

Lecture Notes in Computer Science

1125

J. von Wright J. Grundy J. Harrison (Eds.)

Theorem Proving in Higher Order Logics

9th International Conference, TPHOLs'96
Turku, Finland, August 1996
Proceedings



Springer

Lecture Notes in Computer Science

1125

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

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

Springer

Berlin

Heidelberg

New York

Barcelona

Budapest

Hong Kong

London

Milan

Paris

Santa Clara

Singapore

Tokyo

J. von Wright J. Grundy J. Harrison (Eds.)

Theorem Proving in Higher Order Logics

9th International Conference, TPHOLs'96
Turku, Finland, August 26-30, 1996
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Joakim von Wright

Jim Grundy

John Harrison

Åbo Akademi University, Department of Computer Science

Lemminkäinengatan 14A, 20520 Turku, Finland

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Theorem proving in higher order logics : 9th international conference ; proceedings / TPHOL '96, Turku, Finland, August 26 - 30, 1996 / J. von Wright ... (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1996 (Lecture notes in computer science ; Vol. 1125)

ISBN 3-540-61587-3

NE: Wright, Joakim von [Hrsg.]; TPHOL <9, 1996, Turku>; GT

CR Subject Classification (1991): B.6.3, D.2.4, F3.1, F.4.1, I.2.3

ISSN 0302-9743

ISBN 3-540-61587-3 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 1996

Printed in Germany

Typesetting: Camera-ready by author

SPIN 10513526 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

This volume contains the proceedings of the *The 9th International Conference on Theorem Proving in Higher Order Logics* (TPHOLs'96). The previous meetings in the series were known initially as HOL Users Meetings, and later as Workshops on Higher Order Logic Theorem Proving and its Applications. The new name for the series reflects a broadening in scope of the conferences, which now encompass work related to all aspects of theorem proving in higher order logics, particularly when based on a secure mechanization of logic. As a sign of the broad scope of the conference, these proceedings contain papers describing work using the Alf, Coq, HOL, Isabelle, LAMBDA, LEGO, NuPrl, and PVS theorem provers.

The forty-six papers submitted to TPHOLs'96 were generally of high standard. All submissions were fully refereed, each paper being read by at least three reviewers appointed by the programme committee. Twenty-seven papers were selected for presentation as full research contributions. These are the papers contained in this volume. The conference also continued the tradition of its predecessors of providing an open venue for the discussion and sharing of preliminary results. Thus the programme included an informal poster session where twenty researchers were invited to present their work. The poster papers are available in a supplementary proceedings produced as a General Publication of the Turku Centre for Computer Science (TUCS).

The organizers are pleased that Mike Gordon and Andrzej Trybulec accepted invitations to be guest speakers at the conference. In addition to the two invited lectures, the conference also included two tutorials, by Paul Jackson and Christine Paulin-Mohring.

The conference was sponsored by the Turku Centre for Computer Science, the Research Institute of the Foundation of Åbo Akademi, and the Academy of Finland. Their financial support is gratefully acknowledged. We also want to thank Christel Engblom, Sirpa Nummila, and Gundel Westerholm who assisted in matters of local organization.

August 1996

Joakim von Wright
Jim Grundy
John Harrison

Conference Organization

Conference Chair:

Joakim von Wright (Åbo Akademi)

Programme Committee:

Flemming Andersen (Tele Danmark)	Paul Loewenstein (Sun)
Albert Camilleri (Hewlett-Packard)	Tom Melham (U. Glasgow)
Tony Cant (DSTO)	Tobias Nipkow (TU München)
Elsa Gunter (AT&T)	Christine Paulin (ENS Lyon)
Joshua Guttman (MITRE)	Larry Paulson (U. Cambridge)
John Herbert (SRI)	Tom Schubert (Portland State U.)
Paul Jackson (U. Edinburgh)	David Shepherd (SGS-THOMSON)
Ramayya Kumar (FZI Karlsruhe)	Phil Windley (BYU)
Tim Leonard (DEC)	Joakim von Wright (Åbo Akademi)

