

Marsha Chechik · Jean-François Raskin (Eds.)

Tools and Algorithms for the Construction and Analysis of Systems

22nd International Conference, TACAS 2016
Held as Part of the European Joint Conferences
on Theory and Practice of Software, ETAPS 2016
Eindhoven, The Netherlands, April 2–8, 2016
Proceedings

Contents

Unifying Talk

- Robots at the Edge of the Cloud 3
Rupak Majumdar

Abstraction and Verification I

- Finding Recurrent Sets with Backward Analysis and Trace Partitioning 17
Alexey Bakhirkin and Nir Piterman
- Tactics for the Dafny Program Verifier 36
Gudmund Grov and Vytautas Tumas
- Synthesizing Ranking Functions from Bits and Pieces 54
Caterina Urban, Arie Gurfinkel, and Temesghen Kahsai
- Abstraction Refinement and Antichains for Trace Inclusion of Infinite State Systems 71
Radu Iosif, Adam Rogalewicz, and Tomáš Vojnar

Probabilistic and Stochastic Systems I

- Efficient Syntax-Driven Lumping of Differential Equations 93
Luca Cardelli, Mirco Tribastone, Max Tschaikowski, and Andrea Vandin
- Faster Statistical Model Checking for Unbounded Temporal Properties 112
Przemysław Daca, Thomas A. Henzinger, Jan Křetínský, and Tatjana Petrov
- Safety-Constrained Reinforcement Learning for MDPs. 130
Sebastian Junges, Nils Jansen, Christian Dehnert, Ufuk Topcu, and Joost-Pieter Katoen
- Safety Verification of Continuous-Space Pure Jump Markov Processes 147
Sadegh Esmaeil Zadeh Soudjani, Rupak Majumdar, and Alessandro Abate

Synthesis

- Abstract Learning Frameworks for Synthesis 167
Christof Löding, P. Madhusudan, and Daniel Neider

Synthesizing Piece-Wise Functions by Learning Classifiers	186
<i>Daniel Neider, Shambwaditya Saha, and P. Madhusudan</i>	
An Automaton Learning Approach to Solving Safety Games over Infinite Graphs	204
<i>Daniel Neider and Ufuk Topcu</i>	
Probabilistic and Stochastic Systems II	
Uncertainty Propagation Using Probabilistic Affine Forms and Concentration of Measure Inequalities	225
<i>Olivier Bouissou, Eric Goubault, Sylvie Putot, Aleksandar Chakarov, and Sriram Sankaranarayanan</i>	
Online and Compositional Learning of Controllers with Application to Floor Heating	244
<i>Kim G. Larsen, Marius Mikučionis, Marco Muñoz, Jiří Srba, and Jakob Haahr Taankvist</i>	
Deductive Proofs of Almost Sure Persistence and Recurrence Properties	260
<i>Aleksandar Chakarov, Yuen-Lam Voronin, and Sriram Sankaranarayanan</i>	
Probabilistic CTL*: The Deductive Way	280
<i>Rayna Dimitrova, Luis María Ferrer Fioriti, Holger Hermanns, and Rupak Majumdar</i>	
Tool Papers I	
Parametric Runtime Verification of C Programs	299
<i>Zhe Chen, Zhemin Wang, Yunlong Zhu, Hongwei Xi, and Zhibin Yang</i>	
Coqoon: An IDE for Interactive Proof Development in Coq	316
<i>Alexander Faithfull, Jesper Bengtson, Enrico Tassi, and Carst Tankink</i>	
Multi-core Symbolic Bisimulation Minimisation	332
<i>Tom van Dijk and Jaco van de Pol</i>	
Advances in Symbolic Probabilistic Model Checking with PRISM	349
<i>Joachim Klein, Christel Baier, Philipp Chrszon, Marcus Daum, Clemens Dubslaff, Sascha Klüppelholz, Steffen Märcker, and David Müller</i>	
PRISM-PSY: Precise GPU-Accelerated Parameter Synthesis for Stochastic Systems	367
<i>Milan Češka, Petr Pilař, Nicola Paoletti, Luboš Brim, and Marta Kwiatkowska</i>	

