

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7408>

Erika Ábrahám · Marieke Huisman (Eds.)

Integrated Formal Methods

12th International Conference, IFM 2016
Reykjavik, Iceland, June 1–5, 2016
Proceedings

Editors
Erika Ábrahám
RWTH Aachen University
Aachen
Germany

Marieke Huisman
University of Twente
Enschede
The Netherlands

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-33692-3 ISBN 978-3-319-33693-0 (eBook)
DOI 10.1007/978-3-319-33693-0

Library of Congress Control Number: 2016937350

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer International Publishing Switzerland 2016

Open Access Chapters 5, 16 and 23 are distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>). For further details see license information in the chapters.

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, 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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Preface

Applying formal methods may involve the usage of different formalisms and different analysis techniques to validate a system, either because individual components are most amenable to one formalism or technique, because one is interested in different properties of the system, or simply to cope with the sheer complexity of the system. The iFM conference series seeks to further research into hybrid approaches to formal modeling and analysis; i.e., the combination of (formal and semi-formal) methods for system development, regarding both modeling and analysis. The conference covers all aspects from language design through verification and analysis techniques to tools and their integration into software engineering practice.

These proceedings document the outcome of the 12th International Conference on Integrated Formal Methods, iFM 2016, on recent developments toward this goal. The conference was held in Reykjavik, Iceland, during June 1–5, 2016, hosted by Reykjavik University. Previous editions of iFM were held in York, UK (1999), Schloss Dagstuhl, Germany (2000), Turku, Finland (2002), Kent, UK (2004), Eindhoven, The Netherlands (2005), Oxford, UK (2007), Düsseldorf, Germany (2009), Nancy, France (2010), Pisa, Italy (2012), Turku, Finland (2013), and Bertinoro, Italy (2014).

The conference received 99 submissions of authors from 34 countries. Papers were submitted in four categories: research papers, regular tool papers, short tool papers, and case study papers. All papers were reviewed by at least three members of the Program Committee. After careful deliberations, the Program Committee selected 30 papers for presentation.

In addition to these papers, this volume contains contributions of three invited keynote speakers: Reiner Hähnle, TU Darmstadt, Germany; Laura Kovács, Chalmers University of Technology, Sweden, and TU Wien, Austria; and Marsha Chechik, University of Toronto, Canada:

- Martin Hentschel, Reiner Hähnle, and Richard Bubel: “Can Formal Methods Improve the Efficiency of Code Reviews?”
- Laura Kovács: “Symbolic Computation and Automated Reasoning for Program Analysis”
- Marsha Chechik, Michalis Famelis, and Rick Salay: “Perspectives of Model Transformation Reuse”

Invited presentations are always the highlights of a conference; these contributions are therefore gratefully acknowledged.

iFM was accompanied by the following satellite events, managed by the workshop chairs, Marcel Kyas, University of Reykjavik, Iceland, and Wojciech Mostowski, Halmstad University, Sweden:

- The 6th International Symposium on Unifying Theories of Programming (UTP 2016)
- Workshop on Pre- and Post-Deployment Verification Techniques (PrePost)

- Workshop on Formal Methods for and on the Cloud (iFMCloud 2016)
- Workshop on Verification and Validation of Cyber-Physical Systems (V2CPS)
- PhD Symposium at iFM 2016 on Formal Methods: Algorithms, Tools and Applications (PhD-iFM 2016)

The conference would not have been possible without the enthusiasm and dedication of the iFM general chair, Marjan Sirjani, and the support of the School of Computer Science at Reykjavik University, Iceland. For the work of the Program Committee and the compilation of the proceedings, Andrei Voronkov's EasyChair system was employed; it freed us from many technical matters and allowed us to focus on the program, for which we are grateful. Conferences like iFM rely on the willingness of experts to serve on the Program Committee; their professionalism and their helpfulness were exemplary. Finally, we would like to thank all the authors for their submissions, their willingness to continue improving their papers, and their presentations!

