

Lecture Notes in Computer Science

2410

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Tokyo

Victor A. Carreño

César A. Muñoz Sofiène Tahar (Eds.)

Theorem Proving in Higher Order Logics

15th International Conference, TPHOLs 2002

Hampton, VA, USA, August 20-23, 2002

Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Victor A. Carreño
NASA Langley Research Center
MS 130, Hampton, VA 23681, USA
E-mail: v.a.carreno@larc.nasa.gov

César A. Muñoz
ICASE-Langley Research Center
MS 132C, Hampton, VA 23681, USA
E-mail: munoz@icase.edu

Sofiène Tahar
Concordia University, Electrical and Computer Engineering
1455 de Maisonneuve Blvd. W.
Montréal, Québec H3G 1M8, Canada
E-Mail: tahar@ece.concordia.ca

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Theorem proving in higher order logics : 15th international conference ;
proceedings / TPHOLs 2002, Hampton, VA, USA, August 20 - 23, 2002.
Victor A. Carreno (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ;
Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2410)
ISBN 3-540-44039-9

CR Subject Classification (1998): F.4.1, I.2.3, F.3.1, D.2.4, B.6.3

ISSN 0302-9743

ISBN 3-540-44039-9 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York,
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2002
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Christian Grosche, Hamburg
Printed on acid-free paper SPIN: 10873706 06/3142 5 4 3 2 1 0

Preface

This volume contains the proceedings of the *15th International Conference on Theorem Proving in Higher Order Logics* (TPHOLs 2002) held on 20–23 August 2002 in Hampton, Virginia, USA. The conference serves as a venue for the presentation of work in theorem proving in higher-order logics, and related areas in deduction, formal specification, software and hardware verification, and other applications.

Each of the 34 papers submitted in the full research category was refereed by at least three reviewers from the program committee or by a reviewer appointed by the program committee. Of these submissions, 20 papers were accepted for presentation at the conference and publication in this volume.

Following a well-established tradition in this conference series, TPHOLs 2002 also offered a venue for the presentation of work in progress. For the work in progress track, short introductory talks were given by researchers, followed by an open poster session for further discussion. Papers accepted for presentation in this track have been published as Conference Proceedings CP NASA-2002-211736.

The organizers would like to thank Ricky Butler and Gérard Huet for gracefully accepting our invitation to give talks at TPHOLs 2002. Ricky Butler was instrumental in the formation of the Formal Methods program at the NASA Langley Research Center and has led the group since its beginnings. The NASA Langley Formal Methods group, under Ricky Butler's guidance, has funded, been involved in, or influenced many formal verification projects in the US over more than two decades. In 1998 Gérard Huet received the prestigious Herbrand Award for his fundamental contributions to term rewriting and theorem proving in higher-order logic, as well as many other key contributions to the field of automated reasoning. He is the originator of the Coq System, under development at INRIA-Rocquencourt. Dr. Huet's current main interest is computational linguistics, however his work continues to influence researchers around the world in a wide spectrum of areas in theoretical computer science, formal methods, and software engineering.

The venue of the TPHOLs conference traditionally changes continent each year in order to maximize the likelihood that researchers from all over the world will attend. Starting in 1993, the proceedings of TPHOLs and its predecessor workshops have been published in the following volumes of the Springer-Verlag *Lecture Notes in Computer Science* series:

1993 (Canada)	780	1998 (Australia)	1479
1994 (Malta)	859	1999 (France)	1690
1995 (USA)	971	2000 (USA)	1869
1996 (Finland)	1125	2001 (UK)	2152
1997 (USA)	1275		

The 2002 conference was organized by a team from NASA Langley Research Center, the ICASE Institute at Langley Research Center, and Concordia University. Financial support came from Intel Corporation. The support of all these organizations is gratefully acknowledged.

August 2002

Víctor A. Carreño
César A. Muñoz

Organization

TPHOLs 2002 is organized by NASA Langley and ICASE in cooperation with Concordia University.

