

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*University of Dortmund, Germany*

Madhu Sudan

*Massachusetts Institute of Technology, MA, USA*

Demetri Terzopoulos

*New York University, NY, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Moshe Y. Vardi

*Rice University, Houston, TX, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Konrad Slind Annette Bunker  
Ganesh Gopalakrishnan (Eds.)

# Theorem Proving in Higher Order Logics

17th International Conference, TPHOLs 2004  
Park City, Utah, USA, September 14-17, 2004  
Proceedings

## Volume Editors

Konrad Slind  
Ganesh Gopalakrishnan  
University of Utah  
School of Computing  
50 South Central Campus Drive, Salt Lake City, Utah, UT84112, USA  
E-mail: {slind;ganesh}@cs.utah.edu

Annette Bunker  
Utah State University  
Electrical and Computer Engineering Department  
4120 Old Main Hill, Logan, UT 84341, USA  
E-mail: bunker@helios.ece.usu.edu

Library of Congress Control Number: 2004111288

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

ISSN 0302-9743

ISBN 3-540-23017-3 Springer 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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2004  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik  
Printed on acid-free paper      SPIN: 11319238      06/3142      5 4 3 2 1 0

# Preface

This volume constitutes the proceedings of the *17th International Conference on Theorem Proving in Higher Order Logics* (TPHOLs 2004) held September 14–17, 2004 in Park City, Utah, USA. TPHOLs covers all aspects of theorem proving in higher-order logics as well as related topics in theorem proving and verification.

There were 42 papers submitted to TPHOLs 2004 in the full research category, each of which was refereed by at least 3 reviewers selected by the program committee. Of these submissions, 21 were accepted for presentation at the conference and publication in this volume. In keeping with longstanding tradition, TPHOLs 2004 also offered a venue for the presentation of work in progress, where researchers invited discussion by means of a brief introductory talk and then discussed their work at a poster session. A supplementary proceedings containing papers about in-progress work was published as a 2004 technical report of the School of Computing at the University of Utah.

The organizers are grateful to Al Davis, Thomas Hales, and Ken McMillan for agreeing to give invited talks at TPHOLs 2004.

The TPHOLs conference traditionally changes continents each year in order to maximize the chances that researchers from around the world can attend. Starting in 1993, the proceedings of TPHOLs and its predecessor workshops have been published in the Springer Lecture Notes in Computer Science series:

1993 (Canada)	Vol. 780	1999 (France)	Vol. 1690
1994 (Malta)	Vol. 859	2000 (USA)	Vol. 1869
1995 (USA)	Vol. 971	2001 (UK)	Vol. 2152
1996 (Finland)	Vol. 1125	2002 (USA)	Vol. 2410
1997 (USA)	Vol. 1275	2003 (Italy)	Vol. 2758
1998 (Australia)	Vol. 1479	2004 (USA)	Vol. 3223

We would like to thank Amber Chisholm and Perry Hacker of University of Utah Conference Services for their help in many aspects of organizing and running TPHOLs.

Finally, we thank our sponsors: Intel and the National Science Foundation.

June 2004

Konrad Slind,  
Annette Bunker,  
and Ganesh Gopalakrishnan

## Program Committee

Mark Aagaard (Waterloo)  
David Basin (Zurich)  
Ching-Tsun Chou (Intel)  
Peter Dybjer (Chalmers)  
Jean-Christophe Filliâtre (Paris Sud)  
Mike Gordon (Cambridge)  
Elsa Gunter (NJIT)  
Jason Hickey (Caltech)  
Doug Howe (Carleton)  
Bart Jacobs (Nijmegen)  
Matt Kaufmann (AMD)  
Tom Melham (Oxford)  
Tobias Nipkow (München)  
Christine Paulin-Mohring (Paris Sud)  
Frank Pfenning (CMU)  
Sofène Tahar (Concordia)

