

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

Gilles Barthe Alberto Pardo
Gerardo Schneider (Eds.)

Software Engineering and Formal Methods

9th International Conference, SEFM 2011
Montevideo, Uruguay, November 14-18, 2011
Proceedings



Springer

Volume Editors

Gilles Barthe

Fundación IMDEA Software, Facultad de Informática (UPM)
Campus Montegancedo, 28660 Boadilla del Monte, Madrid, Spain
E-mail: gilles.barthe@imdea.org

Alberto Pardo

Universidad de la República
Facultad de Ingeniería, Instituto de Computación
Julio Herrera y Reissig 565 - Piso 5, 11300 Montevideo, Uruguay
E-mail: pardo@fing.edu.uy

Gerardo Schneider

Chalmers | University of Gothenburg
Department of Computer Science and Engineering
Kunskapsgatan 3, 41756 Gothenburg, Sweden
and
University of Oslo, Department of Informatics
PB 1080 Blindern, 0316 Oslo, Norway,
E-mail: gersch@chalmers.se

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-24689-0

e-ISBN 978-3-642-24690-6

DOI 10.1007/978-3-642-24690-6

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011938201

CR Subject Classification (1998): D.2.4, D.2, F.3, D.3, D.1.5, C.2, C.2.4

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© Springer-Verlag Berlin Heidelberg 2011

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

This volume contains the proceedings of the 9th International Conference on Software Engineering and Formal Methods (SEFM 2011) held on November 14–18, 2011 in Montevideo, Uruguay, under the auspices of the Facultad de Ingeniería (InCo), Universidad de la República, Uruguay. The aim of SEFM is to bring together practitioners and researchers from academia, industry and government to advance the state of the art in formal methods, to scale up their application in software industry and to encourage their integration with practical engineering methods.

The Program Committee of SEFM 2011 received 105 abstracts and 85 full submissions from all over the world. We would like to thank all authors for submitting their papers. Each paper was reviewed by at least three reviewers. Based on the review reports and intensive discussions conducted electronically, the Program Committee selected 22 regular papers, 2 tool papers and 1 short paper (acceptance rate around 29%), for inclusion in this volume. We would like to thank the Program Committee members and all reviewers for their efforts in the selection process.

Besides the regular session, the conference held a special track devoted to “Modelling for Sustainable Development”, organized by Antonio Cerone from UNU-IIST. The special track received 7 submissions and accepted 5 papers, which are included in this volume.

In addition to the contributed papers, the conference program included four keynote speakers: Holger Hermanns (Saarland University, Germany), Mike Hinchey (LERO, Ireland) and Daniel Le Métayer (INRIA, France) for the main track, and Matteo Pedercini (Millennium Institute, USA) for the special track.

As is the tradition with SEFM, the conference was preceded by a graduate school and tutorials. The school courses were offered by: Dave Clarke (Katholieke Universiteit Leuven, Belgium), Klaus Havelund (Jet Propulsion Laboratory, USA), Yassine Lakhnech (University Joseph Fourier / VERIMAG, France), Martin Leucker (University of Lübeck, Germany), Davide Sangiorgi (INRIA, France, and University of Bologna, Italy), and Tarmo Uustalu (Tallin University of Technology, Estonia).

The tutorials were offered by: Gustavo Betarte (Universidad de la República, Uruguay), Pedro D’Argenio (Universidad Nacional de Córdoba, and CONICET, Argentina), Dilian Gurov (KTH, Sweden), Sebastián Uchitel (Imperial College London, UK, and Universidad de Buenos Aires, Argentina), and Santiago Zanella (IMDEA Software, Spain).

We are grateful to the invited speakers, tutorialists, and lecturers for accepting our invitation to address the conference or lecture at the school.

We also would like to thank the members of the Steering Committee and the Organizing Committee as well as several other people whose efforts contributed to making the conference a success. In particular, we would like to thank Carlos Luna and Luis Sierra (Universidad de la República, Uruguay) for helping with the local organization.

