

Contents

An Automata-Theoretic Approach to Modeling Systems and Specifications over Infinite Data	1
<i>Hadar Frenkel, Orna Grumberg, and Sarai Sheinvald</i>	
Learning from Faults: Mutation Testing in Active Automata Learning	19
<i>Bernhard K. Aichernig and Martin Tappler</i>	
Parametric Model Checking Timed Automata Under Non-Zenoness Assumption	35
<i>Étienne André, Hoang Gia Nguyen, Laure Petrucci, and Jun Sun</i>	
Multi-timed Bisimulation for Distributed Timed Automata	52
<i>James Ortiz, Moussa Amrani, and Pierre-Yves Schobbens</i>	
Auto-Active Proof of Red-Black Trees in SPARK.	68
<i>Claire Dross and Yannick Moy</i>	
Analysing Security Protocols Using Refinement in iUML-B	84
<i>Colin Snook, Thai Son Hoang, and Michael Butler</i>	
On Learning Sparse Boolean Formulae for Explaining AI Decisions	99
<i>Susmit Jha, Vasumathi Raman, Alessandro Pinto, Tuhin Sahai, and Michael Francis</i>	
Event-Based Runtime Verification of Temporal Properties Using Time Basic Petri Nets	115
<i>Matteo Camilli, Angelo Gargantini, Patrizia Scandurra, and Carlo Bellettini</i>	
Model-Counting Approaches for Nonlinear Numerical Constraints	131
<i>Mateus Borges, Quoc-Sang Phan, Antonio Filieri, and Corina S. Păsăreanu</i>	
Input Space Partitioning to Enable Massively Parallel Proof	139
<i>Ashlie B. Hocking, M. Anthony Aiello, John C. Knight, and Nikos Aréchiga</i>	
Compositional Model Checking of Interlocking Systems for Lines with Multiple Stations	146
<i>Hugo Daniel Macedo, Alessandro Fantechi, and Anne E. Haxthausen</i>	

Modular Model-Checking of a Byzantine Fault-Tolerant Protocol	163
<i>Benjamin F. Jones and Lee Pike</i>	
Improved Learning for Stochastic Timed Models by State-Merging Algorithms	178
<i>Braham Lotfi Mediouni, Ayoub Nouri, Marius Bozga, and Saddek Bensalem</i>	
Verifying Safety and Persistence Properties of Hybrid Systems Using Flowpipes and Continuous Invariants	194
<i>Andrew Sogokon, Paul B. Jackson, and Taylor T. Johnson</i>	
A Relational Shape Abstract Domain.	212
<i>Hugo Illous, Matthieu Lemerre, and Xavier Rival</i>	
Floating-Point Format Inference in Mixed-Precision	230
<i>Matthieu Martel</i>	
A Verification Technique for Deterministic Parallel Programs.	247
<i>Saeed Darabi, Stefan C.C. Blom, and Marieke Huisman</i>	
Systematic Predicate Abstraction Using Variable Roles	265
<i>Yulia Demyanova, Philipp Rümmer, and Florian Zuleger</i>	
specgen: A Tool for Modeling Statecharts in CSP	282
<i>Brandon Shapiro and Chris Casinghino</i>	
HyPro: A C++ Library of State Set Representations for Hybrid Systems Reachability Analysis	288
<i>Stefan Schupp, Erika Ábrahám, Ibtissem Ben Makhlouf, and Stefan Kowalewski</i>	
Asm2C++: A Tool for Code Generation from Abstract State Machines to Arduino	295
<i>Silvia Bonfanti, Marco Carisconi, Angelo Gargantini, and Atif Mashkoor</i>	
SPEN: A Solver for Separation Logic	302
<i>Constantin Enea, Ondřej Lengál, Mihaela Sighireanu, and Tomáš Vojnar</i>	
From Hazard Analysis to Hazard Mitigation Planning: The Automated Driving Case	310
<i>Mario Gleirscher and Stefan Kugele</i>	
Event-B at Work: Some Lessons Learnt from an Application to a Robot Anti-collision Function	327
<i>Arnaud Dieumegard, Ning Ge, and Eric Jenn</i>	

Reasoning About Safety-Critical Information Flow Between Pilot and Computer.	342
<i>Seth Ahrenbach</i>	
Compositional Falsification of Cyber-Physical Systems with Machine Learning Components	357
<i>Tommaso Dreossi, Alexandre Donzé, and Sanjit A. Seshia</i>	
Verifying a Class of Certifying Distributed Programs.	373
<i>Kim Völlinger and Samira Akili</i>	
Compact Proof Witnesses.	389
<i>Marie-Christine Jakobs and Heike Wehrheim</i>	
Qualification of a Model Checker for Avionics Software Verification	404
<i>Lucas Wagner, Alain Mebsout, Cesare Tinelli, Darren Cofer, and Konrad Slind</i>	
SpeAR v2.0: Formalized Past LTL Specification and Analysis of Requirements	420
<i>Aaron W. Ficarek, Lucas G. Wagner, Jonathan A. Hoffman, Benjamin D. Rodes, M. Anthony Aiello, and Jennifer A. Davis</i>	
Just Formal Enough? Automated Analysis of EARS Requirements	427
<i>Levi Lúcio, Salman Rahman, Chih-Hong Cheng, and Alistair Mavin</i>	
Author Index	435

NASA Formal Methods

9th International Symposium, NFM 2017, Moffett Field,

CA, USA, May 16-18, 2017, Proceedings

Barrett, C.; Davies, M.; Kahsai, T. (Eds.)

2017, XI, 436 p. 124 illus., Softcover

ISBN: 978-3-319-57287-1