Lecture Notes in Computer Science 6617

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

Mihaela Bobaru Klaus Havelund
Gerard J. Holzmann Rajeev Joshi (Eds.)

NASA Formal Methods

Third International Symposium, NFM 2011
Pasadena, CA, USA, April 18-20, 2011
Proceedings

Springer

Volume Editors

Mihaela Bobaru
Klaus Havelund
Gerard J. Holzmann
Rajeev Joshi
NASA Jet Propulsion Laboratory
4800 Oak Grove Drive, M/S 301-285, Pasadena, CA 91109, USA
E-mail: {mihaela.bobaru, klaus.havelund, gh, rajeev.joshi}@jpl.nasa.gov

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-20397-8 e-ISBN 978-3-642-20398-5
DOI 10.1007/978-3-642-20398-5
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011924552

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 Third NASA Formal Methods Symposium (NFM 2011), which was held April 18–20, 2011, in Pasadena, CA, USA. The NASA Formal Methods 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 safety-critical systems.

Within NASA, such systems include manned and unmanned spacecraft, orbiting satellites, and aircraft. Rapidly increasing code size, as well as the adoption of new software development paradigms, e.g., code generation and code synthesis, static source code analysis techniques and tool-based code review methods, bring new challenges and opportunities for significant improvement. Also gaining increasing importance in NASA applications is the use of more rigorous software test methods, 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 in 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. In 2010 the symposium was organized by NASA Langley Research Center and NASA Goddard Space Flight Center, and held at NASA Headquarters, in Washington DC. This year's symposium was organized by the Laboratory for Reliable Software at the Jet Propulsion Laboratory / California Institute of Technology, and held in Pasadena CA.

The topics covered by NFM 2011 included but were not limited to: 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 tool papers describing an operational tool, with examples of its application. The symposium received 141 submissions (112 regular papers and 29 tool papers) out of which 38 were accepted (26 regular papers and 12 tool papers), giving an acceptance rate of 27%. All submissions went through a rigorous reviewing process, where each paper was read by at least three reviewers.

In addition to the refereed papers, the symposium featured three invited talks and three invited tutorials. The invited talks were presented by Rustan Leino from Microsoft Research, on "From Retrospective Verification to Forward-Looking Development," Oege de Moor from the University of Oxford in England, and CEO of Semmle/Inc., on "Do Coding Standards Improve Software Quality?," and Andreas Zeller from Saarland University in Germany, on "Specifications for Free." The invited tutorials were presented by Andreas Bauer from the Australian National University in Australia, and Martin Leucker from Institut für Softwaretechnik und Programmiersprache, Universität zu Lübeck in Germany, on "The Theory and Practice of SALT—Structured Assertion Language for Temporal Logic," Bart Jacobs from the Katholieke Universiteit Leuven in Belgium on "VeriFast: A Powerful, Sound, Predictable, Fast Verifier for C and Java," and Michał Moskal from Microsoft Research, on "Verifying Functional Correctness of C Programs with VCC."

The organizers are grateful to the authors for submitting their work to NFM 2011 and to the invited speakers for sharing their insights. NFM 2011 would not have been possible without the collaboration of the outstanding Steering Committee, Program Committee, and external reviewers, and the general support of the NASA Formal Methods community. The NFM 2011 website can be found at http://lars-lab.jpl.nasa.gov/nfm2011.

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 2011

Mihaela Bobaru
Klaus Havelund
Gerard Holzmann
Rajeev Joshi

Organization

Program Chairs

Mihaela Bobaru	NASA Jet Propulsion Laboratory, USA
Klaus Havelund	NASA Jet Propulsion Laboratory, USA
Gerard Holzmann	NASA Jet Propulsion Laboratory, USA
Rajeev Joshi	NASA Jet Propulsion Laboratory, USA