Organizing Committee:

Jim Grundy (Åbo Akademi)
 John Harrison (Åbo Akademi)
 Joakim von Wright (Åbo Akademi)

Invited Speakers:

Mike Gordon (U. Cambridge)
 Andrzej Trybulec (U. Warsaw, Białystok)

Tutorial Speakers:

Paul Jackson (U. Edinburgh)
 Christine Paulin (ENS Lyon)

Additional Referees:

David Basin	Andrew Gordon	Chris Owens
Paul E. Black	Jim Grundy	Maris Ozols
Rosina Bignall	Kelly Hall	Kim Dam Petersen
Christian Blumenröhr	John Harrison	Jimmi S. Pettersson
Annette Bunker	Michael Jones	Christian Prehofer
Roy L. Crole	Trent Larson	Emil Sekerinski
Anthony Dekker	Thomas Långbacka	Kaisa Sere
Katherine Eastaughffe	Brendan Mahony	Donald Syme
Dirk Eisenbiegler	Michael Norrish	Marina Waldén
Jens Chr. Godskesen		

Contents

Translating Specifications in VDM-SL to PVS	1
<i>S. Agerholm</i>	
A Comparison of HOL and ALF Formalizations of a Categorical Coherence Theorem	17
<i>S. Agerholm, I. Beylin, P. Dybjer</i>	
Modeling a Hardware Synthesis Methodology in Isabelle	33
<i>D. Basin, S. Friedrich</i>	
Inference Rules for Programming Languages with Side Effects in Expressions	51
<i>P. E. Black, P. J. Windley</i>	
Deciding Cryptographic Protocol Adequacy with HOL: The Implementation	61
<i>S. H. Brackin</i>	
Proving Liveness of Fair Transition Systems	77
<i>H. Busch</i>	
Program Derivation Using the Refinement Calculator	93
<i>M. Butler, T. Långbacka</i>	
A Proof Tool for Reasoning About Functional Programs	109
<i>G. Collins</i>	
Coq and Hardware Verification: A Case Study	125
<i>S. Coupet-Grimal, L. Jakubiec</i>	
Elements of Mathematical Analysis in PVS	141
<i>B. Dutertre</i>	
Implementation Issues About the Embedding of Existing High Level Synthesis Algorithms in HOL	157
<i>D. Eisenbiegler, C. Blumenröhr, R. Kumar</i>	
Five Axioms of Alpha-Conversion	173
<i>A. D. Gordon, T. Melham</i>	
Set Theory, Higher Order Logic or Both?	191
<i>M. Gordon</i>	
A Mizar Mode for HOL	203
<i>J. Harrison</i>	

Stålmarck's Algorithm as a HOL Derived Rule	221
<i>J. Harrison</i>	
Towards Applying the Composition Principle to Verify a Microkernel Operating System	235
<i>M. R. Heckman, C. Zhang, B. R. Becker, D. Peticolas, K. N. Levitt, R. A. Olsson</i>	
A Modular Coding of Unity in Coq	251
<i>B. Heyd, P. Crégut</i>	
Importing Mathematics from HOL into Nuprl	267
<i>D. J. Howe</i>	
A Structure Preserving Encoding of Z in Isabelle/HOL	283
<i>Kolyang, T. Santen, B. Wolff</i>	
Improving the Result of High-Level Synthesis Using Interactive Transformational Design	299
<i>M. Larsson</i>	
Using Lattice Theory in Higher Order Logic	315
<i>L. Laibinis</i>	
Formal Verification of Algorithm W: The Monomorphic Case	331
<i>D. Nazareth, T. Nipkow</i>	
Verification of Compiler Correctness for the WAM	347
<i>C. Pusch</i>	
Synthetic Domain Theory in Type Theory: Another Logic of Computable