Lecture Notes in Computer Science 7226

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

Alwyn E. Goodloe Suzette Person (Eds.)

NASA Formal Methods

4th International Symposium, NFM 2012
Norfolk, VA, USA, April 3-5, 2012
Proceedings

Springer

Volume Editors

Alwyn E. Goodloe
Suzette Person
NASA Langley Research Center
MS 130, Hampton VA 23681, USA
E-mail:{a.goodloe, suzette.person}@nasa.gov

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-28890-6 e-ISBN 978-3-642-28891-3
DOI 10.1007/978-3-642-28891-3
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012933117

CR Subject Classification (1998): D.2.4, D.2, D.3, F.3, D.1

LNCS Sublibrary: SL 2 – Programming and Software Engineering

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This publication contains the proceedings of the 4th NASA Formal Methods Symposium (NFM 2012), held April 3–5, 2012, in Norfolk, VA, USA. The NASA Formal Method Symposium is a forum for theoreticians and practitioners from academia, industry, and government, with the goal of identifying challenges and providing solutions to achieving assurance in mission- and safety-critical systems. Within NASA, for example, such systems include autonomous robots, separation assurance algorithms for aircraft, Next Generation Air Transportation (NextGen), and autonomous rendezvous and docking for spacecraft. Rapidly increasing code size and emerging paradigms, such as automated code generation and safety cases, bring new challenges and opportunities for significant improvement. Also gaining increasing importance in NASA applications is the use of more rigorous software test methods and code analysis techniques, founded in theory.

The focus of the symposium is understandably on formal methods, their foundation, current capabilities, as well as their current limitations. The NASA Formal Methods Symposium is an annual event that was created to highlight the state of the art in formal methods, both in theory and practice. The series was originally 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, and took place at Moffett Field, CA. This year, the symposium was organized by NASA Langley Research Center, and held in Norfolk, VA.

The topics covered by NFM 2012 included but were not limited to: theorem proving, symbolic execution, model-based engineering, real-time and stochastic systems, model checking, 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 describing tools, experience reports, and work in progress or preliminary results. The symposium received 93 submissions (66 regular papers and 27 short papers), of which the committee selected 36 papers (26 regular papers and 10 short papers). All submissions went through a rigorous review process.

In addition to the refereed papers, the symposium featured three invited talks and a panel session. The invited talks were presented by Andrew Appel from Princeton University, on "Verified Software Toolchain," Patrick Cousot from École Normale Supérieure, Paris, and New York University, on "Formal Verification by Abstract Interpretation," and Cesare Tinelli from the University of Iowa, on "SMT-Based Model Checking." The panel, composed of Mike

Lowry (NASA Ames), Klaus Havelund (NASA/JPL), and Ricky Butler (NASA Langley), discussed the history and current application of formal methods at NASA.

The organizers are grateful to the authors for submitting their work to NFM 2012 and to the invited speakers for sharing their insights. NFM 2012 would not have been possible without the collaboration of the Steering Committee, Program Committee, and external reviewers, and the general support of the NASA Formal Methods community. Special thanks go to Raymond Meyer for the graphical design of NFM 2012 visual material and the NFM 2012 website, which can be found at http://shemesh.larc.nasa.gov/nfm2012/index.html.

