Lecture Notes in Artificial Intelligence 9706

Subseries of Lecture Notes in Computer Science

More information about this series at http://www.springer.com/series/1244

Nicola Olivetti · Ashish Tiwari (Eds.)

Automated Reasoning

8th International Joint Conference, IJCAR 2016
Coimbra, Portugal, June 27 – July 2, 2016
Proceedings

Springer

Editors

Nicola Olivetti
Aix-Marseille University
Marseille
France

Ashish Tiwari
SRI International
Menlo Park, CA
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Artificial Intelligence
ISBN 978-3-319-40228-4 ISBN 978-3-319-40229-1 (eBook)
DOI 10.1007/978-3-319-40229-1

Library of Congress Control Number: 2016940352

LNCS Sublibrary: SL7 – Artificial Intelligence

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

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Preface

This volume contains the proceedings of the 8th International Joint Conference on Automated Reasoning, IJCAR 2016, held in Coimbra (Portugal) during June 27 – July 2, 2016. IJCAR is the premier international conference covering all topics in automated reasoning, including foundations, implementations, and applications. The 2016 edition of the conference was a merger of three leading events in automated reasoning: International Conference on Automated Deduction (CADE), International Symposium on Frontiers of Combining Systems (FroCoS) and International Conference on Analytic Tableaux and Related Methods (TABLEAUX). Previous IJCAR conferences were held at Siena (Italy) in 2001, Cork (Ireland) in 2004, Seattle (USA) in 2006, Sydney (Australia) in 2008, Edinburgh (UK) in 2010, Manchester (UK) in 2012, and Vienna (Austria) in 2014.

The IJCAR 2016 program consisted of presentations of original research papers and invited talks. Original papers were divided into two categories: regular papers and system desriptions. There were 79 submissions, consisting of 65 regular papers and 14 systems descriptions. Each paper was carefully reviewed by at least three reviewers. All reviewers were either members of the Program Committee (PC) or experts in the area chosen by the PC members. After reviewing and discussing the submissions, the PC accepted 26 regular papers and nine system descriptions.

The program also included four invited talks of the highest scientific value given by Arnon Avron (Tel Aviv University), Gilles Barthe (IMDEA Madrid), Sumit Gulwani, (MSR, Redmond) and André Platzer (CMU, Pittsburgh). The abstracts of the invited talks are included in the present proceedings.

The peer-reviewed research papers are organized in the proceedings in the following sections: Satisfiability of Boolean Formulas, Satisfiability Modulo Theory, Rewriting, Arithmetic Reasoning and Mechanized Mathematics, First-Order Logic and Proof Theory, First-Order Theorem Proving, Higher-Order Theorem Proving, Modal and Temporal Logics, Non-Classical Logics, and Verification. The wide range of sections reflect the variety of topics covered in IJCAR 2016 and witness the maturity of the area of automated reasoning.

During the conference, the International Conference on Automated Deduction (CADE) Herbrand Award for Distinguished Contributions to Automated Reasoning was presented to Zohar Manna and Richard Waldinger. The Best Paper Award was conferred to Jasmin Christian Blanchette (Inria, France), Mathias Fleury (MPI, Germany), and Christoph Weidenbach (MPI, Germany) for their paper titled "A Verified SAT Solver Framework with Learn, Forget, Restart, and Incrementality." Several students received the Woody Bledsoe Travel Awards, named after the late Woody Bledsoe, and funded by CADE Inc. to support student participation.

Several people helped make IJCAR 2016 a success. We want to express our gratitude to the conference chair, Pedro Quaresma, and to the local Organizing Committee who made IJCAR 2016 possible: Sandra Marques Pinto (publicity chair), Reinhard

Kahle (workshop chair), Nuno Baeta, Carlos Caleiro, Nelma Moreira, João Rasga, and Vanda Santos. We thank all the members of the PC for their active participation in the process of evaluating and selecting papers for publication, and during the selection of the invited speakers. We also thank the external reviewers for their precious contribution. The combined expertise of the PC members and the external reviewers ensured that the papers accepted for publication were of the highest scientific quality. We whole-heartedly thank all the authors for submitting their work to IJCAR 2016. On behalf of the PC, we thank the invited speakers for their contribution. We also acknowledge the contributions of the workshop and competition organizers. We extend our thanks to Andrei Voronkov and the EasyChair development team for providing their conference management platform.