Clark Barrett (NYU)  
Yves Bertot (INRIA)  
Thierry Coquand (Chalmers)  
Amy Felty (Ottawa)  
Jacques Fleuriot (Edinburgh)  
Jim Grundy (Intel)  
John Harrison (Intel)  
Peter Homeier (DoD, USA)  
Paul Jackson (Edinburgh)  
Sara Kalvala (Warwick)  
Thomas Kropf (Bosch)  
César Muñoz (NASA)  
Sam Owre (SRI)  
Lawrence Paulson (Cambridge)  
Konrad Slind (Utah)  
Burkhardt Wolff (Freiburg)

## Additional Referees

Stefan Berghofer  
Sylvain Conchon  
Christophe Dehlinger  
Lucas Dixon  
Alfons Geser  
Ali Habibi  
Felix Klaedtke  
Mohamed Layouni  
Nicolas Magaud

Holger Pfeifer  
Sylvan Pinsky  
Tom Ridge  
Norbert Schirmer  
Carsten Schürmann  
Radu I. Siminiceanu  
Laurent Théry  
Luca Viganò  
Martin Wildmoser

# Table of Contents

Error Analysis of Digital Filters Using Theorem Proving .....	1
<i>Behzad Akbarpour and Sofiène Tahar</i>	
Verifying Uniqueness in a Logical Framework .....	18
<i>Penny Anderson and Frank Pfenning</i>	
A Program Logic for Resource Verification .....	34
<i>David Aspinall, Lennart Beringer, Martin Hofmann, Hans-Wolfgang Loidl, and Alberto Momigiano</i>	
Proof Reuse with Extended Inductive Types .....	50
<i>Olivier Boite</i>	
Hierarchical Reflection .....	66
<i>Luís Cruz-Filipe and Freek Wiedijk</i>	
Correct Embedded Computing Futures .....	82
<i>Al Davis</i>	
Higher Order Rippling in ISAPLANNER .....	83
<i>Lucas Dixon and Jacques Fleuriot</i>	
A Mechanical Proof of the Cook-Levin Theorem .....	99
<i>Ruben Gamboa and John Cowles</i>	
Formalizing the Proof of the Kepler Conjecture .....	117
<i>Thomas Hales</i>	
Interfacing Hoare Logic and Type Systems for Foundational Proof-Carrying Code .....	118
<i>Nadeem Abdul Hamid and Zhong Shao</i>	
Extensible Hierarchical Tactic Construction in a Logical Framework .....	136
<i>Jason Hickey and Aleksey Nogin</i>	
Theorem Reuse by Proof Term Transformation .....	152
<i>Einar Broch Johnsen and Christoph Lüth</i>	
Proving Compatibility Using Refinement .....	168
<i>Michael Jones, Aaron Benson, and Dan Delorey</i>	
Java Program Verification via a JVM Deep Embedding in ACL2 .....	184
<i>Hanbing Liu and J. Strother Moore</i>	

Reasoning About CBV Functional Programs in Isabelle/HOL .....	201
<i>John Longley and Randy Pollack</i>	
Proof Pearl: From Concrete to Functional Unparsing .....	217
<i>Jean-François Monin</i>	
A Decision Procedure for Geometry in Coq.....	225
<i>Julien Narboux</i>	
Recursive Function Definition for Types with Binders.....	241
<i>Michael Norrish</i>	
Abstractions for Fault-Tolerant Distributed System Verification .....	257
<i>Lee Pike, Jeffrey Maddalon, Paul Miner, and Alfons Geser</i>	
Formalizing Integration Theory with an Application to Probabilistic Algorithms.....	271
<i>Stefan Richter</i>	
Formalizing Java Dynamic Loading in HOL .....	287
<i>Tian-jun Zuo, Jun-gang Han, and Ping Chen</i>	
Certifying Machine Code Safety: Shallow Versus Deep Embedding.....	305
<i>Martin Wildmoser and Tobias Nipkow</i>	
Term Algebras with Length Function and Bounded Quantifier Alternation.....	321
<i>Ting Zhang, Henny B. Sipma, and Zohar Manna</i>	
<b>Author Index .....</b>	<b>337</b>