

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

Dominique Méry Stephan Merz (Eds.)

Integrated Formal Methods

8th International Conference, IFM 2010
Nancy, France, October 11-14, 2010
Proceedings

Volume Editors

Dominique Méry

Stephan Merz

INRIA Nancy-Grand Est & LORIA, Bâtiment B, équipe MOSEL

615 rue du Jardin Botanique, 54602 Villers-lès-Nancy cédex, France

E-mail: {Dominique.Mery; Stephan.Merz@loria.fr}

Library of Congress Control Number: 2010935597

CR Subject Classification (1998): D.2, F.3, D.3, D.2.4, F.4.1, D.1

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743

ISBN-10 3-642-16264-9 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-16264-0 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 2010

Printed in Germany

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

Printed on acid-free paper 06/3180

Preface

This volume contains the proceedings of IFM 2010, the 8th International Conference on Integrated Formal Methods. The conference took place October 12–14, 2010, at the INRIA research center and the LORIA laboratory in Nancy, France. Previous editions were held in York, Dagstuhl, Turku, Canterbury, Eindhoven, Oxford, and Düsseldorf. The IFM conference series seeks to promote research into the combination of different formal methods, including the combination of formal with semiformal methods, for system development. Such combinations are useful in order to apprehend different aspects of systems, including functional correctness, security, performance, and fault-tolerance. The conference provides a forum for discussing recent advances in the state of the art and for disseminating the results among the academic and industrial community.

IFM 2010 received 59 submissions, covering the spectrum of integrated formal methods and ranging from formal and semiformal notations, semantics, refinement, verification, and model transformations to type systems, logics, tools, and case studies. Each submission was reviewed by at least three members of the Program Committee. The committee decided to accept 20 papers. The conference program also included invited talks by Christel Baier, John Fitzgerald, and Rajeev Joshi. The conference was preceded by a day dedicated to the Workshop on Formal Methods for Web Data Trust and Security (WTS 2010) and two tutorials, one on the verification of C# programs using Spec# and Boogie 2, by Rosemary Monahan, and the other on the TLA⁺ proof system, by Denis Cousineau and Stephan Merz.

We are grateful to the members of the Program Committee and the external reviewers for their care and diligence. The reviewing process and the preparation of the proceedings were facilitated by the EasyChair system that we highly recommend to every program chair. We thank the INRIA Nancy research center for organizational and logistic support, and gratefully acknowledge the financial support by CNRS (through GDR GPL), Nancy University, GIS 3SGS, the Lorraine Region, and the Greater Nancy.

October 2010

Dominique Méry
Stephan Merz

Conference Organization

Program Chairs

Dominique Méry	University of Nancy, France
Stephan Merz	INRIA Nancy, France

Program Committee

Yamine Aït-Ameur	ENSMA Poitiers, France
Jean-Paul Bodeveix	University of Toulouse, France
Bernard Boigelot	University of Liège, Belgium
Eerke Boiten	University of Kent, UK
Jim Davies	University of Oxford, UK
David Déharbe	UFRN Natal, Brazil
John Derrick	University of Sheffield, UK
Jin Song Dong	University of Singapore, Singapore
Wan Fokkink	Free University of Amsterdam, The Netherlands
Martin Fränzle	University of Oldenburg, Germany
Andy Galloway	University of York, UK
Hubert Garavel	INRIA Grenoble, France
Diego Latella	CNR Pisa, Italy
Stefan Leue	University of Konstanz, Germany
Michael Leuschel	University of Düsseldorf, Germany
Heiko Mantel	Technical University of Darmstadt, Germany
Jun Pang	University of Luxemburg, Luxemburg
David Pichardie	INRIA Rennes, France
Wolfram Schulte	Microsoft Research, USA
Graeme Smith	University of Queensland, Australia
Martin Steffen	University of Oslo, Norway
Kenji Taguchi	NII Tokyo, Japan
Helen Treharne	University of Surrey, UK
Elena Troubitsyna	Åbo Akademi, Finland
Heike Wehrheim	University of Paderborn, Germany

