

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

TU Dortmund University, 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 for Informatics, Saarbruecken, Germany

Dimitra Giannakopoulou
Dominique Méry (Eds.)

FM 2012: Formal Methods

18th International Symposium
Paris, France, August 27-31, 2012
Proceedings



Springer

Volume Editors

Dimitra Giannakopoulou
NASA Ames Research Center
Mail Stop 269-2
Moffett Field, CA 94035, USA
E-mail: dimitra.giannakopoulou@nasa.gov

Dominique Méry
Université de Lorraine, LORIA
Campus Scientifique, BP 239
54506 Vandoeuvre-lès-Nancy, France
E-mail: dominique.mery@loria.fr

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-32758-2 e-ISBN 978-3-642-32759-9
DOI 10.1007/978-3-642-32759-9
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012944269

CR Subject Classification (1998): D.2.4-5, F.4, D.2, F.3, J.2, J.3, K.6, F.1.1, F.2.2

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© Springer-Verlag Berlin Heidelberg 2012

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

FM 2012 was the 18th in a series of symposia organized by Formal Methods Europe, an independent association whose aim is to stimulate the use of, and research on, formal methods for software development. The symposia have been notably successful in bringing together innovators and practitioners in precise mathematical methods for software and systems development, industrial users, as well as researchers. In August 2012, the *Conservatoire National des Arts et Métiers* (Le Cnam Paris) hosted FM 2012 in Paris (France).

The special theme of FM 2012 was “Interdisciplinary Formal Methods,” with the goal of highlighting the development and application of formal methods in connection with a variety of disciplines including medicine, biology, human cognitive modeling, human automation interactions, and aeronautics. We were honored to have three invited speakers whose talks emphasized the special theme.

Martin Abadi, with his talk titled “Software Security – A Formal Perspective,” discussed software security with an emphasis on low-level attacks and defenses and on their formal aspects. Asaf Degani gave a talk titled “Formal Methods in the Wild: Trains, Planes, and Automobiles.” Through this talk, Dr. Degani drew upon his experience with aerospace and automotive applications to provide a perspective on how formal methods could improve the design of such applications. Finally, Alan Wasssyng, in his talk titled “Who Are We, and What Are We Doing Here?,” stressed the importance of viewing formal methods from a rigorous software engineering perspective, and discussed his experiences with the certification of software-intensive systems. All three talks raised the awareness of the community to the fact that formal methods live in the intersection of disciplines; research in this domain must also consider how to increase the industrial impact of formal methods.

FM 2012 welcomed submissions in the following areas, among others:

- Interdisciplinary formal methods: techniques, tools and experiences demonstrating formal methods in interdisciplinary frameworks, such as formal methods related to maintenance, human automation interaction, human in the loop, system engineering, medicine and biology
- Formal methods in practice: industrial applications of formal methods, experience with introducing formal methods in industry, tool usage reports, experiments with challenge problems
- Tools for formal methods: advances in automated verification and model-checking, integration of tools, environments for formal methods, experimental validation of tools
- Role of formal methods in software and systems engineering: development processes with formal methods, usage guidelines for formal methods, method integration
- Theoretical foundations: all aspects of theory related to specification, verification, refinement, and static and dynamic analysis

- Teaching formal methods: insight, evaluations and suggestions for courses of action regarding the teaching of formal methods, including teaching experiences, educational resources, the integration of formal methods into the curriculum, the definition of a formal methods body of knowledge, etc

We solicited two types of contributions: research papers and tool demonstration papers. We received submissions from 39 countries around the world: 162 abstracts followed by 132 full submissions. The selection process was rigorous. Each paper received at least four reviews. We obtained external reviews for papers that lacked expertise within the Program Committee. The Program Committee, after long and very careful discussions of the submitted papers, decided to accept only 28 full papers and seven tool papers, which corresponds to an overall acceptance rate of approximately 26%. Some of the accepted papers were additionally shepherded by expert members of the Program Committee to ensure the quality of their final version. The accepted papers made a scientifically strong and exciting program, which triggered interesting discussions and exchange of ideas among the FM participants. The accepted papers cover several aspects of formal methods, including verification, synthesis, runtime monitoring, testing and controller synthesis, as well as novel applications of formal methods in interesting domains such as satellites, autonomous vehicles, and disease dynamics.