We finally thank the University of Coimbra, the hosting institution, and all sponsors for their contribution to the success of the event.

April 2016

Nicola Olivetti
Ashish Tiwari

Organization

IJCAR 2016 was organized by the Department of Mathematics of the Faculty of Sciences and Technology of the University of Coimbra.

Program Committee Chairs

Nicola Olivetti	LSIS, University of Aix-Marseille, France
Ashish Tiwari	SRI International, USA

Program Committee

Franz Baader	TU Dresden, Germany
Peter Baumgartner	NICTA, The Australian National University, Australia
Maria Paola Bonacina	Università degli Studi di Verona, Italy
Agata Ciabattoni	TU Wien, Austria
Leonardo de Moura	Microsoft Research, USA
Hans De Nivelle	University of Wroclaw, Poland
Stephanie Delaune	LSV, CNRS, ENS Cachan, France
Stéphane Demri	LSV, CNRS, ENS Cachan, France
Clare Dixon	University of Liverpool, UK
Christian Fermüller	TU Wien, Austria
Didier Galmiche	Université de Lorraine - LORIA, France
Silvio Ghilardi	Università degli Studi di Milano, Italy
Jürgen Giesl	RWTH Aachen University, Germany
Birte Glimm	Universität Ulm, Germany
Rajeev Goré	The Australian National University, Australia
Reiner Hähnle	Technical University of Darmstadt, Germany
Stefan Hetzl	TU Wien, Austria
Dejan Jovanović	SRI International, USA
Reinhard Kahle	CENTRIA Universidade Nova de Lisboa, Portugal
Deepak Kapur	University of New Mexico, USA
Jordi Levy	IIIA CSIC, Bellaterra, Catalonia, Spain
Carsten Lutz	University of Bremen, Germany
Christopher Lynch	Clarkson University, USA
George Metcalfe	University of Bern, Switzerland
Aart Middeldorp	University of Innsbruck, Austria
Dale Miller	Inria and LIX/Ecole Polytechnique, France
Sara Negri	University of Helsinki, Finland
Nicola Olivetti	LSIS, Aix-Marseille University, France
Jens Otten	University of Potsdam, Germany
Lawrence Paulson	University of Cambridge, UK
Nicolas Peltier	CNRS LIG, Grenoble, France

Andrei Popescu	Middlesex University, London, UK
Christophe Ringeissen	LORIA-Inria Nancy, France
Philipp Ruemmer	Uppsala University, Sweden
Masahiko Sakai	Nagoya University, Japan
Renate A. Schmidt	University of Manchester, UK
Roberto Sebastiani	University of Trento, Italy
Martina Seidl	Johannes Kepler University Linz, Austria
Viorica Sofronie-Stokkermans	Max Planck Institute for Informatics, Germany
Ashish Tiwari	SRI International, USA
Josef Urban	Radboud University, Nijmegen, The Netherlands
Christoph Weidenbach	Max Planck Institute for Informatics, Germany

Local Organizing Committee

Conference Chair

Pedro Quaresma	University of Coimbra, Portugal

Publicity Chair

Sandra Marques Pinto	University of Coimbra, Portugal

Workshops Chair

Reinhard Kahle	New University of Lisbon, Portugal

Local Organization

Nuno Baeta	Polytechnic Institute of Coimbra, Portugal
Carlos Caleiro	IST, University of Lisbon, Portugal
Nelma Moreira	University of Porto, Portugal
João Rasga	CMAF-CIO, University of Lisbon, Portugal
Vanda Santos	CISUC, University of Coimbra, Portugal

Additional Reviewers

E. Abraham
B. Afshari
S. Ahmetaj
P. Backeman
A. Bate
M. Bender
H. Bensaid
C. Benzmüller
M. Bilkova
J.C. Blanchette
F. Blanqui
M. Brenner
T. Brock-Nannestad
M. Bromberger
J. Brotherston
C. Brown
R. Bubel
R. Chadha
K. Chaudhuri
Chung-Kil Hur
C. Dragoi
B. Dutertre
G. Ebner
M. Echenim
S. Enqvist
J.C. Espírito Santo
M. Färber
B. Felgenhauer
M. Ferrari
A.E. Flores Montoya

