Hendrix, Joe
Howar, Falk
Luckow, Kasper
Mattarei, Cristian
Mercer, Eric
Mote, Mark
Mukherjee, Rajdeep
Poetzl, Daniel
Reynolds, Andrew
Sanchez, Huascar
Sun, Youcheng
Tkachuk, Oksana
Zeljić, Aleksandar

Contents

An Automata-Theoretic Approach to Modeling Systems and Specifications over Infinite Data 1
Hadar Frenkel, Orna Grumberg, and Sarai Sheinvald

Learning from Faults: Mutation Testing in Active Automata Learning 19
Bernhard K. Aichernig and Martin Tappler

Parametric Model Checking Timed Automata Under Non-Zenoness Assumption 35
Étienne André, Hoang Gia Nguyen, Laure Petrucci, and Jun Sun

Multi-timed Bisimulation for Distributed Timed Automata 52
James Ortiz, Moussa Amrani, and Pierre-Yves Schobbens

Auto-Active Proof of Red-Black Trees in SPARK. 68
Claire Dross and Yannick Moy

Analysing Security Protocols Using Refinement in iUML-B 84
Colin Snook, Thai Son Hoang, and Michael Butler

On Learning Sparse Boolean Formulae for Explaining AI Decisions 99
Susmit Jha, Vasumathi Raman, Alessandro Pinto, Tuhin Sahai, and Michael Francis

Event-Based Runtime Verification of Temporal Properties Using Time Basic Petri Nets 115
Matteo Camilli, Angelo Gargantini, Patrizia Scandurra, and Carlo Bellettini

Model-Counting Approaches for Nonlinear Numerical Constraints 131
Mateus Borges, Quoc-Sang Phan, Antonio Filieri, and Corina S. Păsăreanu

Input Space Partitioning to Enable Massively Parallel Proof 139
Ashlie B. Hocking, M. Anthony Aiello, John C. Knight, and Nikos Aréchiga

Compositional Model Checking of Interlocking Systems for Lines with Multiple Stations 146
Hugo Daniel Macedo, Alessandro Fantechi, and Anne E. Haxthausen

Modular Model-Checking of a Byzantine Fault-Tolerant Protocol 163
Benjamin F. Jones and Lee Pike

Improved Learning for Stochastic Timed Models
by State-Merging Algorithms 178
Braham Lotfi Mediouni, Ayoub Nouri, Marius Bozga, and Saddek Bensalem

Verifying Safety and Persistence Properties of Hybrid Systems
Using Flowpipes and Continuous Invariants 194
Andrew Sogokon, Paul B. Jackson, and Taylor T. Johnson

A Relational Shape Abstract Domain. 212
Hugo Illous, Matthieu Lemerre, and Xavier Rival

Floating-Point Format Inference in Mixed-Precision 230
Matthieu Martel

A Verification Technique for Deterministic Parallel Programs. 247
Saeed Darabi, Stefan C.C. Blom, and Marieke Huisman

Systematic Predicate Abstraction Using Variable Roles 265
Yulia Demyanova, Philipp Rümmer, and Florian Zuleger

`specgen`: A Tool for Modeling Statecharts in CSP 282
Brandon Shapiro and Chris Casinghino

HyPro: A `C++` Library of State Set Representations for Hybrid
Systems Reachability Analysis 288
Stefan Schupp, Erika Ábrahám, Ibtissem Ben Makhlouf, and Stefan Kowalewski

`Asm2C++`: A Tool for Code Generation from Abstract State Machines
to Arduino 295
Silvia Bonfanti, Marco Carissoni, Angelo Gargantini, and Atif Mashkoor

SPEN: A Solver for Separation Logic 302
Constantin Enea, Ondřej Lengál, Mihaela Sighireanu, and Tomáš Vojnar

From Hazard Analysis to Hazard Mitigation Planning:
The Automated Driving Case 310
Mario Gleirscher and Stefan Kugele

Event-B at Work: Some Lessons Learnt from an Application to a Robot
Anti-collision Function 327
Arnaud Dieumegard, Ning Ge, and Eric Jenn

Reasoning About Safety-Critical Information Flow Between Pilot and Computer 342
Seth Ahrenbach

Compositional Falsification of Cyber-Physical Systems with Machine Learning Components 357
Tommaso Dreossi, Alexandre Donzé, and Sanjit A. Seshia

Verifying a Class of Certifying Distributed Programs. 373
Kim Völlinger and Samira Akili

Compact Proof Witnesses. 389
Marie-Christine Jakobs and Heike Wehrheim

Qualification of a Model Checker for Avionics Software Verification 404
Lucas Wagner, Alain Mebsout, Cesare Tinelli, Darren Cofer, and Konrad Slind

SpeAR v2.0: Formalized Past LTL Specification and Analysis of Requirements 420
Aaron W. Fifarek, Lucas G. Wagner, Jonathan A. Hoffman, Benjamin D. Rodes, M. Anthony Aiello, and Jennifer A. Davis

Just Formal Enough? Automated Analysis of EARS Requirements 427
Levi Lúcio, Salman Rahman, Chih-Hong Cheng, and Alistair Mavin

Author Index 435