We would like to thank all authors who submitted their work to FM 2012. Without their excellent contributions we would not have managed to prepare a strong program. We are grateful to the Program Committee members and external reviewers for their high-quality reviews and dedication. Finally, we wish to thank the Steering Committee members for their excellent support. The logistics of our job as Program Chairs were facilitated by the EasyChair system.

June 2012

Dimitra Giannakopoulou
Dominique Méry

Symposium Organization

We are grateful to Formal Methods Europe (FME) and the Conservatoire National des Arts et Métiers (Le Cnam Paris) for organizing FM 2012. Our special thanks to the faculty, students, and staff of Mefosyloma Research Group, who volunteered their time in the Organizing Committee.

General Chairs

Kamel Barkaoui
Béatrice Bérard

Cedric, CNAM, France
LIP6, UPMC, France

Program Chairs

Dimitra Giannakopoulou
Dominique Méry

NASA Ames, USA
Université de Lorraine, France

Workshop Chairs

Nihal Pekergin
Laure Petrucci
Tayssir Touili

LACL, University Paris-Est Créteil
LIPN, University Paris-Nord
LIAFA, University Paris Diderot - Paris 7

Tutorials Chairs

Serge Haddad
Fabrice Kordon

LSV, ENS Cachan
LIP6, University Pierre et Marie Curie

Industry Day Chairs

Karim Djouani
Thierry Lecomte
Bruno Monsuez
Isabelle Perseil

LISSI, University Paris-Est Créteil
ClearSy R&D, Aix en Provence
LEI, Ensta ParisTech
LTCI, Telecom ParisTech

Doctoral Chairs

Christine Choppy
David Delahaye
Kais Klai
Franck Pommereau

LIPN, University Paris-Nord
Cedric, CNAM
LIPN, University Paris-Nord
IBISC, University of Évry

Publicity Chairs

Hanna Klaudel

Frédéric Lemoine

Franck Pommereau

Olivier Pons

IBISC, University of Évry

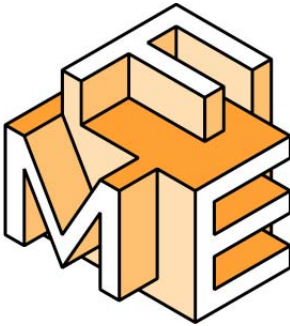
Computer Science Department, CNAM

IBISC, University of Évry

Cedric, CNAM

Sponsors

We are thankful for the organizational support from FME (Formal Methods Europe) and CNAM (Conservatoire National des Arts et Métiers). We gratefully acknowledge sponsorships from the following organizations: Digiteo, Ada-Core, SNCF, LEI, ENSTA ParisTech, Mefosyloma Research Group: CEDRIC (CNAM), LACL (UPEC Créteil), LIP6 (Université Pierre et Marie Curie), LIPN (Université Paris-Nord), LSV (ENS Cachan), IBISC (Univ. Evry), LTCI (Télécom ParisTech).



