

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison, UK

Josef Kittler, UK

John C. Mitchell, USA

Bernhard Steffen, Germany

Demetri Terzopoulos, USA

Gerhard Weikum, Germany

Takeo Kanade, USA

Jon M. Kleinberg, USA

Friedemann Mattern, Switzerland

Moni Naor, Israel

C. Pandu Rangan, India

Doug Tygar, USA

Advanced Research in Computing and Software Science

Subline of Lecture Notes in Computer Science

Subline Series Editors

Giorgio Ausiello, *University of Rome 'La Sapienza', Italy*

Vladimiro Sassone, *University of Southampton, UK*

Subline Advisory Board

Susanne Albers, *TU Munich, Germany*

Benjamin C. Pierce, *University of Pennsylvania, USA*

Bernhard Steffen, *University of Dortmund, Germany*

Deng Xiaotie, *City University of Hong Kong*

Jeannette M. Wing, *Microsoft Research, Redmond, WA, USA*

More information about this series at <http://www.springer.com/series/7407>

Martin Davis · Ansgar Fehnker
Annabelle McIver · Andrei Voronkov (Eds.)

Logic for Programming, Artificial Intelligence, and Reasoning

20th International Conference, LPAR-20 2015
Suva, Fiji, November 24–28, 2015
Proceedings

Editors

Martin Davis
New York University
New York, NY
USA

Annabelle McIver
Macquarie University
Sydney, NSW
Australia

Ansgar Fehnker
University of the South Pacific
Suva
Fiji

Andrei Voronkov
The University of Manchester
Manchester
UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-662-48898-0 ISBN 978-3-662-48899-7 (eBook)
DOI 10.1007/978-3-662-48899-7

Library of Congress Control Number: 2015954999

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

Springer Heidelberg New York Dordrecht London
© Springer-Verlag Berlin Heidelberg 2015

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

Springer-Verlag GmbH Berlin Heidelberg is part of Springer Science+Business Media
(www.springer.com)

Preface

This volume contains the papers presented at the 20th International Conference on Logic for Programming, Artificial Intelligence and Reasoning (LPAR-20), held during November 24–28, 2015, at the University of the South Pacific, Suva, Fiji.

Following the call for papers, LPAR-20 received 117 abstracts, materializing into 92 submissions. Each submission was reviewed by a panel of 53 Program Committee (PC) members. The PC was assisted by 107 additional reviewers and decided to accept 43 papers. The EasyChair system provided an indispensable platform for all matters related to the reviewing process, production of these proceedings, program and Web page generation, and registration of participants.

Several workshops were collocated with LPAR-20. The first workshop on Models for Formal Analysis of Real Systems (MARS 2015) was organized by Rob van Glabbeek and Peter Hoefner of NICTA and Jan Friso Groote from Eindhoven University of Technology. The First International Workshop on Focusing was organized by Iliano Cervesato of Carnegie Mellon University and Carsten Schuermann of ITU Copenhagen and Demtech. The 11th International Workshop on the Implementation of Logics was organized by Boris Konev of the University of Liverpool, Stephan Schulz of DHBW Stuttgart, and Laurent Simon of the University of Bordeaux. We were fortunate to have Peter Baumgartner of NICTA as workshop chair.

The local conference organization was arranged by Geoff Sutcliffe and Ansgar Fehnker, and together they put together an excellent event.

LPAR-20 is grateful for the generous support of Microsoft Research and University of the South Pacific.

