

# Contents – Part I

## Invited Contributions

Safety Verification of Deep Neural Networks . . . . .	3
<i>Xiaowei Huang, Marta Kwiatkowska, Sen Wang, and Min Wu</i>	
Program Verification Under Weak Memory Consistency Using Separation Logic . . . . .	30
<i>Viktor Vafeiadis</i>	
The Power of Symbolic Automata and Transducers . . . . .	47
<i>Loris D'Antoni and Margus Veanes</i>	
Maximum Satisfiability in Software Analysis: Applications and Techniques . . . . .	68
<i>Xujie Si, Xin Zhang, Radu Grigore, and Mayur Naik</i>	

## Probabilistic Systems

Reluplex: An Efficient SMT Solver for Verifying Deep Neural Networks . . .	97
<i>Guy Katz, Clark Barrett, David L. Dill, Kyle Julian, and Mykel J. Kochenderfer</i>	
Automated Recurrence Analysis for Almost-Linear Expected-Runtime Bounds . . . . .	118
<i>Krishnendu Chatterjee, Hongfei Fu, and Aniket Murhekar</i>	
Markov Automata with Multiple Objectives . . . . .	140
<i>Tim Quatmann, Sebastian Junges, and Joost-Pieter Katoen</i>	
Ensuring the Reliability of Your Model Checker: Interval Iteration for Markov Decision Processes . . . . .	160
<i>Christel Baier, Joachim Klein, Linda Leuschner, David Parker, and Sascha Wunderlich</i>	
Repairing Decision-Making Programs Under Uncertainty . . . . .	181
<i>Aws Albarghouthi, Loris D'Antoni, and Samuel Drews</i>	
Value Iteration for Long-Run Average Reward in Markov Decision Processes . . . . .	201
<i>Pranav Ashok, Krishnendu Chatterjee, Przemysław Daca, Jan Křetínský, and Tobias Meggendorfer</i>	

**Data Driven Techniques**

STLInspector: STL Validation with Guarantees. . . . .	225
<i>Hendrik Roehm, Thomas Heinz, and Eva Charlotte Mayer</i>	
Learning a Static Analyzer from Data . . . . .	233
<i>Pavol Bielik, Veselin Raychev, and Martin Vechev</i>	
Synthesis with Abstract Examples . . . . .	254
<i>Dana Drachler-Cohen, Sharon Shoham, and Eran Yahav</i>	
Data-Driven Synthesis of Full Probabilistic Programs . . . . .	279
<i>Sarah Chasins and Phitchaya Mangpo Phothilimthana</i>	
Logical Clustering and Learning for Time-Series Data . . . . .	305
<i>Marcell Vazquez-Chanlatte, Jyotirmoy V. Deshmukh, Xiaoqing Jin, and Sanjit A. Seshia</i>	

**Runtime Verification**

MONTRE: A Tool for Monitoring Timed Regular Expressions . . . . .	329
<i>Dogan Ulus</i>	
Runtime Monitoring with Recovery of the SENT Communication Protocol . . .	336
<i>Konstantin Selyunin, Stefan Jaksic, Thang Nguyen, Christian Reidl, Udo Hafner, Ezio Bartocci, Dejan Nickovic, and Radu Grosu</i>	
Runtime Verification of Temporal Properties over Out-of-Order Data Streams . . . . .	356
<i>David Basin, Felix Klaedtke, and Eugen Zălinescu</i>	

**Cyber-Physical Systems**

Lagrangian Reachability . . . . .	379
<i>Jacek Cyranka, Md. Ariful Islam, Greg Byrne, Paul Jones, Scott A. Smolka, and Radu Grosu</i>	
Simulation-Equivalent Reachability of Large Linear Systems with Inputs . . .	401
<i>Stanley Bak and Parasara Sridhar Duggirala</i>	
MIGHTYL: A Compositional Translation from MITL to Timed Automata . . . .	421
<i>Thomas Brihaye, Gilles Geeraerts, Hsi-Ming Ho, and Benjamin Monmege</i>	
DRYVR: Data-Driven Verification and Compositional Reasoning for Automotive Systems. . . . .	441
<i>Chuchu Fan, Bolun Qi, Sayan Mitra, and Mahesh Viswanathan</i>	