August 2011

Gilles Barthe
Alberto Pardo
Gerardo Schneider

Conference Organization

Conference Committees

Conference Chair	Alberto Pardo, Universidad de la República (Uruguay)
Program Chairs	Gilles Barthe, IMDEA Software Institute (Spain) Gerardo Schneider, Chalmers University of Gothenburg (Sweden), and University of Oslo (Norway)
Local Organization	Carlos Luna, Universidad de la República (Uruguay) Alberto Pardo, Universidad de la República (Uruguay) Luis Sierra, Universidad de la República (Uruguay)
Special Track Chair	Antonio Cerone, UNU-IIST (China)

Steering Committee

Manfred Broy	TU Munich (Germany)
Antonio Cerone	UNU-IIST (China)
Mike Hinchey	LERO (Ireland)
Mathai Joseph	TRDDC (India)
Zhiming Liu	UNU-IIST (China)
Andrea Maggiolo-Schettini	University of Pisa (Italy)

Program Committee

Bernhard K. Aichernig	TU Graz
Luis Barbosa	Universidade do Minho
Gilles Barthe	IMDEA Software Institute
Thomas Anung Basuki	Parahyangan Catholic University
Alexandre Bergel	University of Chile
Gustavo Betarte	Universidad de la República
Ana Cavalcanti	University of York
Pedro R. D'Argenio	Universidad Nacional de Córdoba - CONICET
Van Hung Dang	Vietnam National University
George Eleftherakis	University of Sheffield
José Luiz Fiadeiro	University of Leicester

Martin Fränze	Carl von Ossietzky Universität Oldenburg
Stefania Gnesi	ISTI-CNR
Rob Hierons	Brunel University
Paola Inverardi	Università dell'Aquila
Jean-Marie Jacquet	University of Namur
Tomasz Janowski	UNU-IIST
Jean-Marc Jezequel	University of Rennes 1 and INRIA
Joseph Kiniry	IT University of Copenhagen
Paddy Krishnan	Bond University
Martin Leucker	University of Lübeck
Xuandong Li	Nanjing University
Peter Lindsay	The University of Queensland
Antónia Lopes	University of Lisbon
Nenad Medvidovic	University of Southern California
Mercedes G. Merayo	Universidad Complutense de Madrid
Stephan Merz	INRIA Nancy
Madhavan Mukund	Chennai Mathematical Institute
Martin Musicante	Universidade Federal do Rio Grande do Norte
César Muñoz	NASA
Mizuhito Ogawa	Japan Advanced Institute of Science and Technology
Olaf Owe	University of Oslo
Gordon Pace	University of Malta
Ernesto Pimentel	University of Malaga
Sanjiva Prasad	Indian Institute of Technology Delhi
Anders Ravn	Aalborg University
Leila Ribeiro	Universidade Federal do Rio Grande do Sul
Augusto Sampaio	Universidade Federal de Pernambuco
Gerardo Schneider	Chalmers University of Gothenburg, and University of Oslo
Sebastian Uchitel	Imperial College London and Universidad de Buenos Aires
Willem Visser	Stellenbosch University
Sergio Yovine	CONICET - Universidad de Buenos Aires

Special Track Program Committee

Roberto Barbuti	University of Pisa (Italy)
Antonio Cerone	UNU-IIST (China)
Elsa Estevez	UNU-IIST (China)
Peter Haddawy	UNU-IIST (China)
Siu-Wai Leung	University of Macau (China)
Dora Marinova	Curtin University (Australia)
Paolo Milazzo	University of Pisa (Italy)
Ion Petre	Åbo Akademi University (Finland)

Weishuang Qu	Millennium Institute (USA)
Dave Robertson	University of Edinburgh (UK)
Siraj Shaikh	Coventry University (UK)
Michael Sonnenschein	University of Oldenburg (Germany)
Hefeng Tong	Institute of Scientific and Technical Information of China (China)
Jianhong Wu	York University (Canada)
Shaofa Yang	Chinese Academy of Sciences, SIAT (China)