March 2016

Erika Ábrahám
Marieke Huisman

Organization

Program Chairs

Erika Ábrahám	RWTH Aachen University, Germany
Marieke Huisman	University of Twente, The Netherlands

Steering Committee

Erika Ábrahám	RWTH Aachen University, Germany
Elvira Albert	Complutense University of Madrid, Spain
John Derrick	University of Sheffield, UK
Marieke Huisman	University of Twente, The Netherlands
Einar Broch Johnsen	University of Oslo, Norway
Dominique Méry	Université de Lorraine, France
Luigia Petre	Åbo Akademi University, Finland
Steve Schneider	University of Surrey, UK
Emil Sekerinski	McMaster University, Canada
Marjan Sirjani	University of Reykjavik, Iceland
Helen Treharne	University of Surrey, UK
Heike Wehrheim	University of Paderborn, Germany

Organizing Committee

Marjan Sirjani	University of Reykjavik, Iceland
Marcel Kyas	University of Reykjavik, Iceland
Wojciech Mostowski	Halmstad University, Sweden

Program Committee

Wolfgang Ahrendt	Chalmers University of Technology, Sweden
Elvira Albert	Complutense University of Madrid, Spain
Bernd Becker	Albert-Ludwigs-Universität Freiburg, Germany
Clara Benac Earle	Universidad Politecnica de Madrid, Spain
Borzoo Bonakdarpour	McMaster University, Canada
Ferruccio Damiani	Università di Torino, Italy
Frank de Boer	CWI, The Netherlands
Delphine Demange	University of Rennes 1/IRISA, France
Jan Friso Groote	Eindhoven University of Technology, The Netherlands
Dilian Gurov	KTH Royal Institute of Technology, Sweden
Holger Hermanns	Saarland University, Germany
Einar Broch Johnsen	University of Oslo, Norway

Peter Gorm Larsen	Aarhus University, Denmark
Martin Leucker	University of Lübeck, Germany
Dominique Méry	Université de Lorraine, LORIA, France
Rosemary Monahan	National University of Ireland Maynooth, Ireland
Nadia Polikarpova	MIT, USA
Cesar Sanchez	IMDEA Software Institute, Spain
Sriram Sankaranarayanan	University of Colorado, Boulder, USA
Ina Schaefer	Technische Universität Braunschweig, Germany
Gerardo Schneider	University of Gothenburg, Sweden
Emil Sekerinski	McMaster University, Canada
Armando Tacchella	Università di Genova, Italy
Mark Utting	University of the Sunshine Coast, Australia
Heike Wehrheim	University of Paderborn, Germany
Kirsten Winter	University of Queensland, Australia

Additional Reviewers

Alborodo, Raul Nestor Neri	Dezani-Ciancaglini, Mariangiola
Aliakbary, Sadegh	Din, Crystal Chang
Antignac, Thibaud	Doménech, Jesus
Arenas, Puri	Díaz, Gregorio
Avanzini, Martin	Faghih, Fathiyeh
Balliu, Musard	Filali-Amine, Mamoun
Bartocci, Ezio	Flores Montoya, Antonio E.
Baumann, Christoph	Fontaine, Pascal
Berardi, Stefano	Fredlund, Lars-Ake
Berger, Christian	Furia, Carlo A.
Besson, Frédéric	Ganty, Pierre
Bijo, Shiji	Garavel, Hubert
Bodeveix, Jean-Paul	Giachino, Elena
Bubel, Richard	Gomez-Zamalloa, Miguel
Burchard, Jan	Gordillo, Pablo
Burton, Eden	Guanciale, Roberto
Cardone, Felice	Gómez-Martínez, Elena
Cheng, Zheng	Hallerstede, Stefan
Chimento, Jesus Mauricio	Harder, Jannis
Coppo, Mario	Heckl, Istvan
Cordy, Maxime	Isabel, Miguel
Correas Fernández, Jesús	Isenberg, Tobias
De Carvalho Gomes, Pedro	Itzhaky, Shachar
De Frutos Escrig, David	Jacobs, Bart
De Gouw, Stijn	Jakobs, Marie-Christine
De Vink, Erik	Jensen, Thomas
Decker, Normann	Keshishzadeh, Sarmen

