

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Alfred Kobsa

*University of California, Irvine, CA, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Germany*

Madhu Sudan

*Microsoft Research, Cambridge, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbruecken, Germany*

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

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

© Springer-Verlag Berlin Heidelberg 2011

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, 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.

*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](http://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 Michal 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 Hinckey	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

## VIII Organization

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

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

# Table of Contents

## I. Invited Talks

From Retrospective Verification to Forward-Looking Development .....	1
<i>K. Rustan M. Leino</i>	
Specifications for Free .....	2
<i>Andreas Zeller</i>	

## II. Invited Tutorials

The Theory and Practice of SALT .....	13
<i>Andreas Bauer and Martin Leucker</i>	
VeriFast: A Powerful, Sound, Predictable, Fast Verifier for C and Java .....	41
<i>Bart Jacobs, Jan Smans, Pieter Philippaerts, Frédéric Vogels, Willem Penninckx, and Frank Piessens</i>	
Verifying Functional Correctness of C Programs with VCC .....	56
<i>Michał Moskal</i>	

## III. Regular Papers

Bakar Kiasan: Flexible Contract Checking for Critical Systems Using Symbolic Execution .....	58
<i>Jason Belt, John Hatcliff, Robby, Patrice Chalin, David Hardin, and Xianghua Deng</i>	
Approximate Quantifier Elimination for Propositional Boolean Formulae .....	73
<i>Jörg Brauer and Andy King</i>	
Towards Flight Control Verification Using Automated Theorem Proving .....	89
<i>William Denman, Mohamed H. Zaki, Sofiène Tahar, and Luis Rodrigues</i>	
Generalized Rabin(1) Synthesis with Applications to Robust System Synthesis .....	101
<i>Rüdiger Ehlers</i>	
Integrating an Automated Theorem Prover into Agda .....	116
<i>Simon Foster and Georg Struth</i>	

Efficient Predicate Abstraction of Program Summaries . . . . .	131
<i>Arie Gurfinkel, Sagar Chaki, and Samir Sapra</i>	
Synthesis for PCTL in Parametric Markov Decision Processes . . . . .	146
<i>Ernst Moritz Hahn, Tingting Han, and Lijun Zhang</i>	
Formalizing Probabilistic Safety Claims . . . . .	162
<i>Heber Herencia-Zapana, George Hagen, and Anthony Narkawicz</i>	
The OpenTheory Standard Theory Library . . . . .	177
<i>Joe Hurd</i>	
Instantiation-Based Invariant Discovery . . . . .	192
<i>Temesghen Kahsai, Yeting Ge, and Cesare Tinelli</i>	
Stuttering Mostly Speeds Up Solving Parity Games . . . . .	207
<i>Sjoerd Cranen, Jeroen J.A. Keiren, and Tim A.C. Willemse</i>	
Counterexample-Based Error Localization of Behavior Models . . . . .	222
<i>Tsutomu Kumazawa and Tetsuo Tamai</i>	
Call Invariants . . . . .	237
<i>Shuvendu K. Lahiri and Shaz Qadeer</i>	
Symmetry for the Analysis of Dynamic Systems . . . . .	252
<i>Zarrin Langari and Richard Trefler</i>	
Implementing Cryptographic Primitives in the Symbolic Model . . . . .	267
<i>Peeter Laud</i>	
Model Checking Using SMT and Theory of Lists . . . . .	282
<i>Aleksandar Milicevic and Hillel Kugler</i>	
Automated Test Case Generation with SMT-Solving and Abstract Interpretation . . . . .	298
<i>Jan Peleska, Elena Vorobev, and Florian Lapschies</i>	
Generating Data Race Witnesses by an SMT-Based Analysis . . . . .	313
<i>Mahmoud Said, Chao Wang, Zijiang Yang, and Karem Sakallah</i>	
Applying Atomicity and Model Decomposition to a Space Craft System in Event-B . . . . .	328
<i>Asieh Salehi Fathabadi, Abdolbaghi Rezazadeh, and Michael Butler</i>	
A Theory of Skiplists with Applications to the Verification of Concurrent Datatypes . . . . .	343
<i>Alejandro Sánchez and César Sánchez</i>	
CORAL: Solving Complex Constraints for Symbolic PathFinder . . . . .	359
<i>Matheus Souza, Mateus Borges, Marcelo d'Amorim, and Corina S. Păsăreanu</i>	

Automated Formal Verification of the <i>TTEthernet</i> Synchronization Quality . . . . .	375
<i>Wilfried Steiner and Bruno Dutertre</i>	
Extending the GWV Security Policy and Its Modular Application to a Separation Kernel . . . . .	391
<i>Sergey Tverdyshev</i>	
Combining Partial-Order Reduction and Symbolic Model Checking to Verify LTL Properties . . . . .	406
<i>José Vander Meulen and Charles Pecheur</i>	
Towards Informed Swarm Verification . . . . .	422
<i>Anton Wijs</i>	
Scaling Up with Event-B: A Case Study . . . . .	438
<i>Faqing Yang and Jean-Pierre Jacquot</i>	

## IV. Tool Papers

D-Finder 2: Towards Efficient Correctness of Incremental Design . . . . .	453
<i>Saddek Bensalem, Andreas Griesmayer, Axel Legay, Thanh-Hung Nguyen, Joseph Sifakis, and Rongjie Yan</i>	
Infer: An Automatic Program Verifier for Memory Safety of C Programs . . . . .	459
<i>Cristiano Calcagno and Dino Distefano</i>	
Model Construction and Priority Synthesis for Simple Interaction Systems . . . . .	466
<i>Chih-Hong Cheng, Saddek Bensalem, Barbara Jobstmann, Rongjie Yan, Alois Knoll, and Harald Ruess</i>	
OpenJML: JML for Java 7 by Extending OpenJDK . . . . .	472
<i>David R. Cok</i>	
jSMTLIB: Tutorial, Validation and Adapter Tools for SMT-LIBv2 . . . . .	480
<i>David R. Cok</i>	
opaal: A Lattice Model Checker . . . . .	487
<i>Andreas Engelbrecht Dalsgaard, René Rydhof Hansen, Kenneth Yrke Jørgensen, Kim Gulstrand Larsen, Mads Chr. Olesen, Petur Olsen, and Jiří Srba</i>	
A Tabular Expression Toolbox for Matlab/Simulink . . . . .	494
<i>Colin Eles and Mark Lawford</i>	
LLVM2CSP: Extracting CSP Models from Concurrent Programs . . . . .	500
<i>Moritz Kleine, Björn Bartels, Thomas Göthel, Steffen Helke, and Dirk Prenzel</i>	

XIV Table of Contents

Multi-Core LTSmin: Marrying Modularity and Scalability .....	506
<i>Alfons Laarman, Jaco van de Pol, and Michael Weber</i>	
GiNaCRA: A C++ Library for Real Algebraic Computations .....	512
<i>Ulrich Loup and Erika Ábrahám</i>	
Kopitiam: Modular Incremental Interactive Full Functional Static Verification of Java Code .....	518
<i>Hannes Mehnert</i>	
Milestones: A Model Checker Combining Symbolic Model Checking and Partial Order Reduction .....	525
<i>José Vander Meulen and Charles Pecheur</i>	
<b>Author Index</b> .....	533