Automated Formal Synthesis of Digital Controllers for State-Space Physical Plants . . . . .	462
<i>Alessandro Abate, Iury Bessa, Dario Cattaruzza, Lucas Cordeiro, Cristina David, Pascal Kesseli, Daniel Kroening, and Elizabeth Polgreen</i>	
Classification and Coverage-Based Falsification for Embedded Control Systems . . . . .	483
<i>Arvind Adimoolam, Thao Dang, Alexandre Donzé, James Kapinski, and Xiaoping Jin</i>	
<b>Concurrency</b>	
GPUDrano: Detecting Uncoalesced Accesses in GPU Programs . . . . .	507
<i>Rajeev Alur, Joseph Devietti, Omar S. Navarro Leija, and Nimit Singhania</i>	
Context-Sensitive Dynamic Partial Order Reduction . . . . .	526
<i>Elvira Albert, Puri Arenas, María García de la Banda, Miguel Gómez-Zamalloa, and Peter J. Stuckey</i>	
Starling: Lightweight Concurrency Verification with Views . . . . .	544
<i>Matt Windsor, Mike Dodds, Ben Simner, and Matthew J. Parkinson</i>	
Compositional Model Checking with Incremental Counter-Example Construction . . . . .	570
<i>Anton Wijs and Thomas Neele</i>	
Pithya: A Parallel Tool for Parameter Synthesis of Piecewise Multi-affine Dynamical Systems . . . . .	591
<i>Nikola Beneš, Luboš Brim, Martin Demko, Samuel Pastva, and David Šafránek</i>	
<b>Author Index</b> . . . . .	599

## Contents – Part II

### Analysis of Software and Hardware

Verified Compilation of Space-Efficient Reversible Circuits . . . . .	3
<i>Matthew Amy, Martin Roetteler, and Krysta M. Svore</i>	
Ascertaining Uncertainty for Efficient Exact Cache Analysis . . . . .	22
<i>Valentin Touzeau, Claire Maïza, David Monniaux, and Jan Reineke</i>	
Non-polynomial Worst-Case Analysis of Recursive Programs . . . . .	41
<i>Krishnendu Chatterjee, Hongfei Fu, and Amir Kafshdar Goharshady</i>	
Automated Resource Analysis with Coq Proof Objects . . . . .	64
<i>Quentin Carbonneaux, Jan Hoffmann, Thomas Reps, and Zhong Shao</i>	
Look for the Proof to Find the Program: Decorated-Component-Based Program Synthesis. . . . .	86
<i>Adrià Gascón, Ashish Tiwari, Brent Carmer, and Umang Mathur</i>	
E-QED: Electrical Bug Localization During Post-silicon Validation Enabled by Quick Error Detection and Formal Methods. . . . .	104
<i>Eshan Singh, Clark Barrett, and Subhasish Mitra</i>	
SMTCoq: A Plug-In for Integrating SMT Solvers into Coq . . . . .	126
<i>Burak Ekici, Alain Mebsout, Cesare Tinelli, Chantal Keller, Guy Katz, Andrew Reynolds, and Clark Barrett</i>	

### Foundations of Verification

Efficient Parallel Strategy Improvement for Parity Games . . . . .	137
<i>John Fearnley</i>	
Model-Checking Linear-Time Properties of Parametrized Asynchronous Shared-Memory Pushdown Systems . . . . .	155
<i>Marie Fortin, Anca Muscholl, and Igor Walukiewicz</i>	
Minimization of Symbolic Transducers . . . . .	176
<i>Olli Saarikivi and Margus Veanes</i>	
Abstract Interpretation with Unfoldings . . . . .	197
<i>Marcelo Sousa, César Rodríguez, Vijay D'Silva, and Daniel Kroening</i>	
Cutoff Bounds for Consensus Algorithms. . . . .	217
<i>Ognjen Marić, Christoph Sprenger, and David Basin</i>	

Towards Verifying Nonlinear Integer Arithmetic . . . . .	238
<i>Paul Beame and Vincent Liew</i>	

