More information about this series at http://www.springer.com/series/7408
Integrated Formal Methods

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

Springer
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:

– 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
VIII Organization

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 Faghii, 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
Bubli, 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
## Contents

### Invited Contributions

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

### Program Verification

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

### Probabilistic Systems

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

Monitoring Multi-threaded Component-Based Systems .................................. 141  
Hosein Nazarpour, Yliès Falcone, Saddek Bensalem, Marius Bozga,  
and Jacques Combaz

A Generalised Theory of Interface Automata, Component Compatibility  
and Error .................................................. 160  
Sascha Fendrich and Gerald Lüttgen

On Implementing a Monitor-Oriented Programming Framework for Actor  
Systems .................................................................... 176  
Ian Cassar and Adrian Francalanza

Towards a Thread-Local Proof Technique for Starvation Freedom ........... 193  
Gerhard Schellhorn, Oleg Travkin, and Heike Wehrheim

Reasoning About Inheritance and Unrestricted Reuse in Object-Oriented  
Concurrent Systems .................................................. 210  
Olaf Owe

A Formal Model of the Safety-Critical Java Level 2 Paradigm ................. 226  
Matt Luckcuck, Ana Cavalcanti, and Andy Wellings

## Safety and Liveness

Deciding Monadic Second Order Logic over $\omega$-Words by Specialized  
Finite Automata .................................................... 245  
Stephan Barth

Property Preservation for Extension Patterns of State Transition Diagrams ... 260  
Christian Prehofer

Symbolic Reachability Analysis of B Through ProB and LTSMin .......... 275  
Jens Bendisposto, Philipp Körner, Michael Leuschel, Jeroen Meijer,  
Jaco van de Pol, Helen Treharne, and Jorden Whitefield

## Model Learning

Enhancing Automata Learning by Log-Based Metrics .............................. 295  
Petra van den Bos, Rick Smetsers, and Frits Vaandrager

Refactoring of Legacy Software Using Model Learning and Equivalence  
Checking: An Industrial Experience Report ........................................ 311  
Mathijs Schuts, Jozef Hooman, and Frits Vaandrager
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>On Robust Malware Classifiers by Verifying Unwanted Behaviours</td>
<td>326</td>
</tr>
<tr>
<td>Wei Chen, David Aspinall, Andrew D. Gordon, Charles Sutton,</td>
<td></td>
</tr>
<tr>
<td>and Igor Muttik</td>
<td></td>
</tr>
<tr>
<td><strong>SAT and SMT Solving</strong></td>
<td></td>
</tr>
<tr>
<td>Efficient Deadlock-Freedom Checking Using Local Analysis and SAT</td>
<td>345</td>
</tr>
<tr>
<td>Pedro Antonino, Thomas Gibson-Robinson, and A.W. Roscoe</td>
<td></td>
</tr>
<tr>
<td>SMT Solvers for Validation of B and Event-B Models</td>
<td>361</td>
</tr>
<tr>
<td>Sebastian Krings and Michael Leuschel</td>
<td></td>
</tr>
<tr>
<td>Avoiding Medication Conflicts for Patients with Multimorbidities</td>
<td>376</td>
</tr>
<tr>
<td>Andrii Kovalov and Juliana Küster Filipe Bowles</td>
<td></td>
</tr>
<tr>
<td><strong>Testing</strong></td>
<td></td>
</tr>
<tr>
<td>Temporal Random Testing for Spark Streaming</td>
<td>393</td>
</tr>
<tr>
<td>Adrián Riesco and Juan Rodríguez-Hortalá</td>
<td></td>
</tr>
<tr>
<td>Combining Static Analysis and Testing for Deadlock Detection</td>
<td>409</td>
</tr>
<tr>
<td>Elvira Albert, Miguel Gómez-Zamalloa, and Miguel Isabel</td>
<td></td>
</tr>
<tr>
<td>Fuzzing JavaScript Engine APIs</td>
<td>425</td>
</tr>
<tr>
<td>Renáta Hodován and Ákos Kiss</td>
<td></td>
</tr>
<tr>
<td><strong>Theorem Proving and Constraint Satisfaction</strong></td>
<td></td>
</tr>
<tr>
<td>A Component-Based Approach to Hybrid Systems Safety Verification</td>
<td>441</td>
</tr>
<tr>
<td>Andreas Müller, Stefan Mitsch, Werner Retschitzegger, Wieland Schwing, and André Platzer</td>
<td></td>
</tr>
<tr>
<td>Verifying Pointer Programs Using Separation Logic and Invariant Based Programming in Isabelle</td>
<td>457</td>
</tr>
<tr>
<td>Viorel Preoteasa</td>
<td></td>
</tr>
<tr>
<td>A Constraint Satisfaction Method for Configuring Non-local Service Interfaces</td>
<td>474</td>
</tr>
<tr>
<td>Pavel Zaichenkov, Olga Tveretina, and Alex Shafarenko</td>
<td></td>
</tr>
<tr>
<td><strong>Case Studies</strong></td>
<td></td>
</tr>
<tr>
<td>Rule-Based Consistency Checking of Railway Infrastructure Designs</td>
<td>491</td>
</tr>
<tr>
<td>Bjørnar Luteberget, Christian Johansen, and Martin Steffen</td>
<td></td>
</tr>
</tbody>
</table>