Contents

Invited Presentations

Resource Analysis: From Sequential to Concurrent and Distributed Programs .................................................... 3

dElvira Albert, Puri Arenas, Jesús Correas, Samir Genaim, Miguel Gómez-Zamalloa, Enrique Martín-Martín, Germán Pueblán Puebla, and Guillermo Román-Díez

AVACS: Automatic Verification and Analysis of Complex Systems Highlights and Lessons Learned ........................................ 18

Werner Damm

Main Track

Automated Circular Assume-Guarantee Reasoning ....................... 23

Karam Abd Elkader, Orna Grumberg, Corina S. Păsăreanu, and Sharon Shoham

Towards Formal Verification of Orchestration Computations Using the \mathcal{K} Framework .................................................... 40

Musab A. AlTurki and Omar Alzuhaibi

Narrowing Operators on Template Abstract Domains .................... 57

Gianluca Amato, Simone Di Nardo Di Maio, Maria Chiara Meo, and Francesca Scozzari

Detection of Design Flaws in the Android Permission Protocol Through Bounded Verification ........................................ 73

Hamid Bagheri, Eunsuk Kang, Sam Malek, and Daniel Jackson

Privacy by Design in Practice: Reasoning about Privacy Properties of Biometric System Architectures ................................. 90

Julien Bringer, Hervé Chabanne, Daniel Le Métayer, and Roch Lescuyer

A Specification Language for Static and Runtime Verification of Data and Control Properties ............................................. 108

Wolfgang Ahrendt, Jesús Mauricio Chimento, Gordon J. Pace, and Gerardo Schneider

Certificates for Parameterized Model Checking ............................ 126

Sylvain Conchon, Alain Mebsout, and Fatiha Zaïdi
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety, Liveness and Run-Time Refinement for Modular Process-Aware</td>
<td>143</td>
</tr>
<tr>
<td>Information Systems with Dynamic Sub Processes</td>
<td></td>
</tr>
<tr>
<td><em>Søren Debois, Thomas Hildebrandt, and Tijs Slaats</em></td>
<td></td>
</tr>
<tr>
<td>Verifying Opacity of a Transactional Mutex Lock</td>
<td>161</td>
</tr>
<tr>
<td><em>John Derrick, Brijesh Dongol, Gerhard Schellhorn, Oleg Travkin,</em></td>
<td></td>
</tr>
<tr>
<td><em>and Heike Wehrheim</em></td>
<td></td>
</tr>
<tr>
<td>A Framework for Correctness Criteria on Weak Memory Models</td>
<td>178</td>
</tr>
<tr>
<td><em>John Derrick and Graeme Smith</em></td>
<td></td>
</tr>
<tr>
<td>Semantics-Preserving Simplification of Real-World Firewall Rule Sets</td>
<td>195</td>
</tr>
<tr>
<td><em>Cornelius Diekmann, Lars Hupel, and Georg Carle</em></td>
<td></td>
</tr>
<tr>
<td>Parameter Synthesis Through Temporal Logic Specifications</td>
<td>213</td>
</tr>
<tr>
<td><em>Thao Dang, Tommaso Dreossi, and Carla Piazza</em></td>
<td></td>
</tr>
<tr>
<td>Trace-Length Independent Runtime Monitoring of Quantitative Policies</td>
<td>231</td>
</tr>
<tr>
<td>in LTL</td>
<td></td>
</tr>
<tr>
<td><em>Xiaoning Du, Yang Liu, and Alwen Tiu</em></td>
<td></td>
</tr>
<tr>
<td>Probabilistic Bisimulation for Realistic Schedulers</td>
<td>248</td>
</tr>
<tr>
<td><em>Christian Eisentraut, Jens Chr. Godskesen, Holger Hermanns,</em></td>
<td></td>
</tr>
<tr>
<td><em>Lei Song, and Lijun Zhang</em></td>
<td></td>
</tr>
<tr>
<td>QPMC: A Model Checker for Quantum Programs and Protocols</td>
<td>265</td>
</tr>
<tr>
<td><em>Yuan Feng, Ernst Moritz Hahn, Andrea Turrini, and Lijun Zhang</em></td>
<td></td>
</tr>
<tr>
<td>Automated Verification of RPC Stub Code</td>
<td>273</td>
</tr>
<tr>
<td><em>Matthew Fernandez, June Andronick, Gerwin Klein, and Ihor Kuz</em></td>
<td></td>
</tr>
<tr>
<td>Property-Driven Fence Insertion Using Reorder Bounded Model Checking</td>
<td>291</td>
</tr>
<tr>
<td><em>Saurabh Joshi and Daniel Kroening</em></td>
<td></td>
</tr>
<tr>
<td>Verifying the Safety of a Flight-Critical System</td>
<td>308</td>
</tr>
<tr>
<td><em>Guillaume Brat, David Bushnell, Misty Davies,</em></td>
<td></td>
</tr>
<tr>
<td><em>Dimitra Giannakopoulou, Falk Howar, and Temesghen Kahsai</em></td>
<td></td>
</tr>
<tr>
<td>Proving Safety with Trace Automata and Bounded Model Checking</td>
<td>325</td>
</tr>
<tr>
<td><em>Daniel Kroening, Matt Lewis, and Georg Weissenbacher</em></td>
<td></td>
</tr>
<tr>
<td>Verifying Parameterized Timed Security Protocols</td>
<td>342</td>
</tr>
<tr>
<td><em>Li Li, Jun Sun, Yang Liu, and Jin Song Dong</em></td>
<td></td>
</tr>
<tr>
<td>Abstraction of Elementary Hybrid Systems by Variable Transformation</td>
<td>360</td>
</tr>
<tr>
<td><em>Jiang Liu, Naijun Zhan, Hengjun Zhao, and Liang Zou</em></td>
<td></td>
</tr>
</tbody>
</table>
Contents XV

