

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

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

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Jayadev Misra Tobias Nipkow
Emil Sekerinski (Eds.)

FM 2006: Formal Methods

14th International Symposium on Formal Methods
Hamilton, Canada, August 21-27, 2006
Proceedings

Volume Editors

Jayadev Misra
University of Texas at Austin
Department of Computer Sciences, Taylor Hall
1 University Station, C0500, Austin, Texas 78712-1188, USA
E-mail: misra@cs.utexas.edu

Tobias Nipkow
Technische Universität München
Institut für Informatik
Boltzmannstr. 3, 85748 Garching, Germany
E-mail: nipkow@in.tum.de

Emil Sekerinski
McMaster University
Department of Computing and Software
1280 Main Street West, Hamilton, Ontario, L8S 4K1 Canada
E-mail: emil@mcmaster.ca

Library of Congress Control Number: 2006930417

CR Subject Classification (1998): D.2, F.3, D.3, D.1, J.1, K.6, F.4

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN	0302-9743
ISBN-10	3-540-37215-6 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-37215-8 Springer Berlin Heidelberg New York

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.

Springer is a part of Springer Science+Business Media
springer.com

© Springer-Verlag Berlin Heidelberg 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11813040 06/3142 5 4 3 2 1 0

Preface

This volume contains the proceedings of Formal Methods 2006, the 14th International Symposium on Formal Methods, held at McMaster University, Hamilton, Canada, during August 21-27, 2006. Formal Methods Europe (FME, www.fmeurope.org) is an independent association which aims to stimulate the use of, and research on, formal methods for system development. The first symposium in this series was VDM Europe in 1987. The scope of the symposium has grown since then, encompassing all aspects of software and hardware which are amenable to formal analysis. As in the previous years, this symposium brings together researchers, tool developers, vendors and users.

We received 145 submissions from 31 countries, making it a truly international event. Each submission was carefully refereed by at least three reviewers. The Program Committee selected 36 papers for presentation at the symposium, after an intensive, in-depth discussion. We would like to thank all the Program Committee members and the referees for their excellent and efficient work.

Apart from the regular contributions, there were five invited talks for the general symposium (Ernie Cohen, Nicholas Griffin, Thomas A. Henzinger, Peter Lindsay and George Necula); the contribution of Henzinger (with Sifakis as a co-author) and an abstract from Cohen are included in this volume.

Nicholas Griffin gave a general and informal talk about Russell's work in logic and the foundations of mathematics in the early years of the twentieth century. It focussed on the philosophical views that underlay Russell's attempts to solve the Russell paradox (and several others) which culminated in the ramified theory of types.

The FM 2006 symposium was planned to include four workshops and ten tutorials. Additionally, there was a Doctoral Symposium which included presentations by doctoral students, and a Poster and Tool Exhibition.

An Industry Day was organized by the Formal Techniques Industrial Association (ForTIA) alongside the main symposium. This was directly related to the main theme of the symposium: the use of well-founded formal methods in the industrial practice of software design, development and maintenance. The theme of the Industry Day in this symposium was "Formal Methods for Security and Trust in Industrial Applications." There were eight invited talks for Industry Day (Randolph Johnson, Jan Jürjens, Scott A. Lintelman, Dusko Pavlovic, Werner Stephan, Michael Waidner, Jim Woodcock and David von Oheimb); abbreviated versions of some of the talks are included in this volume.

The electronic submission, refereeing and Program Committee discussions would not have been possible without support of the EasyChair system, developed by Andrei Voronkov at the University of Manchester, UK. In addition to developing a system of great flexibility, Andrei was available for help and advice throughout; our heart-felt thanks to him. Our thanks to Springer, and,

particularly, Ursula Barth, Anna Kramer and Frank Holzwarth, for help with preparation of this volume.

August 2006

Jayadev Misra
Tobias Nipkow
Emil Sekerinski

Symposium Organization

We are grateful to the Computing and Software Center at McMaster University, Hamilton, Canada and Formal Methods Europe for organizing FM 2006. Our special thanks to the faculty, students and staff of McMaster University who volunteered their time in the Organizing Committee.

