Preface

This volume contains the papers presented at the 24th International Conference on Automated Deduction (CADE-24), held June 9–14, 2013, in Lake Placid, New York, USA. CADE is the major forum for the presentation of research in all aspects of automated deduction, including foundations, applications, implementations, and practical experiences.

The Program Committee accepted 31 papers (22 full papers and 9 system descriptions) out of 71 submissions (53 full papers and 18 system descriptions). The acceptance rate was 43.66% overall, 41.51% for full papers, and 50% for system descriptions. Each submission was reviewed by at least three Program Committee (PC) members or external reviewers appointed by the PC members in charge. The main criteria for evaluation were originality and significance, technical quality and completeness, comparison with related work and completeness of references, quality of presentation, clarity, and readability.

The Best Paper Award was conferred to Radu Iosif (Verimag and CNRS, Grenoble, France), Adam Rogalewicz, and Jiri Simacek (Brno University of Technology, Czech Republic), for their paper entitled "The Tree Width of Separation Logic with Recursive Definitions," which proves decidability of satisfiability and entailment in an expressive fragment of separation logic, a logic relevant to program verification. According to separation logic experts who reviewed it, this paper closes in a creative and insightful way a problem that was open since 2004 and that was attacked unsuccessfully by several scholars.

The technical program of the conference included four invited talks by Jean-Christophe Filliâtre (CNRS and LRI Université Paris Sud XI, France), on "One Logic to Use Them All," Greg Morrisett (Harvard University, USA) on "Defining, Testing, and Reasoning About an x86 Decoder," Natarajan Shankar (SRI International, USA) on "Automated Reasoning, Fast and Slow," and Douglas R. Smith (Kestrel Institute and Kestrel Technology LLC, USA) on "Coalgebraic Specification and Refinement." This volume includes the invited papers by Jean-Christophe Filliâtre and Natarajan Shankar. The talk by Doug Smith focused on using coalgebraic concepts to specify the requirements on dynamical systems and then use deductive techniques to calculate refinements of the specifications into correct-by-construction code. The emphasis was on deduction for purposes of generating correct code rather than performing ad hoc verification on manually written code.

During the conference, the Herbrand Award for Distinguished Contributions to Automated Reasoning was presented to Greg Nelson for his invention of equality sharing, also known as the Nelson-Oppen method, and his pioneering work on theorem proving and program checking, including fast congruence closure algorithms and the Simplify theorem prover. The Selection Committee for the Herbrand Award consisted of the CADE-24 Program Committee members, the trustees of CADE Inc., and the Herbrand Award winners of the last ten years.

The conference issued a call for workshops out of which the following seven proposals were approved:

- Automated Deduction: Decidability, Complexity, Tractability (ADDCT) by Silvio Ghilardi, Ulrike Sattler, Viorica Sofronie-Stokkermans, and Ashish Tiwari
- Automated Reasoning in Security (ARSEC) by Paliath Narendran, Christopher A. Lynch, Andrew Marshall, and Dan Dougherty
- Empirically Successful Automated Reasoning with Artificial Intelligence (ESARAI) by Boris Konev, Stephan Schulz, and Geoff Sutcliffe
- Knowledge-Intensive Automated Reasoning (KInAR) by Ulrich Furbach and Björn Pelzer
- Methods for Modalities (M4M) by Carlos Areces
- Proof Exchange for Theorem Proving (PxTP) by Jasmin Christian Blanchette and Josef Urban
- The StarExec Web Service for the Evaluation of Logic Solvers (StarExec) by Aaron Stump, Geoff Sutcliffe, and Cesare Tinelli

Similarly, a call for tutorials generated the following five:

- Reasoning in Lightweight Description Logics, by Franz Baader
- Program Verification with the KeY System, by Bernhard Beckert and Reiner Hähnle
- Becoming a Power User of SMT: The CVC4 Solver, by Morgan Deters, Dejan Jovanović, Clark W. Barrett, and Cesare Tinelli
- State-of-the-art SAT Solving, by Marijn Heule
- The Twelf System, by Carsten Schürmann, Taus Brock-Nannestad, and Chris Martens

During the conference, the CADE-24 ATP System Competition – CASC-24 – was held, organized by Geoff Sutcliffe, who contributed the following description.