January 2012

Alwyn Goodloe
Suzette Person

Organization

Program Committee

Nikolaj Bjorner	Microsoft Research, USA
Jonathan P. Bowen	Museophile Limited, UK
Julia Braman	NASA- Johnson Space Center, USA
Ricky Butler	NASA Langley Research Center, USA
Rance Cleaveland	University of Maryland, USA
Darren Cofer	Rockwell Collins, USA
Ewen Denney	SGT/NASA Ames, USA
Dino Distefano	Queen Mary, University of London, UK
Jin Song Dong	National University of Singapore, Singapore
Jean-Christophe Filliatre	CNRS, France
Dimitra Giannakopoulou	NASA Ames, USA
Alwyn Goodloe	NASA Langley Research Center, USA
Eric Goubault	CEA/Saclay, France
George Hagen	NASA Langley Research Center, USA
John Hatcliff	Kansas State University, USA
Klaus Havelund	Jet Propulsion Laboratory, California Institute of Technology, USA
Mats Heimdahl	University of Minnesota, USA
Gerard Holzmann	JPL, USA
Joe Hurd	Galois, Inc., USA
Bart Jacobs	Katholieke Universiteit Leuven, Belgium
Ken Mcmillan	Cadence Berkeley Labs, USA
Eric Mercer	Brigham Young University, USA
Cesar Munoz	National Aeronautics and Space Administration, USA
Anthony Narkawicz	NASA Langley, USA
Natasha Neogi	National Institute of Aerospace, USA
Corina Pasareanu	CMU/NASA Ames Research Center, USA
Charles Pecheur	UC Louvain, Belgium
Suzette Person	NASA Langley Research Center, USA
Kristin Yvonne Rozier	NASA Ames Research Center, USA
Natarajan Shankar	SRI International, USA
Oleg Sokolsky	University of Pennsylvania, USA
Sofiene Tahar	Concordia University, USA
Oksana Tkachuk	Fujitsu Laboratories of America
Willem Visser	Stellenbosch University, South Africa
Michael Whalen	University of Minnesota, USA
Virginie Wiels	ONERA / DTIM, France
Jim Woodcock	University of York, UK

Additional Reviewers

Ancona, Davide
Aridhi, Henda
Ayoub, Anaheed
Belt, Jason
Beringer, Lennart
Bouissou, Olivier
Brotherston, James
Busard, Simon
Combefis, Sebastien
Cruanes, Simon
Cuoq, Pascal
Denman, William
Di Vito, Ben
Dubreil, Jeremy
Florian, Mihai
Gawanmeh, Amjad
Gui, Lin
Haucourt, Emmanuel
Holloway, C. Michael
Jourdan, Jacques-Henri
Khan-Afshar, Sanaz
King, Andrew
Le Gall, Tristan
Lemay, Michael
Leslie, Rebekah
Liu, Liya
Mahboubi, Assia
Mhamdi, Tarek
Miller, Sheena
Miner, Paul
Mullier, Olivier
Namjoshi, Kedar
Owre, Sam
Pai, Ganesh
Paskevich, Andrei
Rocha, Camilo
Rozier, Eric
Rungta, Neha
Sanán, David
Schrammel, Peter
Shi, Ling
Siminiceanu, Radu
Smans, Jan
Song, Songzheng
Spitters, Bas
Tan, Tian Huat
Vanoverberghe, Dries
Wang, Shaohui
Zhang, Shaojie
Zheng, Manchun

Table of Contents

SMT-Based Model Checking 1
Cesare Tinelli

Verified Software Toolchain (Abstract) 2
Andrew W. Appel

Formal Verification by Abstract Interpretation 3
Patrick Cousot

Quantitative Timed Analysis of Interactive Markov Chains 8
Dennis Guck, Tingting Han, Joost-Pieter Katoen, and Martin R. Neuhäußer

Lessons Learnt from the Adoption of Formal Model-Based Development 24
Alessio Ferrari, Alessandro Fantechi, and Stefania Gnesi

Symbolic Execution of Communicating and Hierarchically Composed UML-RT State Machines 39
Karolina Zurowska and Juergen Dingel

Inferring Definite Counterexamples through Under-Approximation 54
Jörg Brauer and Axel Simon

Modifying Test Suite Composition to Enable Effective Predicate-Level Statistical Debugging 70
Ross Gore and Paul F. Reynolds Jr.

Rigorous Polynomial Approximation Using Taylor Models in COQ 85
Nicolas Brisebarre, Mioara Joldeş, Érik Martin-Dorel, Micaela Mayero, Jean-Michel Muller, Ioana Paşca, Laurence Rideau, and Laurent Théry

Enhancing the Inverse Method with State Merging 100
Étienne André, Laurent Fribourg, and Romain Soulat

Class-Modular, Class-Escape and Points-to Analysis for Object-Oriented Languages 106
Alexander Herz and Kalmer Apinis

Testing Static Analyzers with Randomly Generated Programs 120
Pascal Cuoq, Benjamin Monate, Anne Pacalet, Virgile Prevosto, John Regehr, Boris Yakobowski, and Xuejun Yang

Compositional Verification of Architectural Models 126
Darren Cofer, Andrew Gacek, Steven Miller, Michael W. Whalen, Brian LaValley, and Lui Sha

A Safety Case Pattern for Model-Based Development Approach 141
Anaheed Ayoub, Baek-Gyu Kim, Insup Lee, and Oleg Sokolsky