September 2015

Martin Davis
Ansgar Fehnker
Annabelle McIver
Andrei Voronkov

Organization

Program Committee

Cyrille Valentin Artho	AIST, Japan
Franz Baader	Technical University of Dresden, Germany
Christel Baier	Technical University of Dresden, Germany
Peter Baumgartner	National ICT, Australia
Armin Biere	Johannes Kepler University, Austria
Maria Paola Bonacina	Università degli Studi di Verona, Italy
Lei Bu	Nanjing University, China
Franck Cassez	Macquarie University, Australia
Krishnendu Chatterjee	Institute of Science and Technology (IST)
Michael Codish	Ben-Gurion University of the Negev, Israel
Hubert Comon-Lundh	ENS Cachan, France
Martin Davis	Courant Institute of Mathematical Sciences, New York University, USA
Joerg Endrullis	Vrije Universiteit Amsterdam, The Netherlands
Javier Esparza	Technische Universität München, Germany
Ansgar Fehnker	University of the South Pacific, Fiji
Christian Fermüller	TU Wien, Austria
Bernd Fischer	Stellenbosch University, South Africa
Jürgen Giesl	RWTH Aachen, Germany
Rajeev Gore	The Australian National University, Australia
Tim Griffin	University of Cambridge, UK
Kim Guldstrand Larsen	Aalborg University, Denmark
Miki Hermann	LIX, Ecole Polytechnique, France
Dejan Jovanović	SRI International, Singapore
Laura Kovacs	Chalmers University of Technology, Sweden
Dexter Kozen	Cornell University, USA
Temur Kutsia	RISC, Johannes Kepler University Linz, Austria
Rustan Leino	Microsoft Research, USA
Joe Leslie-Hurd	Intel Corporation, USA
Luigi Liquori	Inria, France
Christopher Lynch	Clarkson University, USA
Annabelle McIver	Macquarie University, Australia
Kenneth McMillan	Microsoft Research, USA
Aart Middeldorp	University of Innsbruck, Austria
Marius Minea	Politehnica University of Timisoara, Romania
Matteo Mio	CNRS/ENS-Lyon, France
Joachim Niehren	Inria Lille, France
Prakash Panangaden	McGill University, Canada

Christine Paulin-Mohring	Université Paris-Sud, France
Andreas Podelski	University of Freiburg, Germany
Sanjiva Prasad	Indian Institute of Technology Delhi, India
Revantha Ramanayake	Vienna University of Technology, Austria
Grigore Rosu	University of Illinois at Urbana-Champaign, USA
Michael Rusinowitch	LORIA–Inria Nancy, France
Torsten Schaub	University of Potsdam, Germany
Helmut Seidl	TU München, Germany
Geoff Sutcliffe	University of Miami, USA
Gancho Vachkov	The University of the South Pacific (USP), Fiji
Ron Van Der Meyden	UNSW, Australia
Tomas Vojnar	Brno University of Technology, Czech Republic
Andrei Voronkov	The University of Manchester, UK
Toby Walsh	NICTA and UNSW, Australia

Additional Reviewers

Abreu, Salvador	Flouris, Giorgos	Ludwig, Michel
Baelde, David	Frohn, Florian	Luigi, Liquori
Bellin, Gianluigi	Fuhs, Carsten	Madelaine, Guillaume
Ben-Amram, Amir	Gay, Simon	Maffezioli, Paolo
Blanchette, Jasmin	Gebler, Daniel	Mathieson, Luke
Bochman, Alexander	Gebser, Martin	Mayer-Eichberger, Valentin
Borchmann, Daniel	González De Aledo, Pablo	Mayr, Richard
Bordenabe, Nicolás E.	Gorogiannis, Nikos	Meyer, Philipp J.
Casini, Giovanni	Graham-Lengrand, Stéphane	Michalewski, Henryk
Cerna, David	Grädel, Erich	Miculan, Marino
Cervesato, Iliano	Guenot, Nicolas	Moore, Brandon
Chaudhuri, Avik	Hagihara, Shigeki	Munch-Maccagnoni, Guillaume
Chaudhuri, Kaustuv	Heizmann, Matthias	Myreen, Magnus O.
Clouston, Ranald	Holik, Lukas	Napoli, Amedeo
Courcelle, Bruno	Hölldobler, Steffen	Nigam, Vivek
Cruz-Filipe, Luís	Ibsen-Jensen, Rasmus	Obermeier, Philipp
Das, Anupam	Kaliszyk, Cezary	Parigot, Michel
Davies, Jessica	Kincaid, Zachary	Park, Daejun
Delzanno, Giorgio	Kolanski, Rafal	Pek, Edgar
Dima, Catalin	Kotelnikov, Evgenii	Peled, Doron
Downen, Paul	Krishnaswami, Neelakantan	Peltier, Nicolas
Dutertre, Bruno	Kuijjer, Louwe B.	Pientka, Brigitte
Dyckhoff, Roy	Kuprianov, Andrey	Popeea, Corneliu
Escobar, Santiago	Leino, Rustan	Preining, Norbert
Felgenhauer, Bertram	Leuschner, Linda	Qi, Guilin
Fernandez Gil, Oliver		
Fichte, Johannes Klaus		

Ranise, Silvio
Redl, Christoph
Rezk, Tamara
Ricciotti, Wilmer
Sanchez, Cesar
Sangnier, Arnaud
Saurin, Alexis
Schwitter, Rolf
Schäf, Martin
Seidl, Martina
Sickert, Salomon

Simkus, Mantas
Stefanescu, Andrei
Sternagel, Christian
Strassburger, Lutz
Takeuti, Izumi
Talcott, Carolyn
Terui, Kazushige
Thiemann, René
Toninho, Bernardo
Trivedi, Ashutosh
Verma, Rakesh