Additional Reviewers

Abraham, Erika	Almeida, José Bacelar	Asirelli, Patrizia
Baliosian, Javier	Baltazar, Pedro	Bocchi, Laura
Boronat, Artur	Brandán Briones, Laura	Bu, Lei
Buntrock, Gerhard	Bøgholm, Thomas	Cadavid Gómez, Juan-José
Cajueiro, Adalberto	Calegari, Daniel	Castro, Pablo
Costa, Umberto	Crole, Roy	Cubo, Javier
Dang Duc, Hanh	Decker, Normann	Demange, Delphine
Dolques, Xavier	Fantechi, Alessandro	Filliâtre, Jean-Christophe
Fontaine, Pascal	Forejt, Vojtech	Francalanza, Adrian
Giménez, Eduardo	Goodloe, Alwyn	Hagen, George
Hauptmann, Benedikt	Hungar, Hardi	Iyoda, Juliano
Jöbstl, Elisabeth	Kromodimoeljo, Sentot	Kunz, César
Lal, Akash	Legay, Axel	Li, Xin
Martins Moreira, Anamaria	Martins, Francisco	Massoni, Tiago
Mehta, Farhad	Mori, Marco	Nakajima, Shin
Narkawicz, Anthony	Nguyen, Tang	Nowotka, Dirk
Ogata, Kazuhiro	Okikka, Joseph	Owens, Scott
Pelozo, Silvia	Pham Ngoc, Hung	Prisacariu, Cristian
Ramalingam, Ganesan	Ramanujam, R.	Rinetzky, Noam
Rodrigues, Nuno	Rosa, Cristián	Rossi, Matteo
Sannier, Nicolas	Schapachnik, Fernando	Schlatte, Rudolf
Seki, Hiroyuki	Shankar, Natarajan	Siminiceanu, Radu
Smith, Graeme	Spalazzese, Romina	Srba, Jiri
Sternagel, Christian	Stocks, Phil	Stümpel, Annette
Swaminathan, Mani	Teige, Tino	Thoma, Daniel
Thuong Tran, Thi Mai	Vallespir, Diego	Vicario, Enrico
Vighio, Saleem	Vorobyov, Kostyantyn	Wang, Linzhang
Winter, Kirsten	Zhao, Jianhua	

Sponsors

- ANII (Agencia Nacional de Investigación e Innovación, Uruguay)
- CSIC (Comisión Sectorial de Investigación Científica, Universidad de la República, Uruguay)
- PEDECIBA Informática (Programa de Desarrollo de las Ciencias Básicas, Uruguay)

Table of Contents

Keynote Talks

Formal Methods in Energy Informatics	1
<i>Holger Hermanns</i>	
Formal Methods as a Link between Software Code and Legal Rules	3
<i>Daniel Le Métayer</i>	
Developing Model-Checking Mechanisms for ASSL: An Experience Report	19
<i>Emil Vassev and Mike Hinchey</i>	
Models and Communication in the Policy Process	35
<i>Matteo Pedercini</i>	

Regular Papers

Distributed Implementation of Systems with Multiparty Interactions and Priorities	38
<i>Imene Ben-Hafaiedh, Susanne Graf, and Nejla Mazouz</i>	
Verification of PLC Properties Based on Formal Semantics in Coq	58
<i>Jan Olaf Blech and Sidi Ould Biha</i>	
Broadcast Psi-calculi with an Application to Wireless Protocols	74
<i>Johannes Borgström, Shuqin Huang, Magnus Johansson, Palle Raabjerg, Björn Victor, Johannes Åman Pohjola, and Joachim Parrow</i>	
A Formalisation of Java Strings for Program Specification and Verification	90
<i>Richard Bubel, Reiner Hähnle, and Ulrich Geilmann</i>	
dCTL: A Branching Time Temporal Logic for Fault-Tolerant System Verification	106
<i>Pablo F. Castro, Cecilia Kilmurray, Araceli Acosta, and Nazareno Aguirre</i>	
A Machine-Checked Framework for Relational Separation Logic	122
<i>Juan Manuel Crespo and César Kunz</i>	
A Dataflow Analysis to Improve SAT-Based Bounded Program Verification	138
<i>Bruno Cuervo Parrino, Juan Pablo Galeotti, Diego Garbervetsky, and Marcelo F. Frias</i>	