PVS Linear Algebra Libraries for Verification of Control Software Algorithms in C/ACSL 147
Heber Herencia-Zapana, Romain Jobredeaux, Sam Owre, Pierre-Loïc Garoche, Eric Feron, Gilberto Perez, and Pablo Ascariz

Temporal Action Language (TAL): A Controlled Language for Consistency Checking of Natural Language Temporal Requirements (Preliminary Results) 162
Wenbin Li, Jane Huffman Hayes, and Mirosław Truszczyński

Some Steps into Verification of Exact Real Arithmetic 168
Norbert Th. Müller and Christian Uhrhan

Runtime Verification Meets Android Security 174
Andreas Bauer, Jan-Christoph Küster, and Gil Vegliach

Specification in PDL with Recursion 181
Xinxin Liu and Bingtian Xue

Automatically Proving Thousands of Verification Conditions Using an SMT Solver: An Empirical Study 195
Aditi Tagore, Diego Zaccai, and Bruce W. Weide

Sound Formal Verification of Linux's USB BP Keyboard Driver 210
Willem Penninckx, Jan Tobias Mühlberg, Jan Smans, Bart Jacobs, and Frank Piessens

Learning Markov Models for Stationary System Behaviors 216
Yingke Chen, Hua Mao, Manfred Jaeger, Thomas Dyhre Nielsen, Kim Guldstrand Larsen, and Brian Nielsen

The Use of Rippling to Automate Event-B Invariant Preservation Proofs 231
Yuhui Lin, Alan Bundy, and Gudmund Grov

Thread-Modular Model Checking with Iterative Refinement 237
Wenrui Meng, Fei He, Bow-Yaw Wang, and Qiang Liu

Towards LTL Model Checking of Unmodified Thread-Based C & C++ Programs 252
Jiři Barnat, Luboš Brim, and Petr Ročkai

Integrating Statechart Components in Polyglot 267
Daniel Balasubramanian, Corina S. Păsăreanu, Jason Biatek, Thomas Pressburger, Gabor Karsai, Michael Lowry, and Michael W. Whalen

Using PVS to Investigate Incidents through the Lens of Distributed Cognition 273
Paolo Masci, Huayi Huang, Paul Curzon, and Michael D. Harrison

Automated Analysis of Parametric Timing-Based Mutual Exclusion Algorithms 279
Roberto Bruttomesso, Alessandro Carioni, Silvio Ghilardi, and Silvio Ranise

Efficient Symbolic Execution of Value-Based Data Structures for Critical Systems 295
Jason Belt, Robby, Patrice Chalin, John Hatcliff, and Xianghua Deng

Generating Verifiable Java Code from Verified PVS Specifications 310
Leonard Lensink, Sjaak Smetsers, and Marko van Eekelen

Belief Bisimulation for Hidden Markov Models: Logical Characterisation and Decision Algorithm 326
David N. Jansen, Flemming Nielson, and Lijun Zhang

Abstract Model Repair 341
George Chatzieleftheriou, Borzoo Bonakdarpour, Scott A. Smolka, and Panagiotis Katsaros

CLSE: Closed-Loop Symbolic Execution 356
Rupak Majumdar, Indranil Saha, K.C. Shashidhar, and Zilong Wang

On the Development and Formalization of an Extensible Code Generator for Real Life Security Protocols 371
Michael Backes, Alex Busenius, and Cătălin Hriţcu

Incremental Verification with Mode Variable Invariants in State Machines 388
Temesghen Kahsai, Pierre-Loïc Garoche, Cesare Tinelli, and Mike Whalen

A Semantic Analysis of Wireless Network Security Protocols 403
Damiano Macedonio and Massimo Merro

Runtime Verification with Predictive Semantics 418
Xian Zhang, Martin Leucker, and Wei Dong

A Case Study in Verification of Embedded Network Software 433
Kalyan C. Regula, Hampton Smith, Heather Harton Keown, Jason O. Hallstrom, Nigamanth Sridhar, and Murali Sitaraman

Checking and Distributing Statistical Model Checking 449
Peter Bulychev, Alexandre David, Kim Guldstrand Larsen, Axel Legay, Marius Mikučionis, and Danny Bøgsted Poulsen

Author Index 465