Vyskocil, Jiri
Wilson, David
Woltzenlogel Paleo,
Bruno
Wunderlich, Sascha
Yamada, Akihisa
Zarrieß, Benjamin
Zhang, Cheng
Zhang, Yi

Satisfiability: From Quality to Quantities

(Abstract of Invited Talk)

Nikolaj Bjørner

Microsoft Research
nbjorner@microsoft.com

Satisfiability Modulo Theories, SMT, solvers have in the past decade enabled a number of software engineering tools thanks to improved theorem proving technologies, their support for domains that are commonly used in software and a confluence of advances in symbolic analysis methodologies. These methodologies are diverse and range from bug localization, symbolic model checking algorithms, dynamic symbolic execution for uncovering bugs and creating parametric unit tests, certified development using program verification tools, compiler validation, biological modeling, model based design tools, web sanitizers, and runtime analysis. The synergy with application domains has lead to a constant stream of inspiration for improved domain support and algorithmic advances. A simultaneous trend in applications is leading research on SMT solvers into calculating with quantities. We believe this is part of an overall trend of tools for checking and synthesizing quantitative, including probabilistic, properties.

Using Network Verification as a starting point, we describe how the SMT solver Z3 is used at scale in Microsoft Azure to check network access restrictions and router configurations. Z3 is used in a monitoring system, called SecGuru, that continuously checks configurations as they appear on routers. We learned early on that network operators required a tool that could return a set of models in a compact way. This led us to develop a domain specific algorithm, that works well for access control lists. It enumerates models compactly in fractions of a second. A more ambitious effort is to check reachability properties in large data-centers. Again, our experience was that the domain called for special purpose data-structures and symmetry reduction methods that turn analysis of data-centers with hundreds of routers and a million forwarding rules into very small finite state systems that can be analyzed in fractions of a second.

Our experience with Network Verification is not unlike other domains as we are reaching a point where qualitative analysis has shown its use, but a larger elephant is lurking in the room: most systems rely on performance guarantees. Thus, the need for checking and synthesizing quantitative properties. To support SMT with quantities we have embarked on long term projects on integrating optimization algorithms with Z3 and integrating methods for counting the number of solutions to constraints. In this context we developed a new MaxSAT algorithm that exploits dualities between unsatisfiable cores and correction sets and we illustrate some uses of the emerging quantitative features in Z3.

The work rests on collaboration with a large number of colleagues including Karthick Jayaraman, George Varghese, Nina Narodytska, Nuno Lopes, Andrey Rybalchenko, Leonardo de Moura, Christoph Wintersteiger, Gordon Plotkin.

Contents

Skolemization for Substructural Logics	1
<i>Petr Cintula, Denisa Diaconescu, and George Metcalfe</i>	
Reasoning About Embedded Dependencies Using Inclusion Dependencies . . .	16
<i>Miika Hannula</i>	
Cobra: A Tool for Solving General Deductive Games	31
<i>Miroslav Klimoš and Antonín Kučera</i>	
On Anti-subsumptive Knowledge Enforcement	48
<i>Éric Grégoire and Jean-Marie Lagniez</i>	
Value Sensitivity and Observable Abstract Values for Information Flow Control	63
<i>Luciano Bello, Daniel Hedin, and Andrei Sabelfeld</i>	
SAT-Based Minimization of Deterministic ω -Automata	79
<i>Souheib Baarir and Alexandre Duret-Lutz</i>	
FEMaLeCoP: Fairly Efficient Machine Learning Connection Prover	88
<i>Cezary Kaliszyk and Josef Urban</i>	
Decidability, Introduction Rules and Automata	97
<i>Gilles Dowek and Ying Jiang</i>	
Analyzing Internet Routing Security Using Model Checking	112
<i>Adi Sosnovich, Orna Grumberg, and Gabi Nakibly</i>	
Boolean Formulas for the Static Identification of Injection Attacks in Java . . .	130
<i>Michael D. Ernst, Alberto Lovato, Damiano Macedonio, Ciprian Spiridon, and Fausto Spoto</i>	
An Adequate Compositional Encoding of Bigraph Structure in Linear Logic with Subexponentials	146
<i>Kaustuv Chaudhuri and Giselle Reis</i>	
Controller Synthesis for MDPs and Frequency $LTL_{\setminus GU}$	162
<i>Vojtěch Forejt, Jan Krčál, and Jan Křetínský</i>	
Automated Benchmarking of Incremental SAT and QBF Solvers	178
<i>Uwe Egly, Florian Lonsing, and Johannes Oetsch</i>	
A Labelled Sequent Calculus for Intuitionistic Public Announcement Logic . . .	187
<i>Shoshin Nomura, Katsuhiko Sano, and Satoshi Tojo</i>	