P. Fontaine
P. Fournier
F. Frohn
J. Giráldez-Cru
N. Gorogiannis
A. Griggio
C. Haase
K. Hashimoto
J. Hensel
M. Hentschel
J. Hölzl
Z. Hou
U. Hustadt
J. Ilin
D. Jiang
S. Joosten
C. Kaliszyk
M. Kaminski
Y. Kazakov
W. Keller
M. Kerber
E. Kieronski
T. King
I. Konnov
T. Kotek
C. Kupke
T. Kutsia
R. Kuznets
P. Lammich
M. Lange
D. Larchey-Wendling
A. Leitsch
B. Lellmann
S. Lucas
A. Marshall
D. Mery
P.J. Meyer
J. Nagele
C. Nalon
N. Nishida
M. Ogawa
E. Orlandelli
D. Petrisan
E. Pimentel
G. Primiero
R. Ramanayake
G. Reis
A. Reynolds
R. Rowe
D. Rydeheard
A. Sangnier
M. Schiller
T. Schneider
S. Schulz
M. Suda
G. Sutcliffe
G. Sutre
R. Thiemann
T.K. Tran
P. Trentin
V. Van Oostrom
L. Vigneron
M. Villaret
M. Volpe
J. Von Plato
J. Vyskocil
U. Waldmann
H. Wansing
F. Wiedijk
T. Wies
B. Woltzenlogel Paleo
N. Zhang
A. Zeljić
D. Zufferey

IJCAR Steering Committee

Franz Baader	TU Dresden, Germany
Maria Paola Bonacina	Università degli Studi di Verona, Italy
Christian Fermüller	TU Wien, Austria
Stefan Hetzl	TU Wien, Austria
Nicola Olivetti	LSIS, University of Aix-Marseille, France
Jens Otten	University of Potsdam, Germany
Ashish Tiwari	SRI International, USA

Sponsors

University of Coimbra
CISUC, Centre for Informatics and Systems of the University of Coimbra
CMA.FCT.UNL Centre for Mathematics and Applications, FCT/UNL
CMUC, Centre for Mathematics, University of Coimbra
CMUP, Centre for Mathematics, University of Porto
IT, Instituto de Telecomunicações
FCT, Portuguese Foundation for Science and Technology
CMC, Câmara Municipal de Coimbra
Coimbra City Hall

Abstracts of Invited Talks

A Logical Framework for Developing and Mechanizing Set Theories

Arnon Avron

School of Computer Science, Tel Aviv University, 69978 Tel Aviv, Israel
aa@cs.tau.ac.il

Abstract. We describe a framework for formalizing mathematics which is based on the usual set theoretical foundations of mathematics. Its most important feature is that it reflects real mathematical practice in making an extensive use of statically defined abstract set terms, in the same way they are used in ordinary mathematical discourse. We also show how large portions of scientifically applicable mathematics can be developed in this framework in a straightforward way, using just rather weak set theories which are predicatively acceptable. The key property of those theories is that every object which is used in it is defined by some closed term of the theory. This allows for a very concrete, computationally-oriented interpretation. However, the development is not committed to such interpretation, and can easily be extended for handling stronger set theories, including *ZFC* itself.

Verification of Differential Private Computations

Gilles Barthe

IMDEA Software Institute, Madrid, Spain

Differential privacy [3, 4], is a statistical notion of privacy which achieves compelling trade-offs between input privacy and accuracy (of outputs). Differential privacy is also an attractive target for verification: despite their apparent simplicity, recently proposed algorithms have intricate privacy and accuracy proofs. We present two program logics for reasoning about privacy and accuracy properties of probabilistic computations. Our first program logic [2] is used for proving accuracy bounds and captures reasoning about the union bound, a simple but effective tool from probablility theory. Our second program logic [1] is used for proving privacy and captures fine-grained reasoning about probabilistic couplings [6, 8], a powerful tool for studying Markov chains. We illustrate the strengths of our program logics with novel and elegant proofs of challenging examples from differential privacy. Finally, we discuss the relationship between our approach and general-purpose frameworks for the verification of probabilistic programs, such as PPDL [5] and pGCL [7].