Symposium Chairs

General Chair	Emil Sekerinski, McMaster University, Canada
Program Chairs	Jayadev Misra, University of Texas, Austin, USA
	Tobias Nipkow, Universität München, Germany
Industry Day Chairs	Volkmar Lotz, SAP Research Labs, France
	Asuman Suenbuel, SAP Research Labs, USA
Tools and Poster Chair	Marsha Chechik, University of Toronto, Canada
Workshops Chair	Tom Maibaum, McMaster University, Canada
Tutorials Chair	Jin Song Dong, National University, Singapore
Doctoral Symposium Chair	Ana Cavalcanti, University of York, UK
	Augusto Sampaio, UFPE, Brazil
	Jim Woodcock, University of York, UK
Sponsorship Chair	Jürgen Dingel, Queen's University, Canada

Organizing Committee at McMaster University

Publicity	Wolfram Kahl, Alan Wasssyng, Jeff Zucker
Book Exhibition	Spencer Smith
Tools and Posters	Spencer Smith
Social Events	Ridha Khedri
Facilities Co-ordination	William Farmer, Mark Lawford
Events Co-ordination	Ryszard Janicki
Finances	Ryszard Janicki
Website Services	Doris Burns, Jan Maibaum

Program Committee

Jean-Raymond Abrial, ETH, Zurich, Switzerland
Alex Aiken, Stanford University, Stanford, USA
Keijiro Araki, Kyushu University, Fukuoka, Japan
Ralph-Johan Back, Abo Akademi, Turku, Finland

Gilles Barthe, INRIA at Sophia-Antipolis, France
 David Basin, ETH, Zurich, Switzerland
 Frank de Boer, CWI, Amsterdam, The Netherlands
 Ed Brinksma, Embedded Systems Institute, Eindhoven, The Netherlands
 Michael Butler, University of Southampton, Southampton, UK
 Rance Cleaveland, University of Maryland, College Park, USA
 Jorge Cuellar, Siemens Research, Munich, Germany
 Werner Damm, OFFIS, Oldenburg, Germany
 Javier Esparza, University of Stuttgart, Stuttgart, Germany
 José Fiadeiro, University of Leicester, UK
 Susanne Graf, Verimag, Grenoble, France
 Ian Hayes, University of Queensland, Queensland, Australia
 Gerard Holzmann, NASA/JPL Labs, Pasadena, USA
 Cliff Jones, University of Newcastle upon Tyne, UK
 Axel van Lamsweerde, Université Catholique de Louvain, Belgium
 Gary T. Leavens, Iowa State University, Ames, USA
 Rustan Leino, Microsoft Research, Redmond, USA
 Xavier Leroy, INRIA, Rocquencourt, France
 Dominique Méry, LORIA and Université Henri Poincaré, Nancy, France
 Carroll Morgan, University of New South Wales, NSW, Australia
 David Naumann, Stevens Institute of Technology, Hoboken, USA
 Ernst-Rüdiger Olderog, University of Oldenburg, Oldenburg, Germany
 Paritosh Pandya, TIFR, Mumbai, India
 Sriram Rajamani, Microsoft Research, Bangalore, India
 John Rushby, SRI International, Menlo Park, USA
 Steve Schneider, University of Surrey, Guildford, UK
 Vitaly Shmatikov, University of Texas, Austin, USA
 Bernhard Steffen, University of Dortmund, Dortmund, Germany
 P.S. Thiagarajan, National University of Singapore, Singapore
 Martin Wirsing, Universität München, Germany
 Pierre Wolper, Université de Liège, Liège, Belgium

External Reviewers

J. Abendroth	Andrew Appel	Krzysztof Apt
Yuji Arichika	Eugene Asarin	Anindya Banerjee
Mike Barnett	Don Batory	Maurice ter Beek
Yves Bertot	Sylvie Boldo	Marcello Bonsangue
Laura Brandan Briones	Achim Brucker	Dominique Cansell
David Carrington	Paul Caspi	Antonio Cau
Patrice Chalin	Tom Chothia	Dave Clarke
Joey Coleman	Robert Colvin	Olivier Constant
Phil Cook	William Cook	Karl Crary
Maximiliano Cristia	Adrian Curic	Roberto Delicata

