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

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 Wassyng, 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	Cedric, CNAM, France
Béatrice Bérard	LIP6, UPMC, France

Program Chairs

Dimitra Giannakopoulou	NASA Ames, USA
Dominique Méry	Université de Lorraine, France

Workshop Chairs

Nihal Pekergin	LACL, University Paris-Est Créteil
Laure Petrucci	LIPN, University Paris-Nord
Tayssir Touili	LIAFA, University Paris Diderot - Paris 7

Tutorials Chairs

Serge Haddad	LSV, ENS Cachan
Fabrice Kordon	LIP6, University Pierre et Marie Curie

Industry Day Chairs

Karim Djouani	LISSI, University Paris-Est Créteil
Thierry Lecomte	ClearSy R&D, Aix en Provence
Bruno Monsuez	LEI, Ensta ParisTech
Isabelle Perseil	LTCI, Telecom ParisTech

Doctoral Chairs

Christine Choppy	LIPN, University Paris-Nord
David Delahaye	Cedric, CNAM
Kais Klai	LIPN, University Paris-Nord
Franck Pommereau	IBISC, University of Évry

Publicity Chairs

Hanna Klaudel	IBISC, University of Évry
Frédéric Lemoine	Computer Science Department, CNAM
Franck Pommereau	IBISC, University of Évry
Olivier Pons	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 orgnanizations: Digiteo, AdaCore, 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).

Program Committee

Yamine Ait Ameur	IRIT/ENSEIHT, France
Keijiro Araki	Kyushu University, Japan
Jos Baeten	TUE, The Netherlands
Howard Barringer	The University of Manchester, UK
Saddek Bensalem	VERIMAG, France
Bruno Blanchet	INRIA, France
Ahmed Bouajjani	LIAFA, University of Paris 7 (Paris Diderot), France
Patricia Bouyer	LSV, CNRS and ENS Cachan, France
Victor Braberman	Universidad de Buenos Aires, Argentina
Michael Butler	University of Southampton, UK
Andrew Butterfield	Trinity College Dublin, Ireland
Ana Cavalcanti	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
Aguirre, Nazareno
Aiguier, Marc
Akshay, S.
Albarghouthi, Aws
Alves, Vander
Andrews, Zoe
Axel, Legay
Ballarini, Paolo
Banach, Richard
Bartocci, Ezio
Batina, Lejla
Batista, Thais
Bauer, Sebastian
Becker, Klaus
Bernardi, Giovanni
Beyer, Dirk
Blech, Jan Olaf
Bortolussi, Luca
Bosnacki, Dragan
Boström, Pontus
Boyer, Benoit
Bozga, Marius
Brain, Martin
Bryans, Jeremy W.
Cassez, Franck
Castro, Pablo
Cerny, Pavol
Chawdhary, Aziem
Chen, Taolue
Chen, Zhenbang
Cheng, Chih-Hong
Cheng, Chihong
Chiang, Wei-Fan
Cirstea, Horatiu
Clark, Allan
Cohen, Cyril
Colley, John
Craciun, Florin
Danos, Vincent
David, Alexandre
David, Cristina
de Halleux, Jonathan
De Vink, Erik
de Vries, Edsko
Decker, Normann
Degerlund, Fredrik
Diciolla, Marco
Dimitrova, Rayna
D'ippolito, Nicolas
Dixit, Manoj
Dobrikov, Ivo
Dongol, Brijesh
Draeger, Klaus
Dragoi, Cezara
Du, Dehui
Edmunds, Andrew
Ehlers, Rüdiger
Enea, Constantin
Faber, Johannes
Falcone, Ylies
Fantechi, Alessandro
Faymonville, Peter
Feng, Lu
Ferrari, Alessio
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
Mikučionis, 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
Yeganefard, Sanaz
Zantema, Hans
Zhang, Chenyi
Zhang, Lingming
Zhu, Ping
Zubkova, Nadya
Zufferey, Damien

Table of Contents