le cnam

Program Committee

Yamine Ait Ameur

Keijiro Araki

Jos Baeten

Howard Barringer

Saddek Bensalem

Bruno Blanchet

Ahmed Bouajjani

IRIT/ENSEIHT, France

Kyushu University, Japan

TUE, The Netherlands

The University of Manchester, UK

VERIMAG, France

INRIA, France

LIAFA, University of Paris 7 (Paris Diderot),
France

Patricia Bouyer

Victor Braberman

Michael Butler

Andrew Butterfield

Ana Cavalcanti

LSV, CNRS and ENS Cachan, France

Universidad de Buenos Aires, Argentina

University of Southampton, UK

Trinity College Dublin, Ireland

University of York, UK

Krishnendu Chatterjee	Institute of Science and Technology (IST), Austria
Marsha Chechik	University of Toronto, Canada
Yu-Fang Chen	Academia Sinica, Taiwan
Leonardo De Moura	Microsoft Research, USA
Dino Distefano	Queen Mary, University of London, UK
Matt Dwyer	University of Nebraska, USA
Bernd Finkbeiner	Saarland University, Germany
J.S. Fitzgerald	Newcastle University, UK
Dimitra Giannakopoulou	NASA Ames Research Center, USA
Stefania Gnesi	ISTI-CNR, Italy
Patrice Godefroid	Microsoft Research, USA
Ganesh Gopalakrishnan	University of Utah, USA
Kim Guldstrand Larsen	Aalborg University, Denmark
Klaus Havelund	Jet Propulsion Laboratory, California Institute of Technology, USA
Ian J. Hayes	University of Queensland, Australia
Matthew Hennessy	Trinity College Dublin, Ireland
Jane Hillston	University of Edinburgh, UK
Bart Jacobs	Institute for Computing and Information Sciences (ICIS), Radboud University Nijmegen, The Netherlands
Claude Jard	ENS Cachan Bretagne, France
Panagiotis Katsaros	Aristotle University of Thessaloniki, Greece
Sarfraz Khurshid	The University of Texas at Austin, USA
Daniel Kroening	Oxford University, UK
Marta Kwiatkowska	Oxford University, UK
Pascale Le Gall	Université d'Evry, France
Rustan Leino	Microsoft Research, USA
Michael Leuschel	University of Düsseldorf, Germany
Zhiming Liu	United Nations University - International Institute for Software Technology, Macau
Tom Maibaum	McMaster University, Canada
Rupak Majumdar	Max Planck Institute, Germany
Annabelle Mciver	Macquarie University, Australia
Dominique Méry	Université de Lorraine, LORIA, France
Cesar Munoz	National Aeronautics and Space Administration, USA
Fernando Orejas	UPC, Spain
Isabelle Perseil	INSERM, France
Andre Platzer	Carnegie Mellon University, USA
Shengchao Qin	Teesside University, UK
S. Ramesh	General Motors R&D, India
Jean-Francois Raskin	ULB, Belgium
Neha Rungta	NASA Ames Research Center, USA
Augusto Sampaio	Federal University of Pernambuco, Brazil

Bernhard Schaetz	TU München, Germany
Wolfram Schulte	Microsoft Research, USA
Kaisa Sere	Abo Akademi University, Finland
Bernhard Steffen	University of Dortmund, Germany
Kenji Taguchi	AIST, Japan
Francois Vernadat	LAAS-CNRS INSA, France
Willem Visser	Stellenbosch University, South Africa
Michael Whalen	University of Minnesota, USA

Additional Reviewers

Aananthakrishnan, Sriram	Chiang, Wei-Fan
Aguirre, Nazareno	Cirstea, Horatiu
Aiguier, Marc	Clark, Allan
Akshay, S.	Cohen, Cyril
Albarghouthi, Aws	Colley, John
Alves, Vander	Craciun, Florin
Andrews, Zoe	Danos, Vincent
Axel, Legay	David, Alexandre
Ballarini, Paolo	David, Cristina
Banach, Richard	de Halleux, Jonathan
Bartocci, Ezio	De Vink, Erik
Batina, Lejla	de Vries, Edsko
Batista, Thais	Decker, Normann
Bauer, Sebastian	Degerlund, Fredrik
Becker, Klaus	Diciolla, Marco
Bernardi, Giovanni	Dimitrova, Rayna
Beyer, Dirk	D'ippolito, Nicolas
Blech, Jan Olaf	Dixit, Manoj
Bortolussi, Luca	Dobrikov, Ivo
Bosnacki, Dragan	Dongol, Brijesh
Boström, Pontus	Draeger, Klaus
Boyer, Benoit	Dragoi, Cezara
Bozga, Marius	Du, Dehui
Brain, Martin	Edmunds, Andrew
Bryans, Jeremy W.	Ehlers, Rüdiger
Cassez, Franck	Enea, Constantin
Castro, Pablo	Faber, Johannes
Cerny, Pavol	Falcone, Ylies
Chawdhary, Aziem	Fantechi, Alessandro
Chen, Taolue	Faymonville, Peter
Chen, Zhenbang	Feng, Lu
Cheng, Chih-Hong	Ferrari, Alessio
Cheng, Chihong	Florian, Mihai

