

Lecture Notes in Computer Science

1690

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

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Yves Bertot Gilles Dowek André Hirschowitz
Christine Paulin Laurent Théry (Eds.)

Theorem Proving in Higher Order Logics

12th International Conference, TPHOLs '99
Nice, France, September 14-17, 1999
Proceedings



Springer

Series Editors

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

Volume Editors

Yves Bertot
Gilles Dowek
Laurent Théry
INRIA Sophia Antipolis
2004 Route des Lucioles, F-06902 Sophia Antipolis Cedex, France

André Hirschowitz
University of Nice - Sophia Antipolis
Parc Valrose, F-06108 Nice Cedex 2, France

Christine Paulin
University of Paris XI
15, rue Georges Clemenceau, F-91405 Orsay Cedex, France

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Theorem proving in higher order logics : 12th international conference ; proceedings / TPHOLs '99, Nice, France, September 14 - 17, 1999 / Yves Bertot ... (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1690)
ISBN 3-540-66463-7

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

ISSN 0302-9743

ISBN 3-540-66463-7 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 1999
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10704460 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

This book contains the proceedings of *the 12th International Conference on Theorem Proving in Higher Order Logics* (TPHOLs'99), which was held in Nice at the University of Nice-Sophia Antipolis, September 14–17, 1999. Thirty-five papers were submitted as completed research, and each of them was refereed by at least three reviewers appointed by the program committee. Twenty papers were selected for publication in this volume.

Following a well-established tradition in this series of conferences, a number of researchers also came to discuss work in progress, using short talks and displays at a poster session. These papers are included in a supplementary proceedings volume. These supplementary proceedings take the form of a book published by INRIA in its series of research reports, under the following title : *Theorem Proving in Higher Order Logics: Emerging Trends 1999*.

The organizers were pleased that Dominique Bolignano, Arjeh Cohen, and Thomas Kropf accepted invitations to be guest speakers for TPHOLs'99. For several years, D. Bolignano has been the leader of the VIP team in the Dyade consortium between INRIA and Bull and is now at the head of a company *Trusted Logic*. His team has been concentrating on the use of formal methods for the effective verification of security properties for protocols used in electronic commerce. A. Cohen has had a key influence on the development of computer algebra in The Netherlands and his contribution has been of particular importance to researchers interested in combining the several known methods of using computers to perform mathematical investigations. T. Kropf is an important actor in the Europe-wide project PROSPER, which aims to deliver the benefits of mechanized formal analysis to system builders in industry. Altogether, these invited speakers gave us a panorama of applications for theorem proving and discussed its impact on the progress of scientific investigation as well as technological advances.

This year has confirmed the evolution of the conference from HOL-users' meeting to conference with a larger scope, spanning over uses of a variety of theorem proving systems, such as Coq, Isabelle, LAMBDA, LEGO, NuPrl, or PVS, as can be seen from the fact that the organizers do not belong to the HOL-user community.

Since 1993, the proceedings have been published by Springer-Verlag as Volumes 780, 859, 971, 1125, 1275, 1479, and 1690 of *Lecture Notes in Computer Science*. The conference was sponsored by the laboratory of mathematics of the University of Nice-Sophia Antipolis, Intel, France Télécom, and INRIA.

September 1999

Yves Bertot, Gilles Dowek,
André Hirschowitz, Christine Paulin,
Laurent Théry

Organization

Yves Bertot (INRIA)
Gilles Dowek (INRIA)
André Hirschowitz (Université de Nice)
Christine Paulin (Université de Paris-Sud)
Laurent Théry (INRIA)