The CADE ATP System Competition (CASC) is an annual evaluation of fully automatic, classical logic automated theorem proving (ATP) systems – the world championship for such systems. Its main purpose is to provide a public evaluation of the relative capabilities of ATP systems. Additionally, CASC aims at stimulating ATP research, motivating development and implementation of robust, useful and easily deployable ATP systems, providing an inspiring environment for personal interaction between ATP researchers, and exposing ATP systems within and beyond the ATP community. Fulfillment of these objectives offers insight and stimulus for the development of more powerful ATP systems, leading to increased and more effective use. The CASC-24 web-site provides access to all systems and competition resources: `http://www.tptp.org/CASC/24`. CASC-24 was run in divisions according to problem and system characteristics:

- THF: Typed Higher-Order Form Theorems (axioms with a provable conjecture)
- TFA: Typed First-Order with Arithmetic Theorems (axioms with a provable conjecture)

- FOF: First-Order Form Theorems (axioms with a provable conjecture)
- FNT: First-Order Form Syntactically Non-propositional Non-theorems
- EPR: Effectively PRopositional Clause Normal Form Theorems and Non--theorems
- LTB: First-Order Form Theorems (axioms with a provable conjecture) from Large Theories, presented in Batches

In the THF, TFA, and EPR divisions, provers were ranked based on the number of problems solved, without being required to produce a proof or model. In the FOF, FNT, and LTB divisions, provers were ranked based on the number of problems solved with an acceptable proof or model output. The LTB division featured a 24-hour training period before the competition, during which systems could use a set of problems and solutions for tuning and training, but no human intervention was allowed. Problems for CASC-24 were taken from the TPTP Problem Library, using a version released after the start of the competition, so that new problems had not been seen by the entrants. Ties were broken according to the average time over problems solved.

Several students received Woody Bledsoe Travel Awards, thus named to remember the late Woody Bledsoe, funded by CADE Inc. to sponsor student participation. Best Paper Award winners, CASC divisions winners, and Woody Bledsoe Travel Awards recipients were announced during the banquet.

Many people contributed to making CADE-24 a success. I am very grateful to the members of the Program Committee and the external reviewers for carefully reviewing and evaluating the papers. On behalf of the Program Comittee, I thank Andrei Voronkov for the EasyChair system. I thank all authors who submitted papers, all participants of the conference, the invited speakers, the distinguished lecturers, the tutorial speakers, and the workshop organizers. CADE-24 would not have been possible without the dedicated work of the Organizing Committee. First and foremost, Neil Murray and Chris Lynch did a terrific job as Conference Chairs, planning and supervising all the conference events. Christoph Benzmüller and Peter Baumgartner were relentless as Workshop and Competition Chair, and Tutorial Chair, respectively. Heartfelt thanks go to Grant Olney Passmore for being such a proactive Publicity Chair, doing far more than the call of duty. I thank Geoff Sutcliffe for organizing CASC and also helping with publicity. Special thanks go to Catherine Zawadzki and the other personnel of the Crowne Plaza Hotel in Lake Placid, where all conference activities were held.