Reverse Hoare Logic	155
<i>Edsko de Vries and Vasileios Koutavas</i>	
Improving SAT Modulo ODE for Hybrid Systems Analysis by Combining Different Enclosure Methods	172
<i>Andreas Eggers, Nacim Ramdani, Nediaiko Nediaikov, and Martin Fränzle</i>	
Verification of B^+ Trees: An Experiment Combining Shape Analysis and Interactive Theorem Proving	188
<i>Gidon Ernst, Gerhard Schellhorn, and Wolfgang Reif</i>	
Runtime Verification of Component-Based Systems	204
<i>Yliès Falcone, Mohamad Jaber, Thanh-Hung Nguyen, Marius Bozga, and Saddek Bensalem</i>	
Translating Alloy Specifications to UML Class Diagrams Annotated with OCL	221
<i>Ana Garis, Alcino Cunha, and Daniel Riesco</i>	
Safe Distribution of Declarative Processes	237
<i>Thomas Hildebrandt, Raghava Rao Mukkamala, and Tijis Slaats</i>	
Verifying B Proof Rules Using Deep Embedding and Automated Theorem Proving	253
<i>Mélanie Jacquél, Karim Berkani, David Delahaye, and Catherine Dubois</i>	
Hybrid Specification of Reactive Systems: An Institutional Approach . . .	269
<i>Alexandre Madeira, José M. Faria, Manuel A. Martins, and Luís S. Barbosa</i>	
Leveraging State-Based User Preferences in Context-Aware Reconfigurations for Self-Adaptive Systems	286
<i>Marco Mori, Fei Li, Christoph Dorn, Paola Inverardi, and Schahram Dustdar</i>	
Context-Bounded Model Checking of LTL Properties for ANSI-C Software	302
<i>Jeremy Morse, Lucas Cordeiro, Denis Nicole, and Bernd Fischer</i>	
Modular Modelling of Software Product Lines with Feature Nets	318
<i>Radu Muschevici, José Proença, and Dave Clarke</i>	

Synchronizing Asynchronous Conformance Testing	334
<i>Neda Noroozi, Ramtin Khosravi, Mohammad Reza Mousavi, and Tim A.C. Willemse</i>	
Using Coq in Specification and Program Extraction of Hadoop MapReduce Applications	350
<i>Kosuke Ono, Yoichi Hirai, Yoshinori Tanabe, Natsuko Noda, and Masami Hagiya</i>	
ProMoVer: Modular Verification of Temporal Safety Properties	366
<i>Siavash Soleimanifard, Dilian Gurov, and Marieke Huisman</i>	
Usable Verification of Object-Oriented Programs by Combining Static and Dynamic Techniques	382
<i>Julian Tschannen, Carlo A. Furia, Martin Nordio, and Bertrand Meyer</i>	
Short Papers	
Efficient Computation of Dominance in Component Systems (Short Paper)	399
<i>Jaap Boender</i>	
Tool Papers	
The Boogie Verification Debugger (Tool Paper)	407
<i>Claire Le Goues, K. Rustan M. Leino, and Michał Moskal</i>	
Object-Oriented Formal Modeling and Analysis of Interacting Hybrid Systems in HI-Maude	415
<i>Muhammad Fadlisyah, Peter Csaba Ölveczky, and Erika Ábrahám</i>	
Special Track: “Modelling for Sustainable Development”	
Towards an Agent-Based Methodology for Developing Agro-Ecosystem Simulations	431
<i>Jorge Corral and Daniel Calegari</i>	
Development Policy Analysis in Mali: Sustainable Growth Prospects . . .	447
<i>Matteo Pedercini</i>	
Using System Dynamics to Assess the Role of Socio-economic Status in Tuberculosis Incidence	464
<i>Marisa Analía Sánchez</i>	

Energy Consumption and CO ₂ Emissions of Beijing Heating System: Based on a System Dynamics Model	476
<i>Hefeng Tong and Weishuang Qu</i>	
A Formal Approach to Analysing Knowledge Transfer Processes in Developing Countries	486
<i>Jin Tong, Siraj A. Shaikh, and Anne E. James</i>	
Author Index	503