

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

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 of Computer Science, Saarbruecken, Germany

Ana Cavalcanti Dennis Dams (Eds.)

FM 2009: Formal Methods

Second World Congress
Eindhoven, The Netherlands, November 2-6, 2009
Proceedings

Volume Editors

Ana Cavalcanti
University of York
Department of Computer Science
Heslington
York YO10 5DD, UK
E-mail: ana.cavalcanti@cs.york.ac.uk

Dennis Dams
Bell Laboratories
600 Mountain Ave.
Murray Hill
NJ 07974, USA
E-mail: dennis@research.bell-labs.com

Library of Congress Control Number: 2009936485

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	3-642-05088-3 Springer Berlin Heidelberg New York
ISBN-13	978-3-642-05088-6 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.com

© Springer-Verlag Berlin Heidelberg 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12778379 06/3180 5 4 3 2 1 0

Preface

FM 2009, the 16th International Symposium on Formal Methods, marked the 10th anniversary of the First World Congress on Formal Methods that was held in 1999 in Toulouse, France. We wished to celebrate this by advertising and organizing FM 2009 as the Second World Congress in the FM series, aiming to once again bring together the formal methods communities from all over the world. The statistics displayed in the table on the next page include the number of countries represented by the Programme Committee members, as well as of the authors of submitted and accepted papers.

Novel this year was a special track on tools and industrial applications. Submissions of papers on these topics were especially encouraged, but not given any special treatment. (It was just as hard to get a special track paper accepted as any other paper.) What we did promote, however, was a discussion of how originality, contribution, and soundness should be judged for these papers. The following questions were used by our Programme Committee.

- Does the tool provide a proof of concept, or solve an important problem?
- Is there an interesting algorithm implemented in the tool?
- Were new techniques used to implement the tool?
- If it is an industrial application, does it clearly present the lessons learned in relation to the use of formal methods?
- Is the tool available (not necessarily for free) to the community?
- Are there (measured or significant) experiments that support the claims?
- How does the tool scale to larger problems?
- What is the (potential) impact of the tool or case study?
- What is the complexity of the tool or application?

We believe these questions can help future authors and reviewers of such papers.

The authors of a selection of the papers included here will be invited to submit extended versions of their papers to special anniversary issues of two reputable journals: *Formal Aspects of Computing* and *Formal Methods in System Design*.

An event of this scale is only possible when many put their energy and passion together. We have attempted to thank all those people. If you feel you should have been included but are not, rest assured that this is not intentional, and please accept our apologies.

For the first time, a number of scientific events dedicated to Formal Methods and their application decided to co-locate under the heading of *Formal Methods Week (FMweek)*. We hope that you enjoyed FM 2009, as well as several of the other events. Or, did you miss it? Maybe next time then!

August 2009

Ana Cavalcanti
Dennis Dams

Statistics

number of PC members	83
number of countries of PC members	46
number of submissions	139
number of countries of submissions' authors	38
number of reviews per paper**	4
number of papers accepted*	45
number of countries of accepted papers' authors	23
number of invited papers	5

* There are 3 additional papers included from Industry Day

** with a few exceptions in both directions

Organization

Chairs

General	Jos Baeten
Workshop	Erik de Vink
Tutorial	Jan Friso Groote
Publicity	Arend Rensink
Tool Exhibition	Alexander Serebrenik
Doctoral Symposium	Mohammad Mousavi
	Emil Sekerinski
Industry Day	Jozef Hooman
	Andreas Roth
	Marcel Verhoef
Local Organization	Tijn Borghuis
	Christine van Gils
	Heleen de Morrée

