Nikolaj Bjørner · Frank de Boer (Eds.)

FM 2015: Formal Methods

20th International Symposium
Oslo, Norway, June 24–26, 2015
Proceedings

Springer

Contents

Invited Presentations

Resource Analysis: From Sequential to Concurrent and Distributed Programs 3
Elvira Albert, Puri Arenas, Jesús Correas, Samir Genaim, Miguel Gómez-Zamalloa, Enrique Martin-Martin, Germán 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 $\mathbb{K}$ 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

Safety, Liveness and Run-Time Refinement for Modular Process-Aware Information Systems with Dynamic Sub Processes 143
Søren Debois, Thomas Hildebrandt, and Tijs Slaats

Verifying Opacity of a Transactional Mutex Lock 161
John Derrick, Brijesh Dongol, Gerhard Schellhorn, Oleg Travkin, and Heike Wehrheim

A Framework for Correctness Criteria on Weak Memory Models 178
John Derrick and Graeme Smith

Semantics-Preserving Simplification of Real-World Firewall Rule Sets ... 195
Cornelius Diekmann, Lars Hupel, and Georg Carle

Parameter Synthesis Through Temporal Logic Specifications 213
Thao Dang, Tommaso Dreossi, and Carla Piazza

Trace-Length Independent Runtime Monitoring of Quantitative Policies in LTL 231
Xiaoning Du, Yang Liu, and Alwen Tiu

Probabilistic Bisimulation for Realistic Schedulers 248
Christian Eisentraut, Jens Chr. Godskesen, Holger Hermanns, Lei Song, and Lijun Zhang

QPMC: A Model Checker for Quantum Programs and Protocols 265
Yuan Feng, Ernst Moritz Hahn, Andrea Turrini, and Lijun Zhang

Automated Verification of RPC Stub Code 273
Matthew Fernandez, June Andronick, Gerwin Klein, and Ihor Kuz

Property-Driven Fence Insertion Using Reorder Bounded Model Checking 291
Saurabh Joshi and Daniel Kroening

Verifying the Safety of a Flight-Critical System 308
Guillaume Brat, David Bushnell, Misty Davies, Dimitra Giannakopoulou, Falk Howar, and Temesghen Kahsai

Proving Safety with Trace Automata and Bounded Model Checking 325
Daniel Kroening, Matt Lewis, and Georg Weissenbacher

Verifying Parameterized Timed Security Protocols 342
Li Li, Jun Sun, Yang Liu, and Jin Song Dong

Abstraction of Elementary Hybrid Systems by Variable Transformation 360
Jiang Liu, Naijun Zhan, Hengjun Zhao, and Liang Zou

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

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

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

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

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

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

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

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

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

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

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

Industry Track

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

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-Stattelmann, 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