Tool Papers II

T2: Temporal Property Verification	387
<i>Marc Brockschmidt, Byron Cook, Samin Ishtiaq, Heidi Khlaaf, and Nir Piterman</i>	
RTD-Finder: A Tool for Compositional Verification of Real-Time Component-Based Systems.	394
<i>Souha Ben-Rayana, Marius Bozga, Saddek Bensalem, and Jacques Combaz</i>	
TcT: Tyrolean Complexity Tool	407
<i>Martin Avanzini, Georg Moser, and Michael Schaper</i>	
Integrated Environment for Diagnosing Verification Errors.	424
<i>Maria Christakis, K. Rustan M. Leino, Peter Müller, and Valentin Wüstholtz</i>	
JDART: A Dynamic Symbolic Analysis Framework	442
<i>Kasper Luckow, Marko Dimjašević, Dimitra Giannakopoulou, Falk Howar, Malte Isberner, Temesghen Kahsai, Zvonimir Rakamarić, and Vishwanath Raman</i>	

Concurrency

Diagnostic Information for Control-Flow Analysis of Workflow Graphs (a.k.a. Free-Choice Workflow Nets).	463
<i>Cédric Favre, Hagen Völzer, and Peter Müller</i>	
Approaching the Coverability Problem Continuously.	480
<i>Michael Blondin, Alain Finkel, Christoph Haase, and Serge Haddad</i>	
On Atomicity in Presence of Non-atomic Writes.	497
<i>Constantin Enea and Azadeh Farzan</i>	
Formalizing and Checking Thread Refinement for Data-Race-Free Execution Models	515
<i>Daniel Poetzl and Daniel Kroening</i>	

Tool Demos

The xSAP Safety Analysis Platform	533
<i>Benjamin Bittner, Marco Bozzano, Roberto Cavada, Alessandro Cimatti, Marco Gario, Alberto Griggio, Cristian Mattarei, Andrea Micheli, and Gianni Zampedri</i>	

FACT: A Probabilistic Model Checker for Formal Verification with Confidence Intervals	540
<i>Radu Calinescu, Kenneth Johnson, and Colin Paterson</i>	
PrDK: Protocol Programming with Automata	547
<i>Sung-Shik T.Q. Jongmans and Farhad Arbab</i>	
DLC: Compiling a Concurrent System Formal Specification to a Distributed Implementation.	553
<i>Hugues Evrard</i>	
PRISM-Games 2.0: A Tool for Multi-objective Strategy Synthesis for Stochastic Games.	560
<i>Marta Kwiatkowska, David Parker, and Clemens Wiltsche</i>	
Cerberus: Automated Synthesis of Enforcement Mechanisms for Security-Sensitive Business Processes.	567
<i>Luca Compagna, Daniel Ricardo dos Santos, Serena Elisa Ponta, and Silvio Ranise</i>	
Developing and Debugging Proof Strategies by Tinkering	573
<i>Yuhui Lin, Pierre Le Bras, and Gudmund Grov</i>	
v2c – A Verilog to C Translator	580
<i>Rajdeep Mukherjee, Michael Tautschnig, and Daniel Kroening</i>	
Abstraction and Verification II	
Parameterized Compositional Model Checking	589
<i>Kedar S. Namjoshi and Richard J. Trefler</i>	
An $O(m \log n)$ Algorithm for Stuttering Equivalence and Branching Bisimulation.	607
<i>Jan Friso Groote and Anton Wijs</i>	
Interpolants in Nonlinear Theories Over the Reals.	625
<i>Sicun Gao and Damien Zufferey</i>	
Abstraction and Verification III	
PTIME Computation of Transitive Closures of Octagonal Relations	645
<i>Filip Konečný</i>	
Scalable Verification of Linear Controller Software	662
<i>Junkil Park, Miroslav Pajic, Insup Lee, and Oleg Sokolsky</i>	
Partial Order Reduction for Event-Driven Multi-threaded Programs	680
<i>Pallavi Maiya, Rahul Gupta, Aditya Kanade, and Rupak Majumdar</i>	

Acceleration in Multi-PushDown Systems	698
<i>Mohamed Faouzi Atig, K. Narayan Kumar, and Prakash Saivasan</i>	