Kromodimoeljo, Sentot
Krämer, Julia Désirée
Kuraj, Ivan
Lachmann, Remo
Lago, Patricia
Lhotak, Ondrej
Liang, Hongjin
Lienhardt, Michael
Lity, Sascha
Liu, Tianhai
Lucanu, Dorel
Luttik, Bas
Löding, Christof
Malavolta, Ivano
Mariño, Julio
Markin, Grigory
Martin-Martin, Enrique
Mauro, Jacopo
Medhat, Ramy
Meijer, Jeroen
Mennicke, Stephan
Merz, Stephan
Milicevic, Aleksandar
Mogren, Olof
Nanevski, Aleksandar
Neubauer, Felix
Nicolaou, Nicolas
Oortwijn, Wytse
Owe, Olaf
Palmskog, Karl
Paolini, Luca
Petri, Gustavo
Power, James
Pozzato, Gian Luca
Pun, Ka I
Quilbeuf, Jean
Rafnsson, Willard
Reimer, Sven
Rezine, Ahmed
Robillard, Simon
Román-Díez, Guillermo
Sanchez, Alejandro
Sauer, Matthias
Scheffel, Torben
Scheibler, Karsten

Schewe, Sven
Schlatte, Rudolf
Schmaltz, Julien
Schmitz, Malte
Schwarz, Oliver
Scozzari, Francesca
Serbanescu, Vlad Nicolae
Siddique, Umair
Singh, Neeraj
Smith, Graeme
Sproston, Jeremy
Steffen, Martin
Stoller, Scott
Stolz, Volker
Stümpel, Annette
Summers, Alexander J.
Swartjes, Lennart
Talebi, Mahmoud
Tamarit, Salvador
Tapia Tarifa, Silvia Lizeth
Testerink, Bas
Thoma, Daniel
Thorn, Johannes
Thüm, Thomas
Toews, Manuel
Tran-Jørgensen, Peter
Travkin, Oleg
Trivedi, Ashutosh
Ulbrich, Mattias
Walther, Sven
Wasowski, Andrzej
Weng, Min-Hsien
Westman, Jonas
Wille, David
Willemse, Tim
Wimmer, Ralf
Winterer, Leonore
Wong, Peter
Wouda, Sanne
Yang, Fei
Zalinescu, Eugen
Zantema, Hans
Zavattaro, Gianluigi
Zutshi, Aditya

Contents

Invited Contributions

Can Formal Methods Improve the Efficiency of Code Reviews?	3
<i>Martin Hentschel, Reiner Hähnle, and Richard Bubel</i>	
Symbolic Computation and Automated Reasoning for Program Analysis	20
<i>Laura Kovács</i>	
Perspectives of Model Transformation Reuse	28
<i>Marsha Chechik, Michalis Famelis, Rick Salay, and Daniel Strüßer</i>	

Program Verification

On Type Checking Delta-Oriented Product Lines	47
<i>Ferruccio Damiani and Michael Lienhardt</i>	
Modelling and Verifying a Priority Scheduler for an SCJ Runtime Environment.	63
<i>Leo Freitas, James Baxter, Ana Cavalcanti, and Andy Wellings</i>	
Why Just Boogie?: Translating Between Intermediate Verification Languages	79
<i>Michael Ameri and Carlo A. Furia</i>	

Probabilistic Systems

Statistical Approximation of Optimal Schedulers for Probabilistic Timed Automata	99
<i>Pedro R. D'Argenio, Arnd Hartmanns, Axel Legay, and Sean Sedwards</i>	
Probabilistic Formal Analysis of App Usage to Inform Redesign.	115
<i>Oana Andrei, Muffy Calder, Matthew Chalmers, Alistair Morrison, and Mattias Rost</i>	
Extension of PRISM by Synthesis of Optimal Timeouts in Fixed-Delay CTMC.	130
<i>Luboš Korenčíak, Vojtěch Řehák, and Adrian Farmadin</i>	