Using Real-Time Maude to Model Check Energy Consumption
Shin Nakajima ........................................................ 378

Static Differential Program Analysis for Software-Defined Networks
Tim Nelson, Andrew D. Ferguson, and Shriram Krishnamurthi .... 395

A Fully Verified Container Library
Nadia Polikarpova, Julian Tschannen, and Carlo A. Furia ........ 414

Counterexamples for Expected Rewards
Tim Quatmann, Nils Jansen, Christian Dehnert, Ralf Wimmer,
Erika Ábrahám, Joost-Pieter Katoen, and Bernd Becker ........ 435

The Semantics of Cardinality-Based Feature Models via Formal
Languages
Aliakbar Safilian, Tom Maibaum, and Zinovy Diskin ........... 453

Axiomatization of Typed First-Order Logic
Peter H. Schmitt and Mattias Ulbrich ............................. 470

Model-Based Problem Solving for University Timetable Validation and
Improvement
David Schneider, Michael Leuschel, and Tobias Witt ............. 487

Certified Reasoning with Infinity
Asankhaya Sharma, Shengyi Wang, Andreea Costea, Aquinas Hobor,
and Wei-Ngan Chin .................................................. 496

Direct Formal Verification of Liveness Properties in Continuous and
Hybrid Dynamical Systems
Andrew Sogokon and Paul B. Jackson ............................. 514

Rigorous Estimation of Floating-Point Round-off Errors with Symbolic
Taylor Expansions
Alexey Solovyev, Charles Jacobsen, Zvonimir Rakamarić,
and Ganesh Gopalakrishnan ........................................ 532

Static Optimal Scheduling for Synchronous Data Flow Graphs with
Model Checking
Xue-Yang Zhu, Rongjie Yan, Yu-Lei Gu, Jian Zhang,
Wenhui Zhang, and Guangquan Zhang .............................. 551

Industry Track

Eliminating Static Analysis False Positives Using Loop Abstraction
and Bounded Model Checking
Bharti Chimdyalwar, Priyanka Darke, Anooj Chavda,
Sagar Vaghani, and Avriti Chauhan ............................... 573
XVI Contents

Autofunk: An Inference-Based Formal Model Generation Framework for Production Systems ........................................... 577
   William Durand and Sébastien Salva

Software Development and Authentication for Arms Control Information Barriers ............................................ 581
   Neil Evans

Analyzing the Restart Behavior of Industrial Control Applications ...... 585
   Stefan Hauck-Stattemann, Sebastian Biallas, Bastian Schlich,
   Stefan Kowalewski, and Raoul Jetley

Case Study: Static Security Analysis of the Android Goldfish Kernel ... 589
   Tao Liu and Ralf Huuck

Practices for Formal Models as Documents: Evolution of VDM Application to “Mobile FeliCa” IC Chip Firmware ................. 593
   Taro Kurita, Fuyuki Ishikawa, and Keijiro Araki

Formal Virtual Modelling and Data Verification for Supervision Systems ........................................................ 597
   Thierry Lecomte

Using Simulink Design Verifier for Automatic Generation of Requirements-Based Tests ........................................ 601
   Bruno Miranda, Henrique Masini, and Rodrigo Reis

Formalizing the Concept Phase of Product Development .............. 605
   Mathijs Schuts and Jozef Hooman

Author Index .................................................. 609
FM 2015: Formal Methods
20th International Symposium, Oslo, Norway, June 24-26, 2015, Proceedings
Bjørner, N.; de Boer, F. (Eds.)
2015, XVI, 610 p. 156 illus., Softcover
ISBN: 978-3-319-19248-2