

*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

*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*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Jorge Cuellar Tom Maibaum  
Kaisa Sere (Eds.)

# FM 2008: Formal Methods

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

## 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

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 2008  
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-Antipolis, France

## VIII Organization

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 Wasssyng	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	Olivier Bournez
Zoe Andrews	Guillaume Brat
Luis Barbosa	Einar Broch Johnsen
Manuel Barbosa	Sean Callanan
Frédéric Besson	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 Mehltitz  
Larissa Meinicke  
Sun Meng  
Dominique Mery  
Peter Mosses  
Wojciech Mostowski  
Alexandre Mota  
K. Narayan Kumar

Martin Neuhaeuser  
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 Secoleanu  
Tiberiu Secoleanu  
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.



Distributed Systems Design Laboratory

# Table of Contents

## Session 1. Invited Talks

Aspects and Formal Methods . . . . .	1
<i>Shmuel Katz</i>	
Getting Formal Verification into Design Flow . . . . .	12
<i>Arvind, Nirav Dave, and Michael Katelman</i>	
Lessons in the Weird and Unexpected: Some Experiences from Checking Large Real Systems . . . . .	33
<i>Dawson Engler</i>	
Simulation, Orchestration and Logical Clocks . . . . .	34
<i>David Kitchen, Evan Powell, and Jayadev Misra</i>	

## Session 2. Programming Language Analysis

CoVaC: Compiler Validation by Program Analysis of the Cross-Product . . . . .	35
<i>Anna Zaks and Amir Pnueli</i>	
Lazy Behavioral Subtyping . . . . .	52
<i>Johan Dovland, Einar Broch Johnsen, Olaf Owe, and Martin Steffen</i>	
Checking Well-Formedness of Pure-Method Specifications . . . . .	68
<i>Arsenii Rudich, Ádám Darvas, and Peter Müller</i>	

## Session 3. Verification

Verifying Dynamic Pointer-Manipulating Threads . . . . .	84
<i>Thomas Noll and Stefan Rieger</i>	
Proofs and Refutations for Probabilistic Refinement . . . . .	100
<i>A.K. McIver, C.C. Morgan, and C. Gonzalia</i>	
Assume-Guarantee Verification for Interface Automata . . . . .	116
<i>Michael Emmi, Dimitra Giannakopoulou, and Corina S. Păsăreanu</i>	

## Session 4. Real-Time and Concurrency

Automated Verification of Dense-Time MTL Specifications Via Discrete-Time Approximation . . . . .	132
<i>Carlo A. Furia, Matteo Pradella, and Matteo Rossi</i>	

A Model Checking Language for Concurrent Value-Passing Systems . . . .	148
<i>Radu Mateescu and Damien Thivolle</i>	

## Session 5. Grand Challenge Problems

Verification of Mondex Electronic Purses with KIV: From a Security Protocol to Verified Code . . . . .	165
<i>Holger Grandy, Markus Bischof, Kurt Stenzel, Gerhard Schellhorn, and Wolfgang Reif</i>	
Incremental Development of a Distributed Real-Time Model of a Cardiac Pacing System Using VDM . . . . .	181
<i>Hugo Daniel Macedo, Peter Gorm Larsen, and John Fitzgerald</i>	

## Session 6. FM Practice

Industrial Use of Formal Methods for a High-Level Security Evaluation . . . . .	198
<i>Boutheina Chetali and Quang-Huy Nguyen</i>	
Secret Ninja Formal Methods . . . . .	214
<i>Joseph R. Kiniry and Daniel M. Zimmerman</i>	
Specification and Checking of Software Contracts for Conditional Information Flow . . . . .	229
<i>Torben Amtoft, John Hatchiff, Edwin Rodríguez, Robby, Jonathan Hoag, and David Greve</i>	

## Session 7. Runtime Monitoring and Analysis

JML Runtime Assertion Checking: Improved Error Reporting and Efficiency Using Strong Validity . . . . .	246
<i>Patrice Chalin and Frédéric Rioux</i>	
Provably Correct Runtime Monitoring (Extended Abstract) . . . . .	262
<i>Irem Aktug, Mads Dam, and Dilian Gurov</i>	

## Session 8. Communication

A Schedulerless Semantics of TLM Models Written in SystemC Via Translation into LOTOS . . . . .	278
<i>Olivier Ponsini and Wendelin Serwe</i>	
A Rigorous Approach to Networking: TCP, from Implementation to Protocol to Service . . . . .	294
<i>Tom Ridge, Michael Norrish, and Peter Sewell</i>	

## Session 9. Constraint Analysis

Constraint Prioritization for Efficient Analysis of Declarative Models ...	310
<i>Engin Uzuncaova and Sarfraz Khurshid</i>	
Finding Minimal Unsatisfiable Cores of Declarative Specifications .....	326
<i>Emina Torlak, Felix Sheng-Ho Chang, and Daniel Jackson</i>	
Precise Interval Analysis vs. Parity Games .....	342
<i>Thomas Gawlitza and Helmut Seidl</i>	

## Session 10. Design

Introducing Objects through Refinement .....	358
<i>Tim McComb and Graeme Smith</i>	
Masking Faults While Providing Bounded-Time Phased Recovery .....	374
<i>Borzo Bonakdarpour and Sandeep S. Kulkarni</i>	
Towards Consistent Specifications of Product Families .....	390
<i>Alexander Harhurin and Judith Hartmann</i>	

## Session 11. Industry Day

Formal Methods for Trustworthy Skies: Building Confidence in the Security of Aircraft Assets Distribution .....	406
<i>Scott Lintelman, Richard Robinson, Mingyan Li, and Krishna Sampigethaya</i>	
An Industrial Case: Pitfalls and Benefits of Applying Formal Methods to the Development of a Network-Centric RTOS .....	411
<i>Eric Verhulst, Gjalt de Jong, and Vitaliy Mezhyuev</i>	
Software Engineering with Formal Methods: Experiences with the Development of a Storm Surge Barrier Control System.....	419
<i>Klaas Wijbrans, Franc Buve, Robin Rijkers, and Wouter Geurts</i>	
Application of a Formal Specification Language in the Development of the “Mobile FeliCa” IC Chip Firmware for Embedding in Mobile Phone .....	425
<i>Taro Kurita, Miki Chiba, and Yasumasa Nakatsugawa</i>	
Safe and Reliable Metro Platform Screen Doors Control/Command Systems .....	430
<i>Thierry Lecomte</i>	
<b>Author Index</b> .....	435