Henning Dierks	Juegen Doser	Paul Hanks Drielsma
Guillaume Dufay	Andy Edmunds	Martin Ellis
E. Allen Emerson	Neil Evans	Dirk Fahland
Bernd Fischer	John Fitzgerald	Martin Fränzle
Marcelo Frias	Paul Gibson	Simon Goldsmith
Madhu Gopinathan	Bhargav Gulavani	Christian Haack
Stefan Hallerstede	Klaus Havelund	James Heather
Tobias Heindel	Rolf Hennicker	Martin Henson
Wim Hesselink	Matthias Hözl	Marieke Huisman
Hardi Hungar	Daniel Jackson	Suresh Jagannathan
Johan Jeuring	Warren A. Hunt Jr.	Sven Jörges
Aditya Kanade	Stephanie Kemper	Stefan Kiefer
Joseph Kiniry	Alexander Knapp	Barbara König
Piotr Kordy	Piotr Kosiuczenko	Pavel Krcal
Tomas Krilavicius	Ingolf Krueger	Wouter Kuijper
Ruurd Kuiper	Marcel Kyas	Ralf Laemmel
Linas Laibinis	Rom Langerak	Kim Larsen
David Lesens	Kamal Lodaya	Antònia Lopes
Michael Luttenberger	Monika Maidl	Joao Marques-Silva
Erik Arne Mathiesen	Tim McComb	Alistair McEwan
Farhad Mehta	Roland Meyer	Ronald Middelkoop
Ali Mili	Antoine Mine	Bill Mitchell
Anders Moller	Michael Möller	Peter Müller
Prasad Naldurg	Rocco De Nicola	Aditya Nori
Dirk Nowotka	Peter O'Hearn	David von Oheimb
Anne Pacalet	Joachim Parrow	Dirk Pattinson
Mariela Pavlova	Thomas Peikenkamp	Simon Peyton-Jones
David Pichardie	Ken Pierce	Jaco van de Pol
Mike Poppleton	Sanjiva Prasad	Viorel Preoteasa
Alexander Pretschner	Cyril Proch	Harald Raffelt
Hridayesh Rajan	H. Rajasekaran	Axel Rauschmayer
Abdolbaghi Rezazadeh	M. Birna van Riemsdijk	Robby
Abhik Roychoudhury	Oliver Ruething	Theo Ruys
David Rydeheard	Mannu Satpathy	Andreas Schäfer
Norbert Schirmer	Gerardo Schneider	Stefan Schwoon
Paul Sevinc	Murali Sitaraman	Graeme Smith
Colin Snook	Martin Steffen	Mark-Oliver Stehr
Marielle Stoelinga	Ketil Stølen	Harald Störrle
Douglas Stuart	Martyn Thomas	Christian Topnik
Helen Treharne	Stavros Tripakis	Emilio Tuosto
Laurent Voisin	Marina de Vos	Thomas Wahl
Thai Son Wang	Andrzej Wasowski	Heike Wehrheim
Bernd Westphal	Luke Wildman	Martin Wildmoser
Jim Woodcock	Fei Xie	Alex Yakovlev
Letu Yang	Pamela Zave	Gefei Zhang

Sponsors

We are thankful for the organizational support from FME and Formal Techniques Industrial Association (ForTIA). We gratefully acknowledge sponsorships from the following organizations: Microsoft Research, Tourism Hamilton, SAP Labs France, Software Quality Research Laboratory of McMaster University, and Faculty of Engineering of McMaster University.

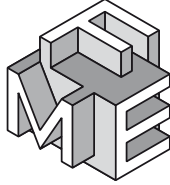


Table of Contents

Invited Talk

The Embedded Systems Design Challenge	1
<i>Thomas A. Henzinger, Joseph Sifakis</i>	

Interactive Verification

The Mondex Challenge: Machine Checked Proofs for an Electronic Purse	16
<i>Gerhard Schellhorn, Holger Grandy, Dominik Haneberg, Wolfgang Reif</i>	
Interactive Verification of Medical Guidelines	32
<i>Jonathan Schmitt, Alwin Hoffmann, Michael Balser, Wolfgang Reif, Mar Marcos</i>	
Certifying Airport Security Regulations Using the Focal Environment	48
<i>David Delahaye, Jean-Frédéric Étienne, Véronique Viguié Donzeau-Gouge</i>	
Proving Safety Properties of an Aircraft Landing Protocol Using I/O Automata and the PVS Theorem Prover: A Case Study	64
<i>Shinya Umeno, Nancy Lynch</i>	

Invited Talk

Validating the Microsoft Hypervisor	81
<i>Ernie Cohen</i>	

Formal Modelling of Systems

Interface Input/Output Automata	82
<i>Kim G. Larsen, Ulrik Nyman, Andrzej Wąsowski</i>	
Properties of Behavioural Model Merging	98
<i>Greg Brunet, Marsha Chechik, Sebastian Uchitel</i>	
Automatic Translation from <i>Circus</i> to Java	115
<i>Angela Freitas, Ana Lucia Caneca Cavalcanti</i>	
Quantitative Refinement <i>and</i> Model Checking for the Analysis of Probabilistic Systems	131
<i>Annabelle K. McIver</i>	

Real Time

Modeling and Validating Distributed Embedded Real-Time Systems with VDM++	147
<i>Marcel Verhoef, Peter Gorm Larsen, Jozef Hooman</i>	
Towards Modularized Verification of Distributed Time-Triggered Systems	163
<i>Jewgenij Botaschanjan, Alexander Gruler, Alexander Harhurin, Leonid Kof, Maria Spichkova, David Trachtenherz</i>	

