

John Fitzgerald · Constance Heitmeyer
Stefania Gnesi · Anna Philippou (Eds.)

FM 2016: Formal Methods

21st International Symposium
Limassol, Cyprus, November 9–11, 2016
Proceedings

Contents

Invited Presentations

- Industrial-Strength Model-Based Testing of Safety-Critical Systems. 3
Jan Peleska and Wen-ling Huang

Research Track

- Counter-Example Guided Program Verification. 25
Parosh Aziz Abdulla, Mohamed Faouzi Atig, and Bui Phi Diep
- Tighter Reachability Criteria for Deadlock-Freedom Analysis 43
Pedro Antonino, Thomas Gibson-Robinson, and A.W. Roscoe
- Compositional Parameter Synthesis 60
Lacramioara Aștefănoaei, Saddek Bensalem, Marius Bozga, Chih-Hong Cheng, and Harald Ruess
- Combining Mechanized Proofs and Model-Based Testing in the Formal Analysis of a Hypervisor 69
Hanno Becker, Juan Manuel Crespo, Jacek Galowicz, Ulrich Hensel, Yoichi Hirai, César Kunz, Keiko Nakata, Jorge Luis Sacchini, Hendrik Tews, and Thomas Tuerk
- A Model Checking Approach to Discrete Bifurcation Analysis 85
Nikola Beneš, Luboš Brim, Martin Demko, Samuel Pastva, and David Šafránek
- State-Space Reduction of Non-deterministically Synchronizing Systems Applicable to Deadlock Detection in MPI 102
Stanislav Böhm, Ondřej Meca, and Petr Jančar
- Formal Verification of Multi-Paxos for Distributed Consensus 119
Saksham Chand, Yanhong A. Liu, and Scott D. Stoller
- Validated Simulation-Based Verification of Delayed Differential Dynamics. 137
Mingshuai Chen, Martin Fränzle, Yangjia Li, Peter N. Mosaad, and Naijun Zhan
- Towards Learning and Verifying Invariants of Cyber-Physical Systems by Code Mutation. 155
Yuqi Chen, Christopher M. Poskitt, and Jun Sun

From Electrical Switched Networks to Hybrid Automata	164
<i>Alessandro Cimatti, Sergio Mover, and Mirko Sessa</i>	
Danger Invariants	182
<i>Cristina David, Pascal Kesseli, Daniel Kroening, and Matt Lewis</i>	
Local Planning of Multiparty Interactions with Bounded Horizons	199
<i>Mahieddine Dellabani, Jacques Combaz, Marius Bozga, and Saddek Bensalem</i>	
Finding Suitable Variability Abstractions for Family-Based Analysis	217
<i>Aleksandar S. Dimovski, Claus Brabrand, and Andrzej Wąsowski</i>	
Recovering High-Level Conditions from Binary Programs	235
<i>Adel Djoudi, Sébastien Bardin, and Éric Goubault</i>	
Upper and Lower Amortized Cost Bounds of Programs Expressed as Cost Relations	254
<i>Antonio Flores-Montoya</i>	
Exploring Model Quality for ACAS X.	274
<i>Dimitra Giannakopoulou, Dennis Guck, and Johann Schumann</i>	
Learning Moore Machines from Input-Output Traces.	291
<i>Georgios Gintamidis and Stavros Tripakis</i>	
Modal Kleene Algebra Applied to Program Correctness.	310
<i>Victor B.F. Gomes and Georg Struth</i>	
Mechanised Verification Patterns for Dafny	326
<i>Gudmund Grov, Yuhui Lin, and Vytautas Tumas</i>	
Formalising and Validating the Interface Description in the FMI Standard . . .	344
<i>Miran Hasanagić, Peter W.V. Tran-Jørgensen, Kenneth Lausdahl, and Peter Gorm Larsen</i>	
An Algebra of Synchronous Atomic Steps	352
<i>Ian J. Hayes, Robert J. Colvin, Larissa A. Meinicke, Kirsten Winter, and Andrius Velykis</i>	
Error Invariants for Concurrent Traces	370
<i>Andreas Holzer, Daniel Schwartz-Narbonne, Mitra Tabaei Befrouei, Georg Weissenbacher, and Thomas Wies</i>	
–	
An Executable Formalisation of the SPARCv8 Instruction Set Architecture: A Case Study for the LEON3 Processor.	388
<i>Zhe Hou, David Sanan, Alwen Tiu, Yang Liu, and Koh Chuen Hoa</i>	