Fontaine, Pascal
 Funes, Diego
 Galpin, Vashti
 Gao, Sicun
 Gaston, Christophe
 Gherghina, Cristian
 Gilmore, Stephen
 Gopinath, Divya
 Gorogiannis, Nikos
 Grigore, Radu
 Gulwani, Sumit
 Haar, Stefan
 Han, Tingting
 Hasuo, Ichiro
 Hawblitzel, Chris
 He, Guanhua
 Heljanko, Keijo
 Hladik, Pierre-Emmanuel
 Holik, Lukas
 Hou, Ping
 Howar, Falk
 Huang, Yanhong
 Ingram, Claire
 Isberner, Malte
 Ishikawa, Fuyuki
 Jacobs, Bart
 Jastram, Michael
 Jonker, Hugo
 Kaiser, Alexander
 Kong, Weiqiang
 Koutavas, Vasileios
 Krebbers, Robbert
 Kupriyanov, Andrey
 Kusakabe, Shigeru
 Ladenberger, Lukas
 Laibinis, Linas
 Larsen, Peter Gorm
 Latella, Diego
 Lawford, Mark
 Le Botlan, Didier
 Lerner, Benjamin
 Leroux, Jerome
 Lewis, Matt
 Li, Chun
 Li, Guodong

Li, Xiaoshan
 Loos, Sarah
 Loreti, Michele
 Maamria, Issam
 Maddalon, Jeff
 Martins, João G.
 Massoni, Tiago
 Mateescu, Maria-Emanuela-Canini
 Melgratti, Hernan
 Mercer, Eric
 Mereacre, Alexandru
 Merz, Stephan
 Mikućionis, Marius
 Mochio, Hiroshi
 Mohalik, Swarup
 Morgan, Carroll
 Moser, Heinrich
 Moskal, Michał
 Mou, Dongyue
 Mounier, Laurent
 Møller, Mikael H.
 Nadales Agut, Damian
 Narkawicz, Anthony
 Naujokat, Stefan
 Navarro-Lopez, Eva
 Ndukwu, Ukachukwu
 Neovius, Mats
 Nimal, Vincent
 Nokhbeh Zaeem, Razieh
 Nyman, Ulrik
 Oliveira, Marcel
 Oliveras, Albert
 Omori, Yoichi
 Parker, David
 Patcas, Lucian
 Pavese, Esteban
 Person, Suzette
 Peter, Hans-Jörg
 Petre, Luigia
 Plagge, Daniel
 Qamar, Nafees
 Quesel, Jan-David
 Quilbeuf, Jean
 Rabe, Markus
 Radhakrishna, Arjun

Raman, Vishwanath
Rathke, Julian
Rayadurgam, Sanjai
Reger, Giles
Renshaw, David
Rezine, Ahmed
Rocha, Camilo
Roveri, Marco
Ruemmer, Philipp
Ruething, Oliver
Rusinowitch, Michael
Rydeheard, David
Rüthing, Oliver
Salay, Rick
Salehi Fathabadi, Asieh
Sampath, Prahladavaradan
Sanders, Jeff
Satpathy, M
Satpathy, Manoranjan
Schäf, Martin
Servais, Frédéric
Serwe, Wendelin
Sezgin, Ali
Sharma, Subodh
Siddiqui, Junaid Haroon
Sighireanu, Mihaela
Siminiceanu, Radu
Singh, Neeraj Kumar
Smans, Jan
Snook, Colin
Solin, Kim
Srba, Jiri
Strazny, Tim
Sun, Jun