References

1. Barthe, G., Gaboardi, M., Grégoire, B., Hsu, J., Strub, P.: Proving differential privacy via probabilistic couplings. In: Proceedings of LICS 2016 (2016). http://arxiv.org/abs/1601.05047
2. Barthe, G., Gaboardi, M., Grégoire, B., Hsu, J., Strub, P.: A program logic for union bounds. CoRR, abs/1602.05681 (2016). http://arxiv.org/abs/1602.05681
3. Dwork, C.: Differential privacy. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006. LNCS, vol. 4052, pp. 1–12. Springer, Berlin (2006)
4. Dwork, C., McSherry, F., Nissim, K., Smith, A.: Calibrating noise to sensitivity in private data analysis. In: IACR Theory of Cryptography Conference (TCC), New York, New York, pp. 265–284 (2006). http://dx.doi.org/10.1007/11681878_14
5. Kozen, D.: A probabilistic PDL. J. Comput. Syst. Sci. **30**(2), 162–178 (1985). http://dx.doi.org/10.1016/0022-0000(85)90012-1. Preliminary version at STOC 1983
6. Lindvall, T.: Lectures on the Coupling Method. Courier Corporation (2002)
7. Morgan, C., McIver, A., Seidel, K.: Probabilistic predicate transformers. ACM Trans. Program. Lang. Syst. **18**(3), 325–353 (1996). doi: 10.1145/229542.229547
8. Thorisson, H.: Coupling, Stationarity, and Regeneration. Springer, New York (2000)

Programming by Examples: Applications, Algorithms, and Ambiguity Resolution

Sumit Gulwani

Microsoft Corporation, Redmond, WA, USA
sumitg@microsoft.com

Abstract. 99 % of computer end users do not know programming, and struggle with repetitive tasks. Programming by Examples (PBE) can revolutionize this landscape by enabling users to synthesize intended programs from example based specifications. A key technical challenge in PBE is to search for programs that are consistent with the examples provided by the user. Our efficient search methodology is based on two key ideas: (i) Restriction of the search space to an appropriate domain-specific language that offers balanced expressivity and readability (ii) A divide-and-conquer based deductive search paradigm that inductively reduces the problem of synthesizing a program of a certain kind that satisfies a given specification into sub-problems that refer to sub-programs or sub-specifications. Another challenge in PBE is to resolve the ambiguity in the example based specification. We will discuss two complementary approaches: (a) machine learning based ranking techniques that can pick an intended program from among those that satisfy the specification, and (b) active-learning based user interaction models. The above concepts will be illustrated using FlashFill, FlashExtract, and FlashRelate—PBE technologies for data manipulation domains. These technologies, which have been released inside various Microsoft products, are useful for data scientists who spend 80 % of their time wrangling with data. The Microsoft PROSE SDK allows easy construction of such technologies.

Logic and Proofs for Cyber-Physical Systems

André Platzer

Computer Science Department, Carnegie Mellon University, Pittsburgh, USA
aplatzer@cs.cmu.edu

Abstract. *Cyber-physical systems* (CPS) combine cyber aspects such as communication and computer control with physical aspects such as movement in space, which arise frequently in many safety-critical application domains, including aviation, automotive, railway, and robotics. But how can we ensure that these systems are guaranteed to meet their design goals, e.g., that an aircraft will not crash into another one?

This paper highlights some of the most fascinating aspects of cyberphysical systems and their dynamical systems models, such as hybrid systems that combine discrete transitions and continuous evolution along differential equations. Because of the impact that they can have on the real world, CPSs deserve proof as safety evidence.

Multi-dynamical systems understand complex systems as a combination of multiple elementary dynamical aspects, which makes them natural mathematical models for CPS, since they tame their complexity by compositionality. The family of *differential dynamic logics* achieves this compositionality by providing compositional logics, programming languages, and reasoning principles for CPS. Differential dynamic logics, as implemented in the theorem prover KeYmaera X, have been instrumental in verifying many applications, including the Airborne Collision Avoidance System ACAS X, the European Train Control System ETCS, automotive systems, mobile robot navigation, and a surgical robot system for skullbase surgery. This combination of strong theoretical foundations with practical theorem proving challenges and relevant applications makes *Logic for CPS* an ideal area for compelling and rewarding research.

Contents

Invited Talks

Satisfiability of Boolean Formulas

Satisfiability Modulo Theory

Rewriting

Arithmetic Reasoning and Mechanizing Mathematics

First-Order Logic and Proof Theory

First-Order Theorem Proving

Higher-Order Theorem Proving

Modal and Temporal Logics

Non-classical Logics

Verification