Lecture Notes in Computer Science 5014

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

Jorge Cuellar Tom Maibaum
Kaisa Sere (Eds.)

FM 2008: Formal Methods

15th International Symposium on Formal Methods
Turku, Finland, May 26-30, 2008
Proceedings

Springer

Volume Editors

Jorge Cuellar
Siemens Corporate Technology
Otto-Hahn-Ring 6
81730 München, Germany
E-mail: jorge.cuellar@siemens.com

Tom Maibaum
McMaster University
Software Quality Research Laboratory
and Department of Computing and Software
1280 Main St West, Hamilton, ON L8S 4K1, Canada
E-mail: tom@maibaum.org

Kaisa Sere
Åbo Akademi University
Department of Information Technology
20520 Turku, Finland
E-mail: kaisa.sere@abo.fi

Library of Congress Control Number: 2008927062

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 3-540-68235-X Springer Berlin Heidelberg New York
ISBN-13 978-3-540-68235-6 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12271788 06/3180 5 4 3 2 1 0

Preface

This volume contains the proceedings of Formal Methods 2008, the 15th International Symposium on Formal Methods, organized by Åbo Akademi University, Turku, Finland, during May 26-30, 2008. The series of Formal Methods conferences is supported by FME (Formal Methods Europe), an independent association which aims to stimulate the use of, and the research on, formal methods for system development. The first event in this series was VDM Europe, held in 1987. The scope of the symposium has grown since then, encompassing all aspects of software and hardware that are amenable to formal analysis.

As in previous years, this symposium brought together innovators and practitioners in precise mathematical methods for software development, academic and industrial users as well as researchers, tool developers and vendors. We received 106 submissions from 24 countries, a demonstration of the international nature of the event. Each submission was carefully refereed by at least three reviewers. The Programme Committee finally selected 23 papers for presentation at the symposium after what was sometimes really extensive discussion! We would like to extend our thanks once more to all the members of the Programme Committee and to all the reviewers for their excellent and efficient work. (The names of all involved appear over the page.) Apart from the regular papers, there were five invited talks at the symposium, given by Arvind, Shmuel Katz, Paolo Bresciani, Jay Misra, and Dawson Engler. Arvind and Katz also submitted papers to accompany their talks and these are included in the volume.

The Formal Methods 2008 symposium also included various related events. There were five workshops, coordinated by the Workshop Chair, John Derrick: Formal aspects of virtual organizations, John Fitzgerald and Jeremy Bryans; Overture/VDM++, Peter Gorm Larsen and Shin Sahara; Refinement Workshop, John Derrick; Pilot Projects for the Grand Challenge in Verified Software, Jim Woodcock, and Computational Models for Cell Processes, Ion Petre and Ralph-Johan Back. There were also seven tutorials, coordinated by the Tutorial Chair, Marina Waldén: Computational Systems Biology (full day), Ion Petre and Ralph-Johan Back; Teaching formal methods to students in high school and introductory university courses (full day), Ralph-Johan Back; Event-B and the Rodin Platform (full day), Jean-Raymond Abrial; Why formal verification remains on the fringes of commercial development (full day), Arvind; Formal Methods and Signal Processing (half day), Raymond Boute; Runtime Model Checking of Multithreaded C Programs Using Automated Instrumentation Dynamic Partial Order Reduction and Distributed Checking (half day), Ganesh Gopalakrishnan and Yu Yang; and Formal modelling and analysis of real-time systems using UPPAAL (half day), Paul Pettersson and Wang Yi. There was also an associated Doctoral Symposium, organized by Elena Troubitsyna, that included presentations by doctoral students as well as a Poster and Tool Exhibition, organized by Michael Leuschel.

An Industry Day was organized by the Formal Techniques Industrial Association (ForTIA) in parallel with the first day of the main symposium. The first invited speaker of the symposium, Arvind, was shared between the main programme and that of the Industry Day. This associated event was organized by Peter Gorm Larsen and Sari Leppänen. Five short contributed papers from the Industry Day are included in this volume.

The electronic submission, refereeing and Programme Committee discussions were well supported (almost always!) by EasyChair, developed by Andrei Voronkov at the University of Manchester, UK. Our thanks to him and also to our publisher Springer, in particular to Anna Kramer for helping with the preparation of the proceedings. Pablo Castro worked hard on putting together this volume, ably assisting the editors. Finally, we would like to thank all the speakers, all the sponsors (listed at the end of the Preface), and especially the Organizing Committee for all the hard work necessary for putting on this great event.

May 2008

Jorge Cuellar
Tom Maibaum

Symposium Organization

The Department of Information Technologies at Åbo Akademi University, Turku, Finland together with the Formal Methods Europe association collaborated to the organization of the Formal Methods 2008 symposium. We would like to acknowledge the hard work of the following persons involved in the process of putting on Formal Methods 2008.

Symposium Chairs

General Chair	Kaisa Sere (Åbo Akademi University)
Programme Chairs	Jorge Cuellar (Siemens, Germany) Tom Maibaum (McMaster University)
Steering Committee	Dines Bjørner, John Fitzgerald, Marie-Claude Gaudel Stefania Gnesi, Ian Hayes, Pamela Zave, Jim Woodcock
Industry Day Chairs	Peter G. Larsen (Eng. College of Aarhus) Sari Leppänen (Nokia, Helsinki)
Workshop Chair	John Derrick (Sheffield University)
Tutorial Chair	Marina Waldén (Åbo Akademi University)
Doctoral Symposium Chair	Elena Troubitsyna (Åbo Akademi University)
Tools and Poster Exhibition Chair	Michael Leuschel (University of Düsseldorf)