Tarasyuk, Anton
Tautschnig, Michael
Tesnim, Abdellatif
Thoma, Daniel
Tiezzi, Francesco
Tkachuk, Oksana
Trachtenherz, David
Traonouez, Louis-Marie
Tribastone, Mirco
Troya, Javier
Tsay, Yih-Kuen
Tsiopoulos, Leonidas
Uchitel, Sebastian
Vafeiadis, Viktor
Vain, Juri
Varacca, Daniele
Venet, Arnaud
Verdejo, Alberto
Verhoef, Marcel
Villard, Jules
Vojnar, Tomas
Wang, Bow-Yaw
Wassyng, Alan
Winter, Kirsten
Wright, Stephen
Yamagata, Yoriyuki
Yang, Guowei
Yeganeh, Sanaz
Zantema, Hans
Zhang, Chenyi
Zhang, Lingming
Zhu, Ping
Zubkova, Nadya
Zufferey, Damien

Table of Contents

Software Security: A Formal Perspective (Notes for a Talk)	1
<i>Martín Abadi</i>	
Formal Methods in the Wild: Trains, Planes, & Automobile	6
<i>Asaf Degani</i>	
Who Are We, and What Are We Doing Here?	7
<i>Alan Wassyn</i>	
Automata Learning through Counterexample Guided Abstraction Refinement	10
<i>Fides Aarts, Faranak Heidarian, Harco Kuppens, Petur Olsen, and Frits Vaandrager</i>	
JULIENNE: A Trace Slicer for Conditional Rewrite Theories	28
<i>María Alpuente, Demis Ballis, Francisco Frechina, and Daniel Romero</i>	
IMITATOR 2.5: A Tool for Analyzing Robustness in Scheduling Problems	33
<i>Étienne André, Laurent Fribourg, Ulrich Kühne, and Romain Soulat</i>	
Maximal and Compositional Pattern-Based Loop Invariants	37
<i>Virginia Aponte, Pierre Courtieu, Yannick Moy, and Marc Sango</i>	
A Formal Approach to Autonomous Vehicle Coordination	52
<i>Mikael Asplund, Atif Manzoor, Mélanie Bouroche, Siobhán Clarke, and Vinny Cahill</i>	
Quantified Event Automata: Towards Expressive and Efficient Runtime Monitors	68
<i>Howard Barringer, Yliès Falcone, Klaus Havelund, Giles Reger, and David Rydeheard</i>	
Decentralised LTL Monitoring	85
<i>Andreas Bauer and Yliès Falcone</i>	
Measles Epidemics and PEPA: An Exploration of Historic Disease Dynamics Using Process Algebra	101
<i>Soufiene Benkirane, Rachel Norman, Erin Scott, and Carron Shankland</i>	