April 2013 Maria Paola Bonacina

Organization

Program Committee

Alessandro Armando	Università di Genova and FBK Trento, Italy
Peter Baumgartner	NICTA and Australian National University, Australia
Christoph Benzmüller	Freie Universität Berlin, Germany
Maria Paola Bonacina **(Chair)**	Università degli Studi di Verona, Italy
Cristina Borralleras	Universitat de Vic, Spain
Thierry Boy De La Tour	Université de Grenoble, France
Évelyne Contejean	CNRS and Université de Paris-Sud, France
Leonardo De Moura	Microsoft Research, USA
Stéphanie Delaune	École Normale Supérieure de Cachan, France
Clare Dixon	University of Liverpool, UK
Pascal Fontaine	Université de Lorraine and LORIA, France
Ulrich Furbach	Universität Koblenz-Landau, Germany
Ruben Gamboa	University of Wyoming, USA
Jürgen Giesl	RWTH Aachen, Germany
Paul B. Jackson	University of Edinburgh, UK
Predrag Janičić	Univerzitet u Beogradu, Serbia
Hélène Kirchner	INRIA Rocquencourt, France
Konstantin Korovin	University of Manchester, UK
K. Rustan M. Leino	Microsoft Research, USA
Christopher A. Lynch	Clarkson University, USA
César A. Muñoz	NASA Langley, USA
Neil V. Murray	University at Albany - SUNY, USA
Lawrence C. Paulson	University of Cambridge, UK
Frank Pfenning	Carnegie Mellon University, USA
Brigitte Pientka	McGill University, Canada
David A. Plaisted	University of North Carolina at Chapel Hill, USA
Christophe Ringeissen	LORIA and INRIA Nancy-Grand Est, France
Ulrike Sattler	University of Manchester, UK
Renate A. Schmidt	University of Manchester, UK
Manfred Schmidt-Schauß	J. W. Goethe Universität, Germany
Stephan Schulz	Technische Universität München, Germany
Viorica Sofronie-Stokkermans	Universität Koblenz-Landau and Max Planck Institut für Informatik, Germany
Ashish Tiwari	SRI International, USA
Uwe Waldmann	Max Planck Institut für Informatik, Germany
Christoph Weidenbach	Max Planck Institut für Informatik, Germany
Jian Zhang	Chinese Academy of Sciences, P.R. China

Organizing Committee

Conference Chairs:	Neil V. Murray University at Albany – SUNY, USA and Christopher A. Lynch Clarkson University, USA
Program Chair:	Maria Paola Bonacina Università degli Studi di Verona, Italy
Workshop and Competition Chair:	Christoph Benzmüller Freie Universität Berlin, Germany
Tutorial Chair:	Peter Baumgartner NICTA and Australian National University, Australia
Publicity Chair:	Grant Olney Passmore Cambridge University and Edinburgh University, UK

Additional Reviewers

Vincent Aravantinos
Mauricio Ayala-Rincón
Hicham Bensaid
Armin Biere
Nikolaj Bjørner
Bruno Blanchet
James Brotherston
Florian Bruse
Damien Doligez
Dan Dougherty
Vijay D'Silva
Mnacho Echenim
Vijay Ganesh
Rajeev Goré
Pieter Hooimeijer
Matthias Horbach
Ullrich Hustadt
Swen Jacobs
Yuncheng Jiang
Moa Johansson
Mark Kaminski
Mohammad Khodadadi
Patrick Koopmann
Pascal Lafourcade
Manuel Lamotte-Schubert
Daniel Le Berre
Etienne Lozes
Feifei Ma
Filip Marić
Andrew Matusiewicz
Charles Morisset
Anthony Narkawicz
Juan Antonio Navarro Pérez
Mladen Nikolić
Peter O'Hearn
Jens Otten
Fabio Papacchini
Grant Olney Passmore
Dirk Pattinson
Nicolas Peltier
Björn Pelzer
Florian Rabe
Silvio Ranise
Conrad Rau
Erik Rosenthal
Kristin Yvonne Rozier
Albert Rubio
Andrey Rybalchenko
David Sabel
Thomas Schneider
Mark E. Stickel
Adam Strzebonski
Thomas Sturm
Geoff Sutcliffe

Andreas Teucke
René Thiemann
Dmitry Tishkovsky
Dmitry Tsarkov
Heng Zhang
Wenhui Zhang

Board of Trustees of CADE Inc.

Franz Baader (President)	Technische Universität Dresden, Germany
Maria Paola Bonacina (PC Chair)	Università degli Studi di Verona, Italy
Amy Felty	University of Ottawa, Canada
Martin Giese (Secretary)	Universitetet i Oslo, Norway
Bernhard Gramlich	Technische Universität Wien, Austria
Neil V. Murray (Treasurer)	University at Albany - SUNY, USA
Lawrence C. Paulson	University of Cambridge, UK
Brigitte Pientka	McGill University, Canada
Renate A. Schmidt (Vice-President)	University of Manchester, UK
Viorica Sofronie-Stokkermans	Universität Koblenz-Landau and MPI für Informatik, Germany
Geoff Sutcliffe	University of Miami, USA
Christoph Weidenbach	MPI für Informatik, Germany

Board of the Association for Automated Reasoning

Martin Giese (Secretary)	Universitetet i Oslo, Norway
Neil V. Murray (CADE)	University at Albany - SUNY, USA
Hans Jürgen Ohlbach	Ludwig-Maximilians-Universität München, Germany
Brigitte Pientka (CADE)	McGill University, Canada
Larry Wos (President)	Argonne National Laboratory, USA

Sponsors

The CADE conference series is sponsored by CADE Inc., sub-corporation of the Association for Automated Reasoning. In addition, CADE-24 gratefully acknowledges support from the *Artificial Intelligence Journal* and Microsoft Research.