Concurrency

Monitoring Multi-threaded Component-Based Systems	141
<i>Hosein Nazarpour, Yliès Falcone, Saddek Bensalem, Marius Bozga, and Jacques Combaz</i>	
A Generalised Theory of Interface Automata, Component Compatibility and Error	160
<i>Sascha Fendrich and Gerald Lüttgen</i>	
On Implementing a Monitor-Oriented Programming Framework for Actor Systems	176
<i>Ian Cassar and Adrian Francalanza</i>	
Towards a Thread-Local Proof Technique for Starvation Freedom.	193
<i>Gerhard Schellhorn, Oleg Travkin, and Heike Wehrheim</i>	
Reasoning About Inheritance and Unrestricted Reuse in Object-Oriented Concurrent Systems.	210
<i>Olaf Owe</i>	
A Formal Model of the Safety-Critical Java Level 2 Paradigm	226
<i>Matt Luckcuck, Ana Cavalcanti, and Andy Wellings</i>	

Safety and Liveness

Deciding Monadic Second Order Logic over ω -Words by Specialized Finite Automata	245
<i>Stephan Barth</i>	
Property Preservation for Extension Patterns of State Transition Diagrams . . .	260
<i>Christian Prehofer</i>	
Symbolic Reachability Analysis of B Through ProB and LTSmin	275
<i>Jens Bendisposto, Philipp Körner, Michael Leuschel, Jeroen Meijer, Jaco van de Pol, Helen Treharne, and Jorden Whitefield</i>	

Model Learning

Enhancing Automata Learning by Log-Based Metrics	295
<i>Petra van den Bos, Rick Smetsers, and Frits Vaandrager</i>	
Refactoring of Legacy Software Using Model Learning and Equivalence Checking: An Industrial Experience Report	311
<i>Mathijs Schuts, Jozef Hooman, and Frits Vaandrager</i>	

On Robust Malware Classifiers by Verifying Unwanted Behaviours	326
<i>Wei Chen, David Aspinall, Andrew D. Gordon, Charles Sutton, and Igor Muttik</i>	

SAT and SMT Solving

Efficient Deadlock-Freedom Checking Using Local Analysis and SAT Solving	345
<i>Pedro Antonino, Thomas Gibson-Robinson, and A.W. Roscoe</i>	
SMT Solvers for Validation of B and Event-B Models	361
<i>Sebastian Krings and Michael Leuschel</i>	
Avoiding Medication Conflicts for Patients with Multimorbidities	376
<i>Andrii Kovalov and Juliana Küster Filipe Bowles</i>	

Testing

Temporal Random Testing for Spark Streaming	393
<i>Adrián Riesco and Juan Rodríguez-Hortala</i>	
Combining Static Analysis and Testing for Deadlock Detection	409
<i>Elvira Albert, Miguel Gómez-Zamalloa, and Miguel Isabel</i>	
Fuzzing JavaScript Engine APIs	425
<i>Renáta Hodován and Ákos Kiss</i>	

Theorem Proving and Constraint Satisfaction

A Component-Based Approach to Hybrid Systems Safety Verification.	441
<i>Andreas Müller, Stefan Mitsch, Werner Retschitzegger, Wieland Schwinger, and André Platzer</i>	
Verifying Pointer Programs Using Separation Logic and Invariant Based Programming in Isabelle	457
<i>Viorel Preoteasa</i>	
A Constraint Satisfaction Method for Configuring Non-local Service Interfaces	474
<i>Pavel Zaichenkov, Olga Tveretina, and Alex Shafarenko</i>	

Case Studies

Rule-Based Consistency Checking of Railway Infrastructure Designs.	491
<i>Bjørnar Luteberget, Christian Johansen, and Martin Steffen</i>	

Formal Verification of Safety PLC Based Control Software 508
Dániel Darvas, István Majzik, and Enrique Blanco Viñuela

CloudSDV Enabling Static Driver Verifier Using Microsoft Azure 523
*Rahul Kumar, Thomas Ball, Jakob Lichtenberg, Nate Deisinger,
Apoorv Upreti, and Chetan Bansal*

Author Index 537