Organizing Committee

Conference Chair:	Víctor A. Carreño (NASA Langley)
Program Chair:	César A. Muñoz (ICASE, NASA LaRC)
	Sofiène Tahar (Concordia University)

Program Committee

Mark Aagaard (Waterloo)	Michael Kohlhase (CMU & Saarland)
David Basin (Freiburg)	Thomas Kropf (Bosch)
Víctor Carreño (NASA Langley)	Tom Melham (Glasgow)
Shiu-Kai Chin (Syracuse)	J Strother Moore (Texas, Austin)
Paul Curzon (Middlesex)	César Muñoz (ICASE, NASA LaRC)
Gilles Dowek (INRIA)	Sam Owre (SRI)
Harald Ganzinger (MPI Saarbrücken)	Christine Paulin-Mohring (INRIA)
Ganesh Gopalakrishnan (Utah)	Lawrence Paulson (Cambridge)
Jim Grundy (Intel)	Frank Pfenning (CMU)
Elsa Gunter (NJIT)	Klaus Schneider (Karlsruhe)
John Harrison (Intel)	Henny Sipma (Stanford)
Doug Howe (Carleton)	Konrad Slind (Utah)
Bart Jacobs (Nijmegen)	Don Syme (Microsoft)
Paul Jackson (Edinburgh)	Sofiène Tahar (Concordia)
Sara Kalvala (Warwick)	Wai Wong (Hong Kong Baptist)

Additional Reviewers

Otmane Ait-Mohamed	Alfons Geser	Harald Rueß
Behzad Akbarpour	Hanne Gottliebsen	Leon van der Torre
Nancy Day	Mike Kishinevsky	Tomas Uribe
Ben Di Vito	Hans de Nivelle	
Jean-Christophe Filliâtre	Andrew Pitts	

Invited Speakers

Ricky Butler (NASA Langley)
Gérard Huet (INRIA)

Sponsoring Institutions

NASA Langley

ICASE

Concordia University

INTEL

Table of Contents

Invited Talks

Formal Methods at NASA Langley	1
<i>Ricky Butler</i>	
Higher Order Unification 30 Years Later	3
<i>Gérard Huet</i>	

Regular Papers

Combining Higher Order Abstract Syntax with Tactical Theorem Proving and (Co)Induction	13
<i>Simon J. Ambler, Roy L. Crole, Alberto Momigiano</i>	
Efficient Reasoning about Executable Specifications in Coq	31
<i>Gilles Barthe, Pierre Courtieu</i>	
Verified Bytecode Model Checkers	47
<i>David Basin, Stefan Friedrich, Marek Gawkowski</i>	
The 5 Colour Theorem in Isabelle/Isar	67
<i>Gertrud Bauer, Tobias Nipkow</i>	
Type-Theoretic Functional Semantics	83
<i>Yves Bertot, Venanzio Capretta, Kuntal Das Barman</i>	
A Proposal for a Formal OCL Semantics in Isabelle/HOL	99
<i>Achim D. Brucker, Burkhart Wolff</i>	
Explicit Universes for the Calculus of Constructions	115
<i>Judicaël Courant</i>	
Formalised Cut Admissibility for Display Logic	131
<i>Jeremy E. Dawson, Rajeev Goré</i>	
Formalizing the Trading Theorem for the Classification of Surfaces	148
<i>Christophe Dehlinger, Jean-François Dufourd</i>	
Free-Style Theorem Proving	164
<i>David Delahaye</i>	
A Comparison of Two Proof Critics: Power vs. Robustness	182
<i>Louise A. Dennis, Alan Bundy</i>	

Two-Level Meta-reasoning in Coq	198
<i>Amy P. Felty</i>	
PuzzleTool: An Example of Programming Computation and Deduction ..	214
<i>Michael J.C. Gordon</i>	
A Formal Approach to Probabilistic Termination.....	230
<i>Joe Hurd</i>	
Using Theorem Proving for Numerical Analysis	246
<i>Micaela Mayero</i>	
Quotient Types: A Modular Approach	263
<i>Aleksey Nogin</i>	
Sequent Schema for Derived Rules	281
<i>Aleksey Nogin, Jason Hickey</i>	
Algebraic Structures and Dependent Records	298
<i>Virgile Prevosto, Damien Doligez, Thérèse Hardin</i>	
Proving the Equivalence of Microstep and Macrostep Semantics.....	314
<i>Klaus Schneider</i>	
Weakest Precondition for General Recursive Programs Formalized in Coq .	332
<i>Xingyuan Zhang, Malcolm Munro, Mark Harman, Lin Hu</i>	
Author Index	349