### **Distributed and Networked Systems**

Network-Wide Configuration Synthesis . . . . .	261
<i>Ahmed El-Hassany, Petar Tsankov, Laurent Vanbever, and Martin Vechev</i>	
Verifying Equivalence of Spark Programs . . . . .	282
<i>Shelly Grossman, Sara Cohen, Shachar Itzhaky, Noam Rinetzkyl, and Mooly Sagiv</i>	
Synchronization Synthesis for Network Programs . . . . .	301
<i>Jedidiah McClurg, Hossein Hojjat, and Pavol Černý</i>	

### **Synthesis**

BoSy: An Experimentation Framework for Bounded Synthesis . . . . .	325
<i>Peter Faymonville, Bernd Finkbeiner, and Leander Tentrup</i>	
Bounded Synthesis for Streett, Rabin, and CTL* . . . . .	333
<i>Ayrat Khalimov and Roderick Bloem</i>	
Quantitative Assume Guarantee Synthesis . . . . .	353
<i>Shaull Almagor, Orna Kupferman, Jan Oliver Ringert, and Yaron Velner</i>	
Syntax-Guided Optimal Synthesis for Chemical Reaction Networks. . . . .	375
<i>Luca Cardelli, Milan Češka, Martin Fränzle, Marta Kwiatkowska, Luca Laurenti, Nicola Paoletti, and Max Whitby</i>	

### **Decision Procedures and Their Applications**

Model Counting for Recursively-Defined Strings . . . . .	399
<i>Minh-Thai Trinh, Duc-Hiep Chu, and Joxan Jaffar</i>	
A Three-Tier Strategy for Reasoning About Floating-Point Numbers in SMT . . . . .	419
<i>Sylvain Conchon, Mohamed Iguernlala, Kailiang Ji, Guillaume Melquiond, and Clément Fumex</i>	
A Correct-by-Decision Solution for Simultaneous Place and Route . . . . .	436
<i>Alexander Nadel</i>	
Scaling Up DPLL(T) String Solvers Using Context-Dependent Simplification . . . . .	453
<i>Andrew Reynolds, Maverick Woo, Clark Barrett, David Brumley, Tianyi Liang, and Cesare Tinelli</i>	

On Expansion and Resolution in CEGAR Based QBF Solving . . . . .	475
<i>Leander Tentrup</i>	
A Decidable Fragment in Separation Logic with Inductive Predicates and Arithmetic . . . . .	495
<i>Quang Loc Le, Makoto Tatsuta, Jun Sun, and Wei-Ngan Chin</i>	
<b>Software Analysis</b>	
Finding Fix Locations for CFL-Reachability Analyses via Minimum Cuts . . .	521
<i>Andrei Marian Dan, Manu Sridharan, Satish Chandra, Jean-Baptiste Jeannin, and Martin Vechev</i>	
Proving Linearizability Using Forward Simulations . . . . .	542
<i>Ahmed Bouajjani, Michael Emmi, Constantin Enea, and Suha Orhun Mutluergil</i>	
EAHyper: Satisfiability, Implication, and Equivalence Checking of Hyperproperties . . . . .	564
<i>Bernd Finkbeiner, Christopher Hahn, and Marvin Stenger</i>	
Automating Induction for Solving Horn Clauses . . . . .	571
<i>Hiroshi Unno, Sho Torii, and Hiroki Sakamoto</i>	
A <b>STORM</b> is Coming: A Modern Probabilistic Model Checker. . . . .	592
<i>Christian Dehnert, Sebastian Junges, Joost-Pieter Katoen, and Matthias Volk</i>	
On Multiphase-Linear Ranking Functions. . . . .	601
<i>Amir M. Ben-Amram and Samir Genaim</i>	
<b>Author Index</b> . . . . .	621

Computer Aided Verification

29th International Conference, CAV 2017, Heidelberg,

Germany, July 24-28, 2017, Proceedings, Part I

Majumdar, R.; Kunčák, V. (Eds.)

2017, XIX, 601 p. 142 illus., Softcover

ISBN: 978-3-319-63386-2