Programme Committee

Ralph-Johan Back	Jasmin Fisher	Nils Klarlund
Jos Baeten	John Fitzgerald	Jens Knoop
Sergey Baranov	Limor Fix	Bob Kurshan
Gilles Barthe	Marc Frappier	Peter Gorm Larsen
Rahma Ben-Ayed	Marcelo Frias	Yves Ledru
Mohamed Bettaz	Masahiro Fujita	Insup Lee
Dines Bjørner	Marie-Claude Gaudel	Huimin Lin
Michael Butler	Stefania Gnesi	Zhiming Liu
Rodrigo Cardoso	Lindsay Groves	Nancy Lynch
Ana Cavalcanti (Chair)	Anthony Hall	Tom Maibaum
Flavio Corradini	Anne Haxthausen	Dino Mandrioli
Jorge Cuellar	Ian Hayes	Annabelle McIver
Dennis Dams (Chair)	Matthew Hennessy	Dominique Mery
Van Hung Dang	Leszek Holenderski	Marius Minea
Jim Davies	Ralf Huuck	Sjouke Mauw
Susanna Donatelli	Predrag Janicic	Peter Mueller
Jin Song Dong	Cliff Jones	Tobias Nipkow
Cindy Eisner	Rajeev Joshi	Manuel Nunez
Lars-Henrik Eriksson	Shmuel Katz	Jose Nuno Oliveira
Juhan-P. Ernits	Moonzoo Kim	Gordon Pace

Paritosh Pandya
 Alberto Pardo
 Frantisek Plasil
 Jaco van de Pol
 Ingrid Rewitzky
 Leila Ribeiro
 Augusto Sampaio
 Steve Schneider

Christel Seguin
 Emil Sekerinski
 Kaisa Sere
 Natalia Sidorova
 Marjan Sirjani
 Ketil Stolen
 Andrzej Tarlecki
 Axel van Lamsweerde

Daniel Varro
 Marcel Verhoef
 Jurgen Vinju
 Willem Visser
 Farn Wang
 Jim Woodcock
 Husnu Yenigun

Additional Reviewers

Nazareno Aguirre
 Bijan Alizadeh
 José Almeida
 David Arney
 Vlastimil Babka
 Ezio Bartocci
 Nazim Benaissa
 Josh Berdine
 Pierre Biebrer
 Jean-Paul Bodeveix
 Reinder Bril
 Lukas Bulwahn
 Andrew Butterfield
 Diletta Cacciagrano
 Cristiano Calcagno
 Jian Chang
 Jia-Fu Chen
 Chen Chunqing
 Manuel Clavel
 Robert Colvin
 Pieter Cuijpers
 Kriangsak Damchoom
 Francesco De Angelis
 Nikhil Dinesh
 Simon Doherty
 Brijesh Dongol
 Andrew Edmunds
 Michel Embe-Jiague
 Gabriel Erzse
 Alessandro Fantechi
 Yuzhang Feng
 Pietro Ferrara
 Miguel Ferreira
 Pascal Fontaine
 Benoît Fraikin

Adrian Francalanza
 David Frutos-Escrig
 Carlo Furia
 Rohit Gheyi
 Mike Gordon
 Bogdan Groza
 Tormod Haavalsrud
 Daniel Hedin
 Rolf Hennicker
 Hsi-Min Ho
 Shin Hong
 Andras Horvath
 Chung-Hao Huang
 Guo-Chiao Huang
 Marieke Huisman
 Juliano Iyoda
 Mohammad-Javad Izadi
 Bart Jacobs
 Tomasz Janowski
 Pavel Jezek
 Sun Jun
 Amir Kantor
 Ehsan Khamespanah
 Ramtin Khosravi
 Jan Kofron
 Natallia Kokash
 Pierre Konopacki
 Barbara Kordy
 Daniel Kroening
 Ruurd Kuiper
 Cesar Kunz
 Ralf Laemmel
 Linas Laibinis
 Jaewoo Lee
 Hermann Lehner

David Lester
 Yang Liu
 Luis Llana
 Kamal Lodaya
 Carlos Luna
 Mass Lund
 Yi Lv
 Issam Maamria
 Pasquale Malacaria
 Petra Malik
 Filip Maric
 Mieke Massink
 Franco Mazzanti
 Mercedes Merayo
 Stephan Merz
 Dale Miller
 Charles Morisset
 Alexandre Mota
 MohammadReza Mousavi
 Ned Nedialkov
 Truong Nguyen
 Van Nguyen
 Rotem Oshman
 Olga Pacheco
 Hong Pan
 Jun Pang
 Pavel Parizek
 David Parker
 Luigia Petre
 Jorge Pinto
 Nir Piterman
 Tomas Poch
 Andrea Polini
 Vinayak Prabhu
 Matteo Pradella