Program Committee

Mark Aagaard (Intel)	Bart Jacobs (Nijmegen)
Sten Agerholm (IFAD)	Sara Kalvala (Warwick)
David Basin (Freiburg)	Tom Melham (Glasgow)
Yves Bertot (INRIA)	Paul Miner (NASA)
Richard Boulton (Edinburgh)	Malcolm Newey (ANU)
Gilles Dowek (INRIA)	Topbias Nipkow (Munich)
Mike Gordon (Cambridge)	Sam Owre (SRI)
Jim Grundy (ANU)	Christine Paulin-Mohring
Elsa Gunter (Lucent)	(Paris, <i>Chair</i>)
Joshua Guttman (Mitre)	Lawrence Paulson (Cambridge)
John Harrison (Intel)	Sofiéne Tahar (Concordia)
Doug Howe (Lucent)	

Invited Speakers

Dominique Bolignano (Trusted Logic)
Arjeh M. Cohen (T.U. Eindhoven)
Thomas Kropf (Tübingen)

Additional Reviewers

O. Ait-Mohamed	M.-S. Jahanpour	K. Sunesen
C. Ballarin	F. Kammüller	D. Syme
G. Bella	P. Lincoln	H. Tews
J. Courant	A. Mader	J. Thayer
P. Curzon	O. Müller	M. Wenzel
D. Cyrluk	A. Pitts	
P. Dybjer	E. Poll	
J.-C. Filliâtre	H. Rueß	

Table of Contents

Recent Advancements in Hardware Verification – How to Make Theorem Proving Fit for an Industrial Usage	1
<i>Thomas Kropf</i>	
Disjoint Sums over Type Classes in HOL	5
<i>Norbert Völker</i>	
Inductive Datatypes in HOL – Lessons Learned in Formal-Logic Engineering	19
<i>Stefan Berghofer and Markus Wenzel</i>	
Isomorphisms – A Link Between the Shallow and the Deep	37
<i>Thomas Santen</i>	
Polytypic Proof Construction	55
<i>Holger Pfeifer and Harald Rueß</i>	
Recursive Function Definition over Coinductive Types	73
<i>John Matthews</i>	
Hardware Verification Using Co-induction in COQ	91
<i>Solange Coupet-Grimal and Line Jakubiec</i>	
Connecting Proof Checkers and Computer Algebra Using <i>OpenMath</i>	109
<i>Olga Caprotti and Arjeh M. Cohen</i>	
A Machine-Checked Theory of Floating Point Arithmetic	113
<i>John Harrison</i>	
Universal Algebra in Type Theory	131
<i>Venanzio Capretta</i>	
Locales – A Sectioning Concept for Isabelle	149
<i>Florian Kammüller, Markus Wenzel, and Lawrence C. Paulson</i>	
Isar – A Generic Interpretative Approach to Readable Formal Proof Documents	167
<i>Markus Wenzel</i>	
On the Implementation of an Extensible Declarative Proof Language	185
<i>Vincent Zammitt</i>	
Three Tactic Theorem Proving	203
<i>Don Syme</i>	

Mechanized Operational Semantics via (Co)Induction	221
<i>Simon J. Ambler and Roy L. Crole</i>	
Representing WP Semantics in Isabelle/ZF	239
<i>Mark Staples</i>	
A HOL Conversion for Translating Linear Time Temporal Logic to ω -Automata	255
<i>Klaus Schneider and Dirk W. Hoffmann</i>	
From I/O Automata to Timed I/O Automata	273
<i>Bernd Grobauer and Olaf Müller</i>	
Formal Methods and Security Evaluation (<i>Invited Talk</i>)	291
<i>Dominique Bolignano</i>	
Importing MDG Verification Results into HOL	293
<i>Haiyan Xiong, Paul Curzon, and Sofiéne Tahar</i>	
Integrating Gandalf and HOL	311
<i>Joe Hurd</i>	
Lifted-FL: A Pragmatic Implementation of Combined Model Checking and Theorem Proving	323
<i>Mark D. Aagaard, Robert B. Jones, and Carl-Johan H. Seger</i>	
Symbolic Functional Evaluation	341
<i>Nancy A. Day and Jeffrey J. Joyce</i>	
Author Index	359