Languages and Automata

Reduction of Nondeterministic Tree Automata	717
<i>Ricardo Almeida, Lukáš Holík, and Richard Mayr</i>	
Online Timed Pattern Matching Using Derivatives	736
<i>Dogan Ulus, Thomas Ferrère, Eugene Asarin, and Oded Maler</i>	
Hybridization Based CEGAR for Hybrid Automata with Affine Dynamics . . .	752
<i>Nima Roohi, Pavithra Prabhakar, and Mahesh Viswanathan</i>	
Complementing Semi-deterministic Büchi Automata	770
<i>František Blahoudek, Matthias Heizmann, Sven Schewe, Jan Strejček, and Ming-Hsien Tsai</i>	

Security

Reasoning About Information Flow Security of Separation Kernels with Channel-Based Communication	791
<i>Yongwang Zhao, David Sanán, Fuyuan Zhang, and Yang Liu</i>	
Some Complexity Results for Stateful Network Verification	811
<i>Yaron Velner, Kalev Alpernas, Aurojit Panda, Alexander Rabinovich, Mooly Sagiv, Scott Shenker, and Sharon Shoham</i>	

Optimization

Characteristic Formulae for Session Types	833
<i>Julien Lange and Nobuko Yoshida</i>	
Bit-Vector Optimization	851
<i>Alexander Nadel and Vadim Ryvchin</i>	
Runtime Monitoring with Union-Find Structures	868
<i>Normann Decker, Jannis Harder, Torben Scheffel, Malte Schmitz, and Daniel Thoma</i>	

Competition on Software Verification: SV-COMP

Reliable and Reproducible Competition Results with BenchExec and Witnesses (Report on SV-COMP 2016)	887
<i>Dirk Beyer</i>	

2LS for Program Analysis (Competition Contribution)	905
<i>Peter Schrammel and Daniel Kroening</i>	
CIVL: Applying a General Concurrency Verification Framework to C/Pthreads Programs (Competition Contribution)	908
<i>Manchun Zheng, John G. Edenhofner, Ziqing Luo, Mitchell J. Gerrard, Michael S. Rogers, Matthew B. Dwyer, and Stephen F. Siegel</i>	
CPA-BAM: Block-Abstraction Memoization with Value Analysis and Predicate Analysis (Competition Contribution)	912
<i>Karlheinz Friedberger</i>	
CPA-RefSel: CPAchecker with Refinement Selection (Competition Contribution)	916
<i>Stefan Löwe</i>	
DIVINE: Explicit-State LTL Model Checker (Competition Contribution)	920
<i>Vladimír Štill, Petr Ročkal, and Jiří Barnat</i>	
Run Forester, Run Backwards! (Competition Contribution)	923
<i>Lukáš Holík, Martin Hruška, Ondřej Lengál, Adam Rogalewicz, Jiří Šimáček, and Tomáš Vojnar</i>	
LCTD: Tests-Guided Proofs for C Programs on LLVM (Competition Contribution)	927
<i>Olli Saarikivi and Keijo Heljanko</i>	
LPI: Software Verification with Local Policy Iteration (Competition Contribution)	930
<i>Egor George Karpenkov</i>	
Hunting Memory Bugs in C Programs with Map2Check (Competition Contribution)	934
<i>Herbert O. Rocha, Raimundo S. Barreto, and Lucas C. Cordeiro</i>	
MU-CSeq 0.4: Individual Memory Location Unwindings (Competition Contribution)	938
<i>Ermenegildo Tomasco, Truc L. Nguyen, Omar Inverso, Bernd Fischer, Salvatore La Torre, and Gennaro Parlato</i>	
Optimized PredatorHP and the SV-COMP Heap and Memory Safety Benchmark (Competition Contribution)	942
<i>Michal Kotoun, Petr Peringer, Veronika Šoková, and Tomáš Vojnar</i>	
Symbiotic 3: New Slicer and Error-Witness Generation (Competition Contribution)	946
<i>Marek Chalupa, Martin Jonáš, Jiri Slaby, Jan Strejček, and Martina Vitovská</i>	

Ultimate Automizer with Two-track Proofs (Competition Contribution) 950
*Matthias Heizmann, Daniel Dietsch, Marius Greitschus, Jan Leike,
 Betim Musa, Claus Schätzle, and Andreas Podelski*

Vienna Verification Tool: IC3 for Parallel Software
 (Competition Contribution). 954
Henning Günther, Alfons Laarman, and Georg Weissenbacher

Author Index 959