Table of Contents

One Logic To Use Them All

Jean-Christophe Filliâtre

[1] CNRS
[2] LRI, Univ. Paris-Sud, Orsay, F-91405
[3] INRIA Saclay – Île-de-France, Orsay, F-91893

The Tree Width of Separation Logic with Recursive Definitions

Radu Iosif[1], Adam Rogalewicz[2], and Jiri Simacek[2]

[1] Verimag/CNRS, Grenoble, France
[2] FIT, Brno University of Technology, IT4Innovations Centre of Excellence, Czech Republic

Hierarchic Superposition With Weak Abstraction

Peter Baumgartner[1] and Uwe Waldmann[2]

[1] NICTA* and Australian National University, Canberra, Australia
Peter.Baumgartner@nicta.com.au
[2] MPI für Informatik, Saarbrücken, Germany
uwe@mpi-inf.mpg.de

* NICTA is funded by the Australian Government as represented by the Department of Broadband, Communications and the Digital Economy and the Australian Research Council through the ICT Centre of Excellence program.

Completeness and Decidability Results for First-order Clauses with Indices*

Abdelkader Kersani and Nicolas Peltier

University of Grenoble (LIG, CNRS)

* This work has been partly funded by the project ASAP of the French *Agence Nationale de la Recherche* (ANR-09-BLAN-0407-01).

A Proof Procedure for Hybrid Logic with Binders, Transitivity and Relation Hierarchies

Marta Cialdea Mayer

Università di Roma Tre, Italy

Tractable Inference Systems: an Extension with a Deducibility Predicate

Hubert Comon-Lundh[1], Véronique Cortier[2], Guillaume Scerri[1 2]

[1] LSV, CNRS & ENS Cachan, France
[2] LORIA, CNRS, France

Computing Tiny Clause Normal Forms

Noran Azmy and Christoph Weidenbach

Max Planck Institute for Informatics

E-KRHyper 1.4: Extensions for Unique Names and Description Logic

Markus Bender, Björn Pelzer, Claudia Schon

Universität Koblenz-Landau, Institut für Informatik, 56070 Koblenz, Germany

Analyzing Vote Counting Algorithms Via Logic

And its Application to the CADE Election Scheme

Bernhard Beckert[1], Rajeev Goré[2], and Carsten Schürmann[3]

[1] Karlsruhe Institute of Technology beckert@kit.edu
[2] The Australian National University Rajeev.Gore@anu.edu.au
[3] IT University of Copenhagen carsten@itu.dk

Automated Reasoning, Fast and Slow*

Natarajan Shankar

Computer Science Laboratory, SRI International, Menlo Park, CA 94025, USA
shankar@csl.sri.com

* This work was supported by NSF Grant CSR-EHCS(CPS)-0834810, NASA Cooperative Agreement NNA10DE73C and by DARPA under agreement number FA8750-12-C-0284. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government. Sam Owre and Shalini Ghosh provided insightful feedback on earlier drafts of the paper.

Foundational Proof Certificates in First-Order Logic

Zakaria Chihani, Dale Miller, and Fabien Renaud

INRIA and LIX, Ecole Polytechnique, Palaiseau, France

Computation in Real Closed Infinitesimal and Transcendental Extensions of the Rationals

Leonardo de Moura[1] and Grant Olney Passmore[2]

[1] Microsoft Research, Redmond
[2] LFCS, Edinburgh and Clare Hall, Cambridge *

* Grant Passmore was supported by the EPSRC [EP/I011005/1 and EP/I010335/1] and by NSF EXPEDITION CNS-0926181.