Industrial Experience

A Story About Formal Methods Adoption by a Railway Signaling Manufacturer	179
<i>Stefano Bacherini, Alessandro Fantechi, Matteo Tempestini, Niccolò Zingoni</i>	
Partially Introducing Formal Methods into Object-Oriented Development: Case Studies Using a Metrics-Driven Approach	190
<i>Yujun Zheng, Jinquan Wang, Kan Wang, Jinyun Xue</i>	

Specification and Refinement

Compositional Class Refinement in Object-Z	205
<i>Tim McComb, Graeme Smith</i>	
A Proposal for Records in Event-B	221
<i>Neil Evans, Michael Butler</i>	
Pointfree Factorization of Operation Refinement	236
<i>José Nuno Oliveira, César Jesus Rodrigues</i>	
A Formal Template Language Enabling Metaproof	252
<i>Nuno Amálio, Susan Stepney, Fiona Polack</i>	

Programming Languages

Dynamic Frames: Support for Framing, Dependencies and Sharing Without Restrictions (Best Paper)	268
<i>Ioannis T. Kassios</i>	
Type-Safe Two-Level Data Transformation	284
<i>Alcino Cunha, José Nuno Oliveira, Joost Visser</i>	

Algebra

Feature Algebra	300
<i>Peter Höfner, Ridha Khedri, Bernhard Möller</i>	

Education

Using Domain-Independent Problems for Introducing Formal Methods	316
<i>Raymond Boute</i>	

Formal Modelling of Systems

Compositional Binding in Network Domains	332
<i>Pamela Zave</i>	
Formal Modeling of Communication Protocols by Graph Transformation	348
<i>Zarrin Langari, Richard Trefler</i>	
Feature Specification and Static Analysis for Interaction Resolution	364
<i>Marc Aiguier, Karim Berkani, Pascale Le Gall</i>	
A Fully General Operational Semantics for UML 2.0 Sequence Diagrams with Potential and Mandatory Choice	380
<i>Mass Soldal Lund, Ketil Stølen</i>	

Formal Aspects of Java

Towards Automatic Exception Safety Verification	396
<i>Xin Li, H. James Hoover, Piotr Rudnicki</i>	
Enforcer – Efficient Failure Injection	412
<i>Cyrille Valentin Artho, Armin Biere, Shinichi Honiden</i>	
Automated Boundary Test Generation from JML Specifications	428
<i>Fabrice Bouquet, Frédéric Dadeau, Bruno Legeard</i>	
Formal Reasoning About Non-atomic JAVA CARD Methods in Dynamic Logic	444
<i>Wojciech Mostowski</i>	

Programming Languages

Formal Verification of a C Compiler Front-End	460
<i>Sandrine Blazy, Zaynah Dargaye, Xavier Leroy</i>	

A Memory Model Sensitive Checker for C#	476
<i>Thuan Quang Huynh, Abhik Roychoudhury</i>	
Changing Programs Correctly: Refactoring with Specifications	492
<i>Fabian Bannwart, Peter Müller</i>	
Mechanical Verification of Recursive Procedures Manipulating Pointers Using Separation Logic	508
<i>Viorel Preoteasa</i>	

Model Checking

Model-Based Variable and Transition Orderings for Efficient Symbolic Model Checking	524
<i>Wendy Johnston, Kirsten Winter, Lionel van den Berg, Paul Strooper, Peter Robinson</i>	
Exact and Approximate Strategies for Symmetry Reduction in Model Checking	541
<i>Alastair F. Donaldson, Alice Miller</i>	
Monitoring Distributed Controllers: When an Efficient LTL Algorithm on Sequences Is Needed to Model-Check Traces	557
<i>Alexandre Genon, Thierry Massart, Cédric Meuter</i>	
PSL Model Checking and Run-Time Verification Via Testers	573
<i>Amir Pnueli, Aleksandr Zaks</i>	

Industry Day: Abstracts of Invited Talks

Formal Methods for Security: Lightweight Plug-In or New Engineering Discipline	587
<i>Werner Stephan</i>	
Formal Methods in the Security Business: Exotic Flowers Thriving in an Expanding Niche	592
<i>David von Oheimb</i>	
Connector-Based Software Development: Deriving Secure Protocols	598
<i>Dusko Pavlovic</i>	
Model-Based Security Engineering for Real	600
<i>Jan Jürjens</i>	
Cost Effective Software Engineering for Security	607
<i>D. Randolph Johnson</i>	
Formal Methods and Cryptography	612
<i>Michael Backes, Birgit Pfitzmann, Michael Waidner</i>	

Verified Software Grand Challenge 617
 Jim Woodcock

Author Index 619