Viorel Preoteasa	Francois Siewe	Ton van Deursen
Niloofar Razavi	Neeraj Singh	Szilvia Varro-Gyapay
Barbara Re	Bjornar Solhaug	Ha Viet
Joris Rehm	Paola Spoletini	Marc Voorhoeve
Abdolbaghi Rezazadeh	Ofer Shtrichman	Shaohui Wang
Tamara Rezk	Jeremy Sproston	Shuling Wang
Oliviero Riganelli	Volker Stolz	Michael Weber
Mauno Rönkkö	Sayantan Surs	James Welch
Fernando Rosa-Velardo	Dejvuth Suwimonteerabuth	Kirsten Winter
Matteo Rossi	Andras Telcs	Simon Winwood
Ragnhild Runde	Mark Timmer	Hong-Hsin Wu
Mar Yah Said	Nikola Trcka	Rong-Shuan Wu
Cesar Sanchez	Helen Treharne	Hsuen-Chin Yang
Stefan Schwoon	Carmela Troncoso	Lv Yi
Fredrik Seehusen	Hoang Truong	Eduardo Zambon
Alexander Serebrenik	Ninh Truong	Santiago Zanella
Ondrej Sery	Edward Turner	Chenyi Zhang
Sharon Shoham	Shinya Umeno	Xian Zhang
Luis Sierra	Jan-Martijn van der Werf	Jianjun Zhao

FM Steering Committee

Dines Bjørner
 John Fitzgerald
 Marie-Claude Gaudel
 Stefania Gnesi
 Ian Hayes
 Jim Woodcock
 Pamela Zave

Workshops

FMIS - Formal Methods for Interactive Systems
 Organizers: Michael Harrison and Mieke Massink

CompMod - Computational Models for Cell Processes
 Organizers: Ralph-Johan Back, Ion Petre and Erik de Vink

FMA - Formal Methods for Aeronautics
 Organizers: Manuela Bujorianu, Michael Fisher, and Corina Pasareanu

QFM - Quantitative Formal Methods: Theory and Applications
 Organizers: Suzana Andova and Annabelle McIver

VDM and Overture
 Organizers: Peter Gorm Larsen and Jeremy Bryans

FAVO - Formal Aspects of Virtual Organizations

Organizers: John Fitzgerald and Jeremy Bryans

FOPARA - Foundational and Practical Aspects of Resource Analysis

Organizers: Marko van Eekelen and Olha Shkaravska

Tutorials

Analyzing UML/OCL Models with HOL-OCL

Tutors: Achim Brucker and Burkhard Wolff

Practical MPI and Pthread Dynamic Verification

Tutors: Ganesh Gopalakrishnan and Robert Kirby

Behavioral Analysis Using mCRL2

Tutors: Aad Mathijssen, Michel Reniers, and Tim Willemse

Constraint-Based Validation of Imperative Programs

Tutors: Michel Rueher and Arnaud Gotlieb

Bounded Model-Checking and Satisfiability-Checking: A Flexible Approach for
System Modeling and Verification

Tutors: Angelo Morzenti, Matteo Pradella, Matteo Rossi

Computational Systems Biology

Tutors: Ion Petre and Ralph-Johan Back

Rely/Guarantee-Thinking

Tutors: Joey Coleman and Cliff Jones

Doctoral Symposium Programme Committee

S. Arun-Kumar

Paulo Borba

Michael Butler

Jin Song Dong

Wan Fokkink

Ichiro Hasuo

Anna Ingolfsdottir

Joost-Pieter Katoen

Ian Mackie

MohammadReza Mousavi

Mila Dalla Preda

Emil Sekerinski

Sandeep Shukla

Bernd-Holger Schlingloff

Elena Troubitsyna

Tarmo Uustalu

Frits Vaandrager

Husnu Yenigun

Best Paper Awards to

Raymond Boute

Andre Platzer and Edmund Clarke

Special Thanks to

The local organizers

EasyChair, Andrei Voronkov, Tatiana Rybina

Congress Office TU/e

Formal Techniques Industrial Association (ForTIA)

