

2018 Formal Methods in Computer Aided Design (FMCAD 2018)

**Austin, Texas, USA
30 October – 2 November 2018**



**IEEE Catalog Number: CFP18FMC-POD
ISBN: 978-1-5386-7567-0**

**Copyright © 2018, FMCAD Inc.
All Rights Reserved**

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP18FMC-POD
ISBN (Print-On-Demand):	978-1-5386-7567-0
ISBN (Online):	978-0-9835678-8-2

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

Table of Contents

Invited Papers

Formal Verification of Deep Neural Networks	1
<i>Nina Narodytska</i>	
Formal Verification of Unsatisfiability Results	2
<i>Marijn Heule</i>	
Deductive Verification of Distributed Protocols in First-Order Logic	3
<i>Oded Padon</i>	
Formal Verification of Financial Algorithms with Imandra	4
<i>Grant Passmore</i>	
Formal Design, Implementation and Verification of Blockchain Languages	5
<i>Grigore Rosu</i>	
The FMCAD 2018 Graduate Student Forum	6
<i>Dejan Jovanović and Andrew Reynolds</i>	

Hardware

CoSA: Integrated Verification for Agile Hardware Design	7
<i>Cristian Mattarei, Makai Mann, Clark Barrett, Ross Daly, Dillon Huff and Pat Hanrahan</i>	
ILA-MCM: Integrating Memory Consistency Models with Instruction-Level Abstractions for Heterogeneous System-on-Chip Verification	12
<i>Hongce Zhang, Caroline Trippel, Yatin Manerkar, Aarti Gupta, Margaret Martonosi and Sharad Malik</i>	
BMC with Memory Models as Modules	22
<i>Hernan Ponce-De-Leon, Florian Furbach, Keijo Heljanko and Roland Meyer</i>	

Quantifiers and SAT

Complete Test Sets And Their Approximations	31
<i>Eugene Goldberg</i>	
Expansion-Based QBF Solving Without Recursion	40
<i>Roderick Bloem, Nicolas Braud-Santoni, Vedad Hadžić, Uwe Egly, Florian Lonsing and Martina Seidl</i>	
Bit-Vector Interpolation and Quantifier Elimination by Lazy Reduction	50
<i>Peter Backeman, Philipp Ruemmer and Aleksandar Zeljić</i>	

Liveness

Analyzing the Fundamental Liveness Property of the Chord Protocol	60
<i>Julien Brunel, David Chemouil and Jeanne Tawa</i>	
k-FAIR = k-LIVENESS + FAIR: Revisiting SAT-based Liveness Algorithms	69
<i>Alexander Ivrii, Ziv Nevo and Jason Baumgartner</i>	
Temporal Prophecy for Proving Temporal Properties of Infinite-State Systems	74
<i>Oded Padon, Jochen Hoenicke, Kenneth L. McMillan, Andreas Podelski, Mooly Sagiv and Sharon Shoham</i>	

Concurrency

Automatic Synchronization for GPU Kernels	85
<i>Sourav Anand and Nadia Polikarpova</i>	
Rely-Guarantee Reasoning for Automated Bound Analysis of Lock-Free Algorithms	94
<i>Thomas Pani, Georg Weissenbacher and Florian Zuleger</i>	

Verification

Template-Based Verification of Heap-Manipulating Programs	103
<i>Viktor Malík, Martin Hruska, Peter Schrammel and Tomas Vojnar</i>	

Using Loop Bound Analysis For Invariant Generation.....	112
<i>Pavel Cadek, Clemens Danninger, Moritz Sinn and Florian Zuleger</i>	
Post-Verification Debugging and Rectification of Finite Field Arithmetic Circuits using Computer Algebra Techniques.....	121
<i>Vikas Rao, Utkarsh Gupta, Irina Iliaeva, Arpitha Srinath, Priyank Kalla and Florian Enescu</i>	
Learning and Synthesis	
Automata Learning for Symbolic Execution.....	130
<i>Bernhard K. Aichernig, Roderick Bloem, Masoud Ebrahimi, Martin Tappler and Johannes Winter</i>	
Functional Synthesis via Input-Output Separation.....	139
<i>Supratik Chakraborty, Dror Fried, Lucas Martinelli Tabajara and Moshe Vardi</i>	
Learning Linear Temporal Properties	148
<i>Ivan Gavran and Daniel Neider</i>	
SMT and CHC	
The Eldarica Horn Solver.....	158
<i>Hossein Hojjat and Philipp Ruemmer</i>	
Trau: SMT solver for string constraints	165
<i>Parosh Aziz Abdulla, Mohamed Faouzi Atig, Yu-Fang Chen, Bui Phi Diep, Lukas Holik, Ahmed Rezzine and Philipp Rümmer</i>	
Solving Constrained Horn Clauses Using Syntax and Data	170
<i>Grigory Fedyukovich, Sumanth Prabhu, Kumar Madhukar and Aarti Gupta</i>	
Rails	
Analysis of Relay Interlocking Systems via SMT-based Model Checking of Switched Multi-Domain Kirchhoff Networks.....	179
<i>Roberto Cavada, Alessandro Cimatti, Sergio Mover, Mirko Sessa, Giuseppe Cadavero and Giuseppe Scaglione</i>	
Design-Time Railway Capacity Verification using SAT modulo Discrete Event Simulation.....	188
<i>Bjørnar Luteberget, Koen Claessen and Christian Johansen</i>	
Certificates	
Complete and Efficient DRAT Proof Checking	197
<i>Adrian Rebola Pardo and Luís Cruz-Filipe</i>	
Semantic-based Automated Reasoning for AWS Access Policies using SMT.....	206
<i>John Backes, Pauline Bolignano, Byron Cook, Catherine Dodge, Andrew Gacek, Kasper Luckow, Neha Rungta, Oksana Tkachuk and Carsten Varming</i>	
A Verified Certificate Checker for Finite-Precision Error Bounds in Coq and HOL4.....	215
<i>Heiko Becker, Nikita Zyuzin, Raphaël Monat, Eva Darulova, Magnus O. Myreen and Anthony Fox</i>	
Certifying Proofs for LTL Model Checking	225
<i>Alberto Griggio, Marco Roveri and Stefano Tonetta</i>	