Hybrid Statistical Estimation of Mutual Information for Quantifying Information Flow	406
<i>Yusuke Kawamoto, Fabrizio Biondi, and Axel Legay</i>	
A Generic Logic for Proving Linearizability	426
<i>Artem Khyzha, Alexey Gotsman, and Matthew Parkinson</i>	
Refactoring Refinement Structure of Event-B Machines	444
<i>Tsutomu Kobayashi, Fuyuki Ishikawa, and Shinichi Honiden</i>	
Towards Concolic Testing for Hybrid Systems	460
<i>Pingfan Kong, Yi Li, Xiaohong Chen, Jun Sun, Meng Sun, and Jingyi Wang</i>	
Explaining Relaxed Memory Models with Program Transformations	479
<i>Ori Lahav and Viktor Vafeiadis</i>	
SpecCert: Specifying and Verifying Hardware-Based Security Enforcement	496
<i>Thomas Letan, Pierre Chifflier, Guillaume Hiet, Pierre Néron, and Benjamin Morin</i>	
Automated Verification of Timed Security Protocols with Clock Drift	513
<i>Li Li, Jun Sun, and Jin Song Dong</i>	
Dealing with Incompleteness in Automata-Based Model Checking	531
<i>Claudio Menghi, Paola Spoletini, and Carlo Ghezzi</i>	
Equivalence Checking of a Floating-Point Unit Against a High-Level C Model	551
<i>Rajdeep Mukherjee, Saurabh Joshi, Andreas Griesmayer, Daniel Kroening, and Tom Melham</i>	
Battery-Aware Scheduling in Low Orbit: The GOMX-3 Case	559
<i>Morten Bisgaard, David Gerhardt, Holger Hermanns, Jan Krčál, Gilles Nies, and Marvin Stenger</i>	
Discounted Duration Calculus	577
<i>Heinrich Ody, Martin Fränzle, and Michael R. Hansen</i>	
Sound and Complete Mutation-Based Program Repair	593
<i>Bat-Chen Rothenberg and Orna Grumberg</i>	
An Implementation of Deflate in Coq	612
<i>Christoph-Simon Senjak and Martin Hofmann</i>	

Decoupling Abstractions of Non-linear Ordinary Differential Equations	628
<i>Andrew Sogokon, Khalil Ghorbal, and Taylor T. Johnson</i>	
Regression Verification for Unbalanced Recursive Functions	645
<i>Ofer Strichman and Maor Veitsman</i>	
Automated Mutual Explicit Induction Proof in Separation Logic	659
<i>Quang-Trung Ta, Ton Chanh Le, Siau-Cheng Khoo, and Wei-Ngan Chin</i>	
Finite Model Finding Using the Logic of Equality with Uninterpreted Functions	677
<i>Amirhossein Vakili and Nancy A. Day</i>	
GPUexplore 2.0: Unleashing GPU Explicit-State Model Checking	694
<i>Anton Wijs, Thomas Neele, and Dragan Bošnački</i>	
Approximate Bisimulation and Discretization of Hybrid CSP	702
<i>Gaogao Yan, Li Jiao, Yangjia Li, Shuling Wang, and Naijun Zhan</i>	
A Linear Programming Relaxation Based Approach for Generating Barrier Certificates of Hybrid Systems	721
<i>Zhengfeng Yang, Chao Huang, Xin Chen, Wang Lin, and Zhiming Liu</i>	
Industry Track	
Model-Based Design of an Energy-System Embedded Controller Using TASTE	741
<i>Roberto Cavada, Alessandro Cimatti, Luigi Crema, Mattia Roccabruna, and Stefano Tonetta</i>	
Simulink to UPPAAL Statistical Model Checker: Analyzing Automotive Industrial Systems	748
<i>Predrag Filipovikj, Nesredin Mahmud, Raluca Marinescu, Cristina Seceleanu, Oscar Ljungkrantz, and Henrik Lönn</i>	
Safety-Assured Formal Model-Driven Design of the Multifunction Vehicle Bus Controller	757
<i>Yu Jiang, Han Liu, Houbing Song, Hui Kong, Ming Gu, Jiaguang Sun, and Lui Sha</i>	
Taming Interrupts for Verifying Industrial Multifunction Vehicle Bus Controllers	764
<i>Han Liu, Yu Jiang, Huafeng Zhang, Ming Gu, and Jiaguang Sun</i>	

Rule-Based Incremental Verification Tools Applied to Railway Designs and Regulations	772
<i>Bjørnar Luteberget, Christian Johansen, Claus Feyling, and Martin Steffen</i>	
RIVER: A Binary Analysis Framework Using Symbolic Execution and Reversible x86 Instructions	779
<i>Teodor Stoenescu, Alin Stefanescu, Sorina Predut, and Florentin Ipate</i>	
Erratum to: Simulink to UPPAAL Statistical Model Checker: Analyzing Automotive Industrial Systems	E1
<i>Predrag Filipovikj, Nesredin Mahmud, Raluca Marinescu, Cristina Seceleanu, Oscar Ljungkrantz, and Henrik Lönn</i>	
Author Index	787