Ursula Barth, Alfred Hofmann, Anna Kramer, Christine Reiss, Jessica Wengzik, and

Gokula Prakash at Springer

Van Abbemuseum

The city of Eindhoven

FMweek 2009

Sponsored by



Table of Contents

Invited Papers

Formal Methods for Privacy	1
<i>Michael Carl Tschantz and Jeannette M. Wing</i>	
What Can Formal Methods Bring to Systems Biology?	16
<i>Nicola Bonzanni, K. Anton Feenstra, Wan Fokkink, and Elzbieta Krepska</i>	
Guess and Verify – Back to the Future	23
<i>Colin O’Halloran</i>	
Verification, Testing and Statistics	33
<i>Sriram K. Rajamani</i>	
Security, Probability and Nearly Fair Coins in the Cryptographers’ Café	41
<i>Annabelle McIver, Larissa Meinicke, and Carroll Morgan</i>	

Model Checking I

Recursive Abstractions for Parameterized Systems	72
<i>Joxan Jaffar and Andrew E. Santosa</i>	
Abstract Model Checking without Computing the Abstraction	89
<i>Stefano Tonetta</i>	
Three-Valued Spotlight Abstractions	106
<i>Jonas Schrieb, Heike Wehrheim, and Daniel Wonisch</i>	
Fair Model Checking with Process Counter Abstraction	123
<i>Jun Sun, Yang Liu, Abhik Roychoudhury, Shanshan Liu, and Jin Song Dong</i>	

Compositionality

Systematic Development of Trustworthy Component Systems	140
<i>Rodrigo Ramos, Augusto Sampaio, and Alexandre Mota</i>	
Partial Order Reductions Using Compositional Confluence Detection . . .	157
<i>Frédéric Lang and Radu Mateescu</i>	

A Formal Method for Developing Provably Correct Fault-Tolerant Systems Using Partial Refinement and Composition	173
<i>Ralph Jeffords, Constance Heitmeyer, Myla Archer, and Elizabeth Leonard</i>	

Verification

Abstract Specification of the UBIFS File System for Flash Memory	190
<i>Andreas Schierl, Gerhard Schellhorn, Dominik Haneberg, and Wolfgang Reif</i>	
Inferring Mealy Machines	207
<i>Muzammil Shahbaz and Roland Groz</i>	
Formal Management of CAD/CAM Processes	223
<i>Michael Kohlhase, Johannes Lemburg, Lutz Schröder, and Ewaryst Schulz</i>	

Concurrency

Translating Safe Petri Nets to Statecharts in a Structure-Preserving Way	239
<i>Rik Eshuis</i>	
Symbolic Predictive Analysis for Concurrent Programs	256
<i>Chao Wang, Sudipta Kundu, Malay Ganai, and Aarti Gupta</i>	
On the Difficulties of Concurrent-System Design, Illustrated with a 2×2 Switch Case Study	273
<i>Edgar G. Daylight and Sandeep K. Shukla</i>	

Refinement

<i>Sums and Lovers</i> : Case Studies in Security, Compositionality and Refinement	289
<i>Annabelle K. McIver and Carroll C. Morgan</i>	
Iterative Refinement of Reverse-Engineered Models by Model-Based Testing	305
<i>Neil Walkinshaw, John Derrick, and Qiang Guo</i>	
Model Checking Linearizability via Refinement	321
<i>Yang Liu, Wei Chen, Yanhong A. Liu, and Jun Sun</i>	

Static Analysis

It's Doomed; We Can Prove It	338
<i>Jochen Hoenicke, K. Rustan M. Leino, Andreas Podelski, Martin Schüf, and Thomas Wies</i>	
“Carbon Credits” for Resource-Bounded Computations Using Amortised Analysis	354
<i>Steffen Jost, Hans-Wolfgang Loidl, Kevin Hammond, Norman Scaife, and Martin Hofmann</i>	
Field-Sensitive Value Analysis by Field-Insensitive Analysis	370
<i>Elvira Albert, Puri Arenas, Samir Genaim, and Germán Puebla</i>	

Theorem Proving

Making Temporal Logic Calculational: A Tool for Unification and Discovery	387
<i>Raymond Boute</i>	
A Tableau for CTL*	403
<i>Mark Reynolds</i>	
Certifiable Specification and Verification of C Programs	419
<i>Christoph Lüth and Dennis Walter</i>	
Formal Reasoning about Expectation Properties for Continuous Random Variables	435
<i>Osman Hasan, Naeem Abbasi, Behzad Akbarpour, Sofiène Tahar, and Reza Akbarpour</i>	