Local Organization

Nicolas Alcaraz
Anne-Lise Charbonnier
Rachida Kasmi
Dominique Méry
Stephan Merz

External Reviewers

Erika Abraham	Mohammad M. Jaghoori	Neeraj Singh
Markus Aderhold	Suresh Jagannathan	Heiko Spiess
Maurice H. ter Beek	Michael Jastram	Barbara Sprick
Nazim Benaïssa	Matthias Kuntz	Dominik Steenken
Yves Bertot	Hironobu Kuruma	Volker Stolz
Sandrine Blazy	Peter Ladkin	Martin Strecker
Andrea Bracciali	Linas Laibinis	Henning Sudbrock
Erik Burger	Florian Leitner-Fischer	Toshinori Takai
Taolue Chen	Peter Lindsay	Anton Tarasyuk
Véronique Cortier	Yang Liu	Tino Teige
Frédéric Dabrowski	Michele Loreti	Thi Mai Thuong Tran
Mohammad T. Dashti	Alexander Lux	Nils Timm
Henning Dierks	Mieke Massink	Sebastian Uchitel
Xinyu Feng	Alexander Metzner	Chen-wei Wang
Mamoun Filali-Amine	Martin Musicante	James Welch
Pascal Fontaine	Anantha Narayanan	Bernd Westphal
Richard Gay	Khanh Nguyen Truong	Anton Wijs
Stefan Hallerstede	Daniel Plagge	Kirsten Winter
Ian J. Hayes	Jean-Baptiste Raclet	Peng Wu
Keijo Heljanko	Thomas Ruhroth	Shaojie Zhang
Alexei Iliasov	Christoph Scheben	Xian Zhang
Ethan Jackson	Rudi Schlatte	Huiquan Zhu

Sponsoring Institutions

- Centre de Recherche INRIA Nancy-Grand Est
- Nancy Université: Université Henri Poincaré Nancy 1, Institut National Polytechnique de Lorraine
- CNRS: GDR GPL – Génie de la Programmation et du Logiciel
- GIS 3SGS: Surveillance, Sûreté et Sécurité des Grands Systèmes
- Communauté Urbaine du Grand Nancy
- Région Lorraine

Table of Contents

On Model Checking Techniques for Randomized Distributed Systems (Invited Talk)	1
<i>Christel Baier</i>	
Collaborative Modelling and Co-simulation in the Development of Dependable Embedded Systems (Invited Talk)	12
<i>John Fitzgerald, Peter Gorm Larsen, Ken Pierce, Marcel Verhoef, and Sune Wolff</i>	
Programming with Miracles (Invited Talk)	27
<i>Rajeev Joshi</i>	
An Event-B Approach to Data Sharing Agreements	28
<i>Alvaro E. Arenas, Benjamin Aziz, Juan Bicarregui, and Michael D. Wilson</i>	
A Logical Framework to Deal with Variability	43
<i>Patrizia Asirelli, Maurice H. ter Beek, Alessandro Fantechi, and Stefania Gnesi</i>	
Adding Change Impact Analysis to the Formal Verification of C Programs	59
<i>Serge Autexier and Christoph Lüth</i>	
Creating Sequential Programs from Event-B Models	74
<i>Pontus Boström</i>	
Symbolic Model-Checking of Optimistic Replication Algorithms	89
<i>Hanifa Boucheneb, Abdessamad Imine, and Manal Najem</i>	
From Operating-System Correctness to Pervasively Verified Applications	105
<i>Matthias Daum, Norbert W. Schirmer, and Mareike Schmidt</i>	
A Compositional Method for Deciding Equivalence and Termination of Nondeterministic Programs	121
<i>Aleksandar Dimovski</i>	
Verification Architectures: Compositional Reasoning for Real-Time Systems	136
<i>Johannes Faber</i>	

Automatic Verification of Parametric Specifications with Complex Topologies	152
<i>Johannes Faber, Carsten Ihlemann, Swen Jacobs, and Viorica Sofronie-Stokkermans</i>	
Satisfaction Meets Expectations: Computing Expected Values of Probabilistic Hybrid Systems with SMT	168
<i>Martin Fränzle, Tino Teige, and Andreas Eggers</i>	
Showing Full Semantics Preservation in Model Transformation – A Comparison of Techniques	183
<i>Mathias Hülbusch, Barbara König, Arend Rensink, Maria Semenyak, Christian Soltenborn, and Heike Wehrheim</i>	
Specification and Verification of Model Transformations Using UML-RSDS	199
<i>Kevin Lano and Shekoufeh Kolahdouz-Rahimi</i>	
Multiformalism and Transformation Inheritance for Dependability Analysis of Critical Systems	215
<i>Stefano Marrone, Camilla Papa, and Valeria Vittorini</i>	
Translating Pi-Calculus into LOTOS NT	229
<i>Radu Mateescu and Gwen Salaün</i>	
Systematic Translation Rules from ASTD to Event-B	245
<i>Jérémy Milhau, Marc Frappier, Frédéric Gervais, and Régine Laleau</i>	
A CSP Approach to Control in Event-B	260
<i>Steve Schneider, Helen Treharne, and Heike Wehrheim</i>	
Towards Probabilistic Modelling in Event-B	275
<i>Anton Tarasyuk, Elena Troubitsyna, and Linas Laibinis</i>	
Safe Commits for Transactional Featherweight Java	290
<i>Thi Mai Thuong Tran and Martin Steffen</i>	
Certified Absence of Dangling Pointers in a Language with Explicit Deallocation	305
<i>Javier de Dios, Manuel Montenegro, and Ricardo Peña</i>	
Integrating Implicit Induction Proofs into Certified Proof Environments	320
<i>Sorin Stratulat</i>	
Author Index	337