Lecture Notes in Computer Science 4085

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

Editorial Board

Jayadev Misra Tobias Nipkow
Emil Sekerinski (Eds.)

FM 2006: Formal Methods

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

Springer

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

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 Wassyng, 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

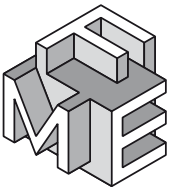
Henning Dierks
Guillaume Dufay
E. Allen Emerson
Bernd Fischer
Marcelo Frias
Madhu Gopinathan
Stefan Hallerstede
Tobias Heindel
Wim Hesselink
Hardi Hungar
Johan Jeuring
Aditya Kanade
Joseph Kiniry
Piotr Kordy
Tomas Krilavicius
Ruurd Kuiper
Linas Laibinis
David Lesens
Michael Luttenberger
Erik Arne Mathiesen
Farhad Mehta
Ali Mili
Anders Moller
Prasad Naldurg
Dirk Nowotka
Anne Pacalet
Mariela Pavlova
David Pichardie
Mike Poppleton
Alexander Pretschner
Hridesh Rajan
Abdolbaghi Rezazadeh
Abhik Roychoudhury
David Rydeheard
Norbert Schirmer
Paul Sevinc
Colin Snook
Marielle Stoelinga
Douglas Stuart
Helen Treharne
Laurent Voisin
Thai Son Wang
Bernd Westphal
Jim Woodcock
Letu Yang

Juegen Doser
Andy Edmunds
Neil Evans
John Fitzgerald
Paul Gibson
Bhargav Gulavani
Klaus Havelund
Rolf Hennicker
Matthias Hölzl
Daniel Jackson
Warren A. Hunt Jr.
Stephanie Kemper
Alexander Knapp
Piotr Kosiuczenko
Ingolf Krueger
Marcel Kyas
Rom Langerak
Kamal Lodaya
Monika Maidl
Tim McComb
Roland Meyer
Antoine Mine
Michael Möller
Rocco De Nicola
Peter O'Hearn
Joachim Parrow
Thomas Peikenkamp
Ken Pierce
Sanjiva Prasad
Cyril Proch
H. Rajasekaran
M. Birna van Riemsdijk
Oliver Ruething
Mannu Satpathy
Gerardo Schneider
Murali Sitaraman
Martin Steffen
Ketil Stølen
Martyn Thomas
Stavros Tripakis
Marina de Vos
Andrzej Wasowski
Luke Wildman
Fei Xie
Pamela Zave

Paul Hankes Drielsma
Martin Ellis
Dirk Fahland
Martin Fränzle
Simon Goldsmith
Christian Haack
James Heather
Martin Henson
Marieke Huisman
Suresh Jagannathan
Sven Jörges
Stefan Kiefer
Barbara König
Pavel Krcal
Wouter Kuijper
Ralf Laemmel
Kim Larsen
Antònia Lopes
Joao Marques-Silva
Alistair McEwan
Ronald Middelkoop
Bill Mitchell
Peter Müller
Aditya Nori
David von Oheimb
Dirk Pattinson
Simon Peyton-Jones
Jaco van de Pol
Viorel Preoteasa
Harald Raffelt
Axel Rauschmayer
Robby
Theo Ruys
Andreas Schäfer
Stefan Schwoon
Graeme Smith
Mark-Oliver Stehr
Harald Störrle
Christian Topnik
Emilio Tuosto
Thomas Wahl
Heike Wehrheim
Martin Wildmoser
Alex Yakovlev
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.



Microsoft Research

tourismhamilton.com

SAP

SQRL
Software Quality Research Laboratory

McMaster University
ENGINEERING

Table of Contents

Real Time

Industrial Experience

Specification and Refinement

Programming Languages

Algebra

Education

Formal Modelling of Systems

Formal Aspects of Java

Programming Languages

Model Checking

Industry Day: Abstracts of Invited Talks