Organizing Committee at Åbo Akademi University

Kaisa Sere (General Chair)
Marina Waldén (Finances)
Luigia Petre (Coordination)
Tiina Haanila (Secretary)
Magnus Dahlvik (Webmaster)
Johannes Eriksson (Photographer)

Programme Committee

Bernhard K. Aichernig	Technical University of Graz, Austria
Keijiro Araki	Kyushu University, Japan
Alessandro Armando	Genova University, Italy
Ralph-Johan Back	Åbo Akademi University, Turku, Finland
Gilles Barthe	INRIA at Sophia-Antiplois, France

David Basin	ETH, Zurich, Switzerland
Frank de Boer	CWI Amsterdam, The Netherlands
Ed Brinksma	University of Twente, The Netherlands
Dawson Engler	Stanford University, USA
Marcelo Frias	University of Buenos Aires, Argentina
Dimitra Giannakopoulou	RIACS/NASA Ames, USA
Radu Grosu	Stony Brook University, USA
Joshua Guttman	MITRE Corporation, USA
Constance Heitmeyer	NRL, USA
Cliff Jones	Newcastle University, UK
Shmuel Katz	Technion, Israel
Paddy Krishnan	Bond University, Australia
Axel van Lamsweerde	Louvain University, Belgium
Rustan Leino	Microsoft Research, Redmond, USA
Dominique Méry	Nancy University, France
Marius Minea	Technical University of Timisoara, Romania
Madhavan Mukund	CMI, Chennai Mathematical Institute, India
Cesar Munoz	National Institute of Aerospace, USA
Tobias Nipkow	Technical University of Munich, Germany
José Nuno Oliveira	University of Minho, Portugal
Paritosh K Pandya	Tata Institute of Fundamental Research, Mumbai, India
John Rushby	SRI, USA
Augusto Sampaio	University of Pernambuco, Brazil
Steve Schneider	University of Surrey, UK
Emil Sekerinski	McMaster University, Canada
Vitaly Shmatikov	University of Texas at Austin, USA
Douglas Smith	Kestrel, USA
Ketil Stølen	SINTEF and University of Oslo, Norway
Andrzej Tarlecki	Warsaw University, Poland
Sebastian Uchitel	Imperial College, UK and University of Buenos Aires, Argentina
Alan Wassyng	McMaster University, Canada
Roel Wieringa	Twente University, The Netherlands
Martin Wirsing	Ludwig-Maximilians-Universität, Munich, Germany
Pierre Wolper	University of Liege, Belgium
Jim Woodcock	University of York, UK

External Reviewers

Nazareno Aguirre
Zoe Andrews
Luis Barbosa
Manuel Barbosa
Frédéric Besson
Olivier Bournez
Guillaume Brat
Einar Broch Johnsen
Sean Callanan
Roberto Carbone

Supratik Chakraborty
Tom Chothia
Piotr Chrzastowski-Wachtel
Jacek Chrzaszcz
Dave Cllarke
Ernie Cohen
Pieter Cuijpers
Pedro D'Argenio
Deepak D'Souza
Ernst-Erich Doberkat
Adalberto Farias
David Feitelson
Maria João Frade
Leo Freitas
Juan Galeotti
Mihaela Gheorghiu Bobaru
Alwyn Goodloe
David Gries
Ian Hayes
Kelly Hayhurst
Alexei Iliasov
Ryszard Janicki
Ralph Jeffords
Michael Kaminski
Felix Klaedtke
Beata Konikowska
Wouter Kuijper
Rom Langerak
Sławomir Lasota
Peng Li
Kamal Lodaya
Mass Soldal Lund
Jeffrey Maddalon
Angelika Mader
Jacopo Mantovani
Jelena Marincic
Nicolas Markey
Peter Mehlitz
Larissa Meinicke
Sun Meng
Dominique Mery
Peter Mosses
Wojciech Mostowski
Alexandre Mota
K. Narayan Kumar
Martin Neuhaeusser
Olga Pacheco
Paritosh Pandya
Matthew Parkinson
Ken Pierce
Marta Pietkiewicz-Koutny
Lorenzo Platania
Serena Elisa Ponta
Ivan Porres
Viorel Preoteasa
R. Ramanujam
Rodrigo Ramos
Atle Refsdal
Arend Rensink
Tamara Rezk
Ragnhild Kobro Runde
Benedikt Schmidt
Cristina Seceleanu
Tiberiu Seceleanu
Fredrik Seehusen
Justin Seyster
Radu Siminiceanu
Bjørnar Solhaug
Kim Solin
Jorge Sousa Pinto
Mike Spivey
Christoph Sprenger
Martin Steffen
Meng Sun
S. P. Suresh
Sarah Thompson
Helen Treharne
Edward Turner
Michael Wahler
Freek Wiedijk
Burkhart Wolff
Andreas Wombacher
Jim Woodcock
Huang Xiaowan
Shaofa Yang
Santiago Zanella Beguelin
Artur Zawlocki
Xiangpeng Zhao
Marcelo d'Amorim
Jaco van de Pol
Xu Wang

Sponsors

We gratefully acknowledge the support and sponsorship from the following organizations: NOKIA, TUCS (Turku Centre for Computer Science), Stiftelsen för Åbo Akademi Forskningsinstitut (Foundation of the Åbo Akademi Research Institute), Faculty of Technology at Åbo Akademi University, Federation of Finnish Learned Societies, FORTIA (Formal Techniques Industrial Association), FME (Formal Methods Europe), and Distributed System Design Laboratory.

Table of Contents

Session 1. Invited Talks

Session 2. Programming Language Analysis

Session 3. Verification

Session 4. Real-Time and Concurrency

Session 5. Grand Chellenge Problems

Session 6. FM Practice

Session 7. Runtime Moitoring and Analysis

Session 8. Communication

Session 9. Constraint Analysis

Session 10. Design

Session 11. Industry Day