Program Committee

Rajeev Alur	University of Pennsylvania, USA
Tom Ball	Microsoft Research, USA
Howard Barringer	University of Manchester, UK
Saddek Bensalem	Verimag Laboratory, France
Nikolaj Bjørner	Microsoft Research, USA
Eric Bodden	Technical University Darmstadt, Germany
Marsha Chechik	University of Toronto, Canada
Rance Cleaveland	University of Maryland, USA
Dennis Dams	Bell Labs/Alcatel-Lucent, Belgium
Ewen Denney	NASA Ames Research Center, USA
Ben Di Vito	NASA Langley, USA
Matt Dwyer	University of Nebraska at Lincoln, USA
Cormac Flanagan	University of California at Santa Cruz, USA
Dimitra Giannakopoulou	NASA Ames Research Center, USA
Patrice Godefroid	Microsoft Research, USA
Alex Groce	Oregon State University, USA
Radu Grosu	Stony Brook University, USA
John Hatcliff	Kansas State University, USA
Mats Heimdahl	University of Minnesota, USA
Mike Hinchey	Lero, the Irish SE Research Centre, Ireland
Sarfraz Khurshid	University of Texas at Austin, USA
Orna Kupferman	Jerusalem Hebrew University, Israel
Kim Larsen	Aalborg University, Denmark
Rupak Majumdar	Max Planck Institute, Germany
Kenneth McMillan	Microsoft Research, USA
César Muñoz	NASA Langley, USA
Madan Musuvathi	Microsoft Research, USA
Kedar Namjoshi	Bell Labs/Alcatel-Lucent, USA
Corina Păsăreanu	NASA Ames Research Center, USA
Shaz Qadeer	Microsoft Research, USA
Grigore Roşu	University of Illinois at Urbana-Champaign, USA

Nicolas Rouquette	NASA Jet Propulsion Laboratory, USA
Kristin Rozier	NASA Ames Research Center, USA
John Rushby	SRI International, USA
Wolfram Schulte	Microsoft Research, USA
Koushik Sen	University of California at Berkeley, USA
Sanjit Seshia	University of California at Berkeley, USA
Natarajan Shankar	SRI International, USA
Willem Visser	University of Stellenbosch, South Africa
Mahesh Viswanathan	University of Illinois at Urbana-Champaign, USA
Mike Whalen	University of Minnesota, USA

Steering Committee

Ewen Denney	NASA Ames Research Center, USA
Ben Di Vito	NASA Langley, USA
Dimitra Giannakopoulou	NASA Ames Research Center, USA
Klaus Havelund	NASA Jet Propulsion Laboratory, USA
Gerard Holzmann	NASA Jet Propulsion Laboratory, USA
César Muñoz	NASA Langley, USA
Corina Păsăreanu	NASA Ames Research Center, USA
James Rash	NASA Goddard Space Flight Center, USA
Kristin Rozier	NASA Ames Research Center, USA

External Reviewers

Ki Yung Ahn
Mihail Asavoae
Richard Banach
Ezio Bartocci
Ananda Basu
Bert van Beek
Shoham Ben-David
Simon Bliudze
Dragan Bosnacki
Marius Bozga
Bryan Brady
Sebastian Burckhardt
Jacob Burnim
Katherine Coons
Pierpaolo Degano
Xianghua Deng
Parasara Sridhar Duggirala
Bruno Dutertre
Tayfun Elmas
Vaidas Gasiunas
Jaco Geldenhuys
Shalini Ghosh
Alwyn Goodloe
Divya Gopinath
Andreas Griesmayer
Arie Gurfinkel
George Hagen
Ian J. Hayes
Daniel Holcomb
Cornelia Inggs
Ethan Jackson
Alan Jeffrey
Susmit Jha
Dongyun Jin
Barbara Jobstmann
Taylor Johnson
Anjali Joshi
Panagiotis Katsaros
Shadi Khalek
Robert Koenighofer

Ruurd Kuiper
Benoit Lahaye
Axel Legay
Wenchao Li
Karthik Manamcheri
Daniel Marino
Patrick Meredith
Michał Moskal
MohammadReza Mousavi
Anthony Narkawicz
Than Hung Nguyen
Sam Owre
Ganesh Pai
Chang-Seo Park
Fiona Polack
Pavithra Prabhakar
Vishwanath Raman
Giles Reger
Elaine Render
Robby
Neha Rungta
David Rydeheard
Mehrdad Sabetzadeh
Rick Salay
Ralf Sasse
Lucas Satabin
Traian Serbanuta
Peter Sestoft
Andreas Sewe
Shalini Shamasunder
K.C. Shashidhar
Elena Sherman
Junaid Siddiqui
Natalia Sidorova
Élodie-Jane Sims
Andrei Stefanescu
Christos Stergiou
Nikolai Tillmann
Ashish Tiwari
Arnaud Venet
Ou Wei
Tim Willemse
Guowei Yang
Razieh Zaeem
Hans Zantema
Chaoqiang Zhang

Table of Contents

I. Invited Talks

II. Invited Tutorials

III. Regular Papers

IV. Tool Papers