Implicit Computational Complexity of Subrecursive Definitions and Applications to Cryptographic Proofs.	203
<i>Patrick Baillot, Gilles Barthe, and Ugo Dal Lago</i>	
TIP: Tools for Inductive Provers.	219
<i>Dan Rosén and Nicholas Smallbone</i>	
Verification of Concurrent Programs Using Trace Abstraction Refinement . . .	233
<i>Franck Cassez and Frowin Ziegler</i>	
Synchronized Recursive Timed Automata	249
<i>Yuya Uezato and Yasuhiko Minamide</i>	
Focused Labeled Proof Systems for Modal Logic	266
<i>Dale Miller and Marco Volpe</i>	
On CTL* with Graded Path Modalities	281
<i>Benjamin Aminof, Aniello Murano, and Sasha Rubin</i>	
On Subexponentials, Synthetic Connectives, and Multi-level Delimited Control	297
<i>Chuck Liang and Dale Miller</i>	
On the Expressive Power of Communication Primitives in Parameterised Systems	313
<i>Benjamin Aminof, Sasha Rubin, and Florian Zuleger</i>	
There Is No Best β -Normalization Strategy for Higher-Order Reasoners.	329
<i>Alexander Steen and Christoph Benzmüller</i>	
Fine Grained SMT Proofs for the Theory of Fixed-Width Bit-Vectors	340
<i>Liana Hadarean, Clark Barrett, Andrew Reynolds, Cesare Tinelli, and Morgan Deters</i>	
Abstract Domains and Solvers for Sets Reasoning.	356
<i>Arlen Cox, Bor-Yuh Evan Chang, Huisong Li, and Xavier Rival</i>	
Sharing HOL4 and HOL Light Proof Knowledge	372
<i>Thibault Gauthier and Cezary Kaliszyk</i>	
Relational Reasoning via Probabilistic Coupling	387
<i>Gilles Barthe, Thomas Espitau, Benjamin Grégoire, Justin Hsu, Léo Stefanescu, and Pierre-Yves Strub</i>	
A Contextual Logical Framework	402
<i>Peter Brottveit Bock and Carsten Schürmann</i>	

Enhancing Search-Based QBF Solving by Dynamic Blocked Clause Elimination	418
<i>Florian Lonsing, Fahiem Bacchus, Armin Biere, Uwe Egly, and Martina Seidl</i>	
Reasoning About Loops Using Vampire in KeY	434
<i>Wolfgang Ahrendt, Laura Kovács, and Simon Robillard</i>	
Compositional Propositional Proofs	444
<i>Marijn J.H. Heule and Armin Biere</i>	
ELPI: Fast, Embeddable, λ Prolog Interpreter	460
<i>Cvetan Dunchev, Ferruccio Guidi, Claudio Sacerdoti Coen, and Enrico Tassi</i>	
Normalisation by Completeness with Heyting Algebras	469
<i>Gaëtan Gilbert and Olivier Hermant</i>	
Using Program Synthesis for Program Analysis	483
<i>Cristina David, Daniel Kroening, and Matt Lewis</i>	
Finding Inconsistencies in Programs with Loops	499
<i>Temesghen Kahsai, Jorge A. Navas, Dejan Jovanović, and Martin Schäf</i>	
Modular Multiset Rewriting	515
<i>Iliano Cervesato and Edmund S.L. Lam</i>	
Modelling Moral Reasoning and Ethical Responsibility with Logic Programming	532
<i>Fiona Berreby, Gauvain Bourgne, and Jean-Gabriel Ganascia</i>	
Constrained Term Rewriting tool	549
<i>Cynthia Kop and Naoki Nishida</i>	
Proof Search in Nested Sequent Calculi	558
<i>Björn Lellmann and Elaine Pimentel</i>	
Tableau-Based Revision over <i>SHIQ</i> TBoxes	575
<i>Thinh Dong, Chan Le Duc, Philippe Bonnot, and Myriam Lamolle</i>	
Gamifying Program Analysis	591
<i>Daniel Fava, Julien Signoles, Matthieu Lemerre, Martin Schäf, and Ashish Tiwari</i>	
Automated Discovery of Simulation Between Programs	606
<i>Grigory Fedyukovich, Arie Gurfinkel, and Natasha Sharygina</i>	
SAT Modulo Intuitionistic Implications	622
<i>Koen Claessen and Dan Rosén</i>	
Author Index	639