Semantics

The Denotational Semantics of <i>slotted-Circus</i>	451
<i>Paweł Gancarski and Andrew Butterfield</i>	
Unifying Probability with Nondeterminism	467
<i>Yifeng Chen and J.W. Sanders</i>	
Towards an Operational Semantics for Alloy	483
<i>Theophilos Giannakopoulos, Daniel J. Dougherty, Kathi Fisler, and Shriram Krishnamurthi</i>	
A Robust Semantics Hides Fewer Errors	499
<i>Steve Reeves and David Streader</i>	

Special Track: Industrial Applications I

Analysis of a Clock Synchronization Protocol for Wireless Sensor Networks	516
<i>Faranak Heidarian, Julien Schmaltz, and Frits Vaandrager</i>	
Formal Verification of Avionics Software Products	532
<i>Jean Souyris, Virginie Wiels, David Delmas, and Hervé Delseny</i>	
Formal Verification of Curved Flight Collision Avoidance Maneuvers: A Case Study	547
<i>André Platzter and Edmund M. Clarke</i>	

Object-Orientation

Connecting UML and VDM++ with Open Tool Support	563
<i>Kenneth Lausdahl, Hans Kristian Agerlund Lintrup, and Peter Gorm Larsen</i>	
Language and Tool Support for Class and State Machine Refinement in UML-B	579
<i>Mar Yah Said, Michael Butler, and Colin Snook</i>	
Dynamic Classes: Modular Asynchronous Evolution of Distributed Concurrent Objects	596
<i>Einar Broch Johnsen, Marcel Kyas, and Ingrid Chieh Yu</i>	
Abstract Object Creation in Dynamic Logic: To Be or Not to Be Created	612
<i>Wolfgang Ahrendt, Frank S. de Boer, and Immo Grabe</i>	

Pointers

Reasoning about Memory Layouts	628
<i>Holger Gast</i>	
A Smooth Combination of Linear and Herbrand Equalities for Polynomial Time Must-Alias Analysis	644
<i>Helmut Seidl, Vesal Vojdani, and Varmo Vene</i>	

Real-Time

On the Complexity of Synthesizing Relaxed and Graceful Bounded-Time 2-Phase Recovery	660
<i>Borzoo Bonakdarpour and Sandeep S. Kulkarni</i>	
Verifying Real-Time Systems against Scenario-Based Requirements	676
<i>Kim G. Larsen, Shuhao Li, Brian Nielsen, and Saulius Pusinskas</i>	

Special Track: Tools and Industrial Applications II

Formal Specification of a Cardiac Pacing System	692
<i>Artur Oliveira Gomes and Marcel Vinícius Medeiros Oliveira</i>	
Automated Property Verification for Large Scale B Models	708
<i>Michael Leuschel, Jérôme Falampin, Fabian Fritz, and Daniel Plagge</i>	
Reduced Execution Semantics of MPI: From Theory to Practice	724
<i>Sarvani Vakkalanka, Anh Vo, Ganesh Gopalakrishnan, and Robert M. Kirby</i>	

Model Checking II

A Metric Encoding for Bounded Model Checking	741
<i>Matteo Pradella, Angelo Morzenti, and Pierluigi San Pietro</i>	
An Incremental Approach to Scope-Bounded Checking Using a Lightweight Formal Method	757
<i>Danhua Shao, Sarfraz Khurshid, and Dewayne E. Perry</i>	
Verifying Information Flow Control over Unbounded Processes	773
<i>William R. Harris, Nicholas A. Kidd, Sagar Chaki, Somesh Jha, and Thomas Reps</i>	
Specification and Verification of Web Applications in Rewriting Logic	790
<i>María Alpuente, Demis Ballis, and Daniel Romero</i>	

Industry-Day Abstracts

Verifying the Microsoft Hyper-V Hypervisor with VCC	806
<i>Dirk Leinenbach and Thomas Santen</i>	
Industrial Practice in Formal Methods: A Review	810
<i>J.C. Bicarregui, J.S Fitzgerald, P.G. Larsen, and J.C.P. Woodcock</i>	
Model-Based GUI Testing Using UPPAAL at Novo Nordisk	814
<i>Ulrik H. Hjort, Jacob Illum, Kim G. Larsen, Michael A. Petersen, and Arne Skou</i>	
Author Index	819