

Lecture Notes in Computer Science

1275

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

Advisory Board: W. Brauer D. Gries J. Stoer

Elsa L. Gunter Amy Felty (Eds.)

Theorem Proving in Higher Order Logics

10th International Conference, TPHOLs '97
Murray Hill, NJ, USA, August 19-22, 1997
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Elsa L. Gunter

Amy Felty

Lucent Technologies, Bell Labs Innovations

600 Mountain Avenue, Murray Hill, NJ 07974-0636, USA

E-mail: (elsa/felty)@research.bell-labs.com

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Theorem proving in higher order logics : 10th international conference ; proceedings / TPHOLS '97, Murray Hill, NJ, USA, August 19 - 22, 1997 / Elsa L. Gunter ; Amy Felty (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1997

ISBN 3-540-63379-0

CR Subject Classification (1991): B.6.3, D.2.4, F.3.1, F.4.1, I.2.3

ISSN 0302-9743

ISBN 3-540-63379-0 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 1997

Printed in Germany

Typesetting: Camera-ready by author

SPIN 10547850 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

This volume contains the proceedings of the tenth international conference on *Theorem Proving in Higher Order Logics* (TPHOLs97), held at Bell Laboratories, Lucent Technologies, in Murray Hill, New Jersey, USA, during August 19-22, 1997. The previous meetings in this series were known initially as HOL Users Meetings, and later as Workshops on Higher Order Logic Theorem Proving and its Applications. The name Theorem Proving in Higher Order Logics was adopted for the first time last year to reflect a broadening in scope of the conference, which now encompasses work related to all aspects of theorem proving in higher order logics, particularly when based on a secure mechanization of those logics. These proceedings include papers describing work in Coq, HOL, Isabelle, LEGO, and PVS theorem provers.

The thirty-two papers submitted this year were generally of high quality. All submissions were fully refereed, each paper being reviewed by at least three reviewers appointed by the program committee (generally members of the committee themselves). Nineteen papers were selected for presentation as full research contributions. These are the papers appearing in this volume. The conference also continued its tradition of providing an open venue for the discussion and sharing of preliminary results and work in progress. Thus, the program included two informal poster sessions where twelve researchers were invited to present their work.

The organizers were pleased that Professor Robert L. Constable, Professor Deepak Kapur, and Dr. Doron Peled accepted invitations to be guest speakers at the conference. All three invited speakers also very kindly produced a written abstract or extended abstract of their talk for inclusion in these proceedings.

The conference was sponsored by Bell Laboratories, Lucent Technologies, and by the Department of Computer and Information Science of the University of Pennsylvania. We also want to thank Jennifer MacDougall who assisted in matters of local organization.

June 1997

Elsa L. Gunter
Amy Felty

Conference Organization

Conference Chair:

Elsa L. Gunter (Bell Labs, Lucent)

Organizing Committee:

Amy Felty (Bell Labs, Lucent)
Elsa L. Gunter (Bell Labs, Lucent)

Program Committee:

Flemming Andersen (Tele Danmark)	Sara Kalvala (U. Warwick)
Yves Bertot (INRIA, Sophia)	Tom Melham (U. Glasgow)
Albert Camilleri (Hewlett-Packard)	Malcolm Newey (ANU)
Bill Farmer (MITRE)	Tobias Nipkow (TU München)
Amy Felty (Bell Labs, Lucent)	Christine Paulin-Mohring (ENS Lyon)
Elsa Gunter (Bell Labs, Lucent)	Larry Paulson (U. Cambridge)
Joshua Guttman (MITRE)	Tom Schubert (Portland State U.)
John Harrison (U. Cambridge)	Phil Windley (BYU)
John Herbert (SRI)	Jockum von Wright (Åbo Akademi)
Doug Howe (Bell Labs, Lucent)	

Invited Speakers:

Robert L. Constable (Cornell U.)
Deepak Kapur (SUNY - Albany)
Doron Peled (Bell Labs, Lucent)

Additional Referees:

Robert Beers	J. Kelly Flanagan	Michael Norrish
Paul E. Black	Ranan Fraer	Maris A. Ozols
Annette Bunker	A. D. Gordon	Mark Steedman
P. Chartier	Jim Grundy	Javier Thayer
Graham Collins	Michael Jones	Myra VanInwegen
Katherine Eastaughffe	Trent Larson	John Van Tassel

Contents

An Isabelle-Based Theorem Prover for VDM-SL <i>Sten Agerholm and Jacob Frost</i>	1
Executing Formal Specifications by Translation to Higher Order Logic Programming <i>James H. Andrews</i>	17
Human-Style Theorem Proving Using PVS <i>Myla Archer and Constance Heitmeyer</i>	33
A Hybrid Approach to Verifying Liveness in a Symmetric Multi-Processor <i>Albert J. Camilleri</i>	49
Formal Verification of Concurrent Programs in LP and in COQ: A Comparative Analysis <i>Bouthaina Chetali and Barbara Heyd</i>	69
<i>Invited paper:</i> ML Programming in Constructive Type Theory <i>Robert L. Constable</i>	87
Possibly Infinite Sequences in Theorem Provers: A Comparative Study <i>Marco Devillers, David Griffioen, and Olaf Müller</i>	89
Proof Normalization for a First-Order Formulation of Higher-Order Logic <i>Gilles Dowek</i>	105
Using a PVS Embedding of CSP to Verify Authentication Protocols <i>Bruno Dutertre and Steve Schneider</i>	121
Verifying the Accuracy of Polynomial Approximations in HOL <i>John Harrison</i>	137
A Full Formalisation of π -Calculus Theory in the Calculus of Constructions <i>Daniel Hirschhoff</i>	153
<i>Invited paper:</i> Rewriting, Decision Procedures and Lemma Speculation for Automated Hardware Verification <i>Deepak Kapur</i>	171
Refining Reactive Systems in HOL Using Action Systems <i>Thomas Långbacka and Joakim von Wright</i>	183

On Formalization of Bicategory Theory <i>Takahisa Mohri</i>	199
Towards an Object-Oriented Prologification Language <i>Wolfgang Naraschewski</i>	215
<i>Invited paper:</i> Verification for Robust Specification <i>Doron Peled</i>	231
A Theory of Structured Model-Based Specifications in Isabelle/HOL <i>Thomas Santen</i>	243
Proof Presentation for Isabelle <i>Martin Simons</i>	259
Derivation and Use of Induction Schemes in Higher-Order Logic <i>Konrad Slind</i>	275
Higher Order Quotients and their Implementation in Isabelle HOL <i>Oscar Slotosch</i>	291
Type Classes and Overloading in Higher-Order Logic <i>Markus Wenzel</i>	307
A Comparative Study of Coq and HOL <i>Vincent Zammit</i>	323
Author Index	339