A Symbiosis of Interval Constraint Propagation and Cylindrical Algebraic Decomposition*

Ulrich Loup[1], Karsten Scheibler[2], Florian Corzilius[1],
Erika Ábrahám[1], and Bernd Becker[2]

[1] RWTH Aachen University, Germany
[2] University of Freiburg, Germany

* This work has been partially supported by the German Research Council (DFG) as part of the Transregional Collaborative Research Center "AVACS" (SFB/TR 14, `http://www.avacs.org/` and the Research Training Group "AlgoSyn" (GRK 1298, `http://www.algosyn.rwth-aachen.de/`)

dReal: An SMT Solver for Nonlinear Theories over the Reals*

Sicun Gao, Soonho Kong, and Edmund M. Clarke

Carnegie Mellon University, Pittsburgh, PA 15213

* This research was sponsored by the National Science Foundation grants no. DMS1068829, no. CNS0926181 and no. CNS0931985, the GSRC under contract no. 1041377, the Semiconductor Research Corporation under contract no. 2005TJ1366, and the Office of Naval Research under award no. N000141010188.

Solving Difference Constraints over Modular Arithmetic

Graeme Gange, Harald Søndergaard, Peter J. Stuckey, and Peter Schachte

Department of Computing and Information Systems
The University of Melbourne, Victoria 3010, Australia

Asymmetric Unification: A New Unification Paradigm for Cryptographic Protocol Analysis*

Serdar Erbatur[1], Santiago Escobar[3], Deepak Kapur[4], Zhiqiang Liu[5], Christopher A. Lynch[5], Catherine Meadows[6], José Meseguer[7], Paliath Narendran[2], Sonia Santiago[3], and Ralf Sasse[8]

[1] Università degli Studi di Verona, serdar.erbatur@gmail.com
[2] University at Albany-SUNY, Albany, NY, USA, dran@cs.albany.edu
[3] DSIC-ELP, Universitat Politècnica de València, Spain
sescobar@dsic.upv.es,ssantiago@dsic.upv.es
[4] University of New Mexico, Albuquerque, NM, USA, kapur@cs.unm.edu
[5] Clarkson University, Potsdam, NY, USA
liuzh@clarkson.edu, clynch@clarkson.edu
[6] Naval Research Laboratory, Washington DC, USA, meadows@itd.nrl.navy.mil
[7] University of Illinois at Urbana-Champaign, USA, meseguer@illinois.edu
[8] Institute of Information Security, ETH Zurich, Switzerland,
ralf.sasse@inf.ethz.ch

* S. Escobar and S. Santiago were partially supported by EU (FEDER) and the Spanish MEC/MICINN under grant TIN 2010-21062-C02-02, and by Generalitat Valenciana PROMETEO2011/052. The following authors were partially supported by NSF: S. Escobar, J. Meseguer, and R. Sasse under CNS 09-04749 and CCF 09-05584 ; D. Kapur under CNS 09-05222; C. Lynch, Z. Liu, and C. Meadows under CNS 09-05378, and P. Narendran and S. Erbatur under CNS 09-05286. Part of the S. Erbatur's work was supported while with the Department of Computer Science, University at Albany, and part of R. Sasse's work was supported while with the Department of Computer Science, University of Illinois at Urbana-Champaign. Portions of this paper appeared in an abstract in the informal proceedings of UNIF'11.

Hierarchical Combination

Serdar Erbatur[1], Deepak Kapur[2], Andrew M Marshall[3], Paliath Narendran[4], and Christophe Ringeissen[5]

[1] Università degli Studi di Verona (Italy)
[2] University of New Mexico (USA)
[3] Naval Research Laboratory (USA)
[4] University at Albany, SUNY (USA)
[5] LORIA – INRIA Nancy-Grand Est (France)

PRocH: Proof Reconstruction for HOLLight

Cezary Kaliszyk and Josef Urban

[1] University of Innsbruck, Austria
[2] Radboud University Nijmegen

An Improved BDD Method for Intuitionistic Propositional Logic: the `BDDIntKt` System

Rajeev Goré and Jimmy Thomson

Logic and Computation Group, Australian National University

Towards Modularly Comparing Programs using Automated Theorem Provers

Chris Hawblitzel, Ming Kawaguchi, Shuvendu K. Lahiri, and Henrique Rebêlo

[1] Microsoft Research, Redmond, WA, USA
[2] University of California, San Diego
[3] Federal University of Pernambuco, Brazil