A Certified Constraint Solver over Finite Domains	116
<i>Matthieu Carlier, Catherine Dubois, and Arnaud Gotlieb</i>	
Collaborative Verification and Testing with Explicit Assumptions	132
<i>Maria Christakis, Peter Müller, and Valentin Wüstholtz</i>	
TLA ⁺ Proofs	147
<i>Denis Cousineau, Damien Doligez, Leslie Lamport, Stephan Merz, Daniel Ricketts, and Hernán Vanzetto</i>	
The Modal Transition System Control Problem	155
<i>Nicolás D'Ippolito, Victor Braberman, Nir Piterman, and Sebastián Uchitel</i>	
When Structural Refinement of Components Keeps Temporal Properties over Reconfigurations	171
<i>Julien Dormoy, Olga Kouchnarenko, and Arnaud Lanoix</i>	
Error Invariants	187
<i>Evren Ermiş, Martin Schäfer, and Thomas Wies</i>	
Correctness of Pointer Manipulating Algorithms Illustrated by a Verified BDD Construction	202
<i>Mathieu Giordano and Martin Strecker</i>	
A Formal Framework for Modelling Coercion Resistance and Receipt Freeness	217
<i>James Heather and Steve Schneider</i>	
Using Time to Add Order to Distributed Testing	232
<i>Robert M. Hierons, Mercedes G. Merayo, and Manuel Núñez</i>	
A Verification Toolkit for Numerical Transition Systems: Tool Paper . . .	247
<i>Hossein Hojjat, Filip Konečný, Florent Garnier, Radu Iosif, Viktor Kuncak, and Philipp Rümmer</i>	
Satellite Rendezvous and Conjunction Avoidance: Case Studies in Verification of Nonlinear Hybrid Systems	252
<i>Taylor T. Johnson, Jeremy Green, Sayan Mitra, Rachel Dudley, and Richard Scott Erwin</i>	
Executing Formal Semantics with the \mathbb{K} Tool	267
<i>David Lazar, Andrei Arusoaie, Traian Florin Şerbănuţă, Chucky Ellison, Radu Mereuta, Dorel Lucanu, and Grigore Roşu</i>	

Automatic Compositional Verification of Timed Systems	272
<i>Shang-Wei Lin, Yang Liu, Jun Sun, Jin Song Dong, and Étienne André</i>	
Applying Software Model Checking Techniques for Behavioral UML Models	277
<i>Orna Grumberg, Yael Meller, and Karen Yorav</i>	
Reachability Analysis of the HTML5 Parser Specification and Its Application to Compatibility Testing	293
<i>Yasuhiko Minamide and Shunsuke Mori</i>	
Theory and Techniques for Synthesizing Efficient Breadth-First Search Algorithms	308
<i>Srinivas Nedunuri, Douglas R. Smith, and William R. Cook</i>	
Improved BDD-Based Discrete Analysis of Timed Systems	326
<i>Truong Khanh Nguyen, Jun Sun, Yang Liu, Jin Song Dong, and Yan Liu</i>	
Experience Report on Designing and Developing Control Components Using Formal Methods	341
<i>Ammar Osaiweran, Tom Fransen, Jan Friso Groote, and Bart van Rijnsoever</i>	
Automatic Dimensional Analysis of Cyber-Physical Systems	356
<i>Sam Owre, Indranil Saha, and Natarajan Shankar</i>	
Validating B, Z and TLA ⁺ Using PROB and Kodkod	372
<i>Daniel Plagge and Michael Leuschel</i>	
From Hoare Logic to Matching Logic Reachability	387
<i>Grigore Roşu and Andrei Ştefănescu</i>	
Distribution of Modal Transition Systems	403
<i>German E. Sibay, Sebastián Uchitel, Victor Braberman, and Jeff Kramer</i>	
Efficient Malware Detection Using Model-Checking	418
<i>Fu Song and Tayssir Touili</i>	
Formalization of Incremental Simplex Algorithm by Stepwise Refinement	434
<i>Mirko Spasić and Filip Marić</i>	
VMC: A Tool for Product Variability Analysis	450
<i>Maurice H. ter Beek, Franco Mazzanti, and Aldi Sulova</i>	

Specification-Based Test Repair Using a Lightweight Formal Method . . .	455
<i>Guowei Yang, Sarfraz Khurshid, and Miryung Kim</i>	
A “Hybrid” Approach for Synthesizing Optimal Controllers of Hybrid Systems: A Case Study of the Oil Pump Industrial Example	471
<i>Hengjun Zhao, Naijun Zhan, Deepak Kapur, and Kim G. Larsen</i>	
Author Index	487