Reuse in Software Verification by Abstract Method Calls *

Reiner Hähnle[1], Ina Schäfer[2], and Richard Bubel[1]

[1] Department of Computer Science, Technische Universität Darmstadt
haehnle|bubel@cs.tu-darmstadt.de
[2] Institute for Software Engineering, Technische Universität Braunschweig
i.schaefer@tu-braunschweig.de

* Partly funded by the EU project FP7-231620 HATS and by the German Science Foundation (SCHA1635/2-1)

Dynamic Logic with Trace Semantics

Bernhard Beckert and Daniel Bruns*

Karlsruhe Institute of Technology (KIT), Germany

* This work has been supported by Deutsche Forschungsgemeinschaft (DFG) under project "Program-level Specification and Deductive Verification of Security Properties (DeduSec)" within SPP 1496 "Reliably Secure Software Systems (RS^3)".

Temporalizing Ontology-Based Data Access*

Franz Baader, Stefan Borgwardt, and Marcel Lippmann

TU Dresden, Germany,
{baader,stefborg,lippmann}@tcs.inf.tu-dresden.de

* Partially supported by DFG SFB 912 (HAEC) and GRK 1763 (QuantLA).

Verifying Refutations with Extended Resolution

Marijn J. H. Heule, Warren A. Hunt Jr., and Nathan Wetzler *

The University of Texas at Austin

* The authors are supported by DARPA contract number N66001-10-2-4087.

Hierarchical Reasoning and Model Generation for the Verification of Parametric Hybrid Systems

Viorica Sofronie-Stokkermans

University of Koblenz-Landau and Max-Planck-Institut für Informatik, Saarbrücken
e-mail: sofronie@uni-koblenz.de

Quantifier Instantiation Techniques for Finite Model Finding in SMT*

Andrew Reynolds[1], Cesare Tinelli[1], Amit Goel[2], Sava Krstić[2], Morgan Deters[3], and Clark Barrett[3]

[1] Department of Computer Science, The University of Iowa
[2] Strategic CAD Labs, Intel Corporation
[3] New York University

* The work of the first two authors was partially funded by a grant from Intel Corporation.

Automating Inductive Proofs using Theory Exploration

Koen Claessen, Moa Johansson, Dan Rosén, and Nicholas Smallbone

Department of Computer Science and Engineering, Chalmers University of Technology

The E-MaLeS 1.1 System

Daniel Kühlwein[1], Stephan Schulz[2], and Josef Urban[1]

[1] Radboud University Nijmegen, Nijmegen, Netherlands*,
[2] Technische Universität München, München, Germany

* The authors were supported by the NWO projects "MathWiki a Web-based Collaborative Authoring Environment for Formal Proofs" and "Learning2Reason".

TFF1: The TPTP Typed First-Order Form with Rank-1 Polymorphism

Jasmin Christian Blanchette[1] and Andrei Paskevich[2,3]

[1] Fakultät fr Informatik, Technische Universität München, Germany
[2] LRI, Université Paris-Sud, CNRS, France
[3] INRIA Saclay – Île-de-France, France

Propositional Temporal Proving with Reductions to a SAT Problem

Richard Williams and Boris Konev

Department of Computer Science, University of Liverpool, Liverpool L69 7ZF

InKreSAT: Modal Reasoning via Incremental Reduction to SAT

Mark Kaminski[1] and Tobias Tebbi[2]

[1] Department of Computer Science, University of Oxford, UK
[2] Saarland University, Saarbrcken, Germany

BV2EPR: A Tool for Polynomially Translating Quantifier-free Bit-Vector Formulas into EPR*

Gergely Kovásznai, Andreas Fröhlich, and Armin Biere

Institute for Formal Models and Verification
Johannes Kepler University, Linz, Austria

* Supported by FWF, NFN Grant S11408-N23 (RiSE).

The 481 Ways to Split a Clause and Deal with Propositional Variables

Kryštof Hoder and Andrei Voronkov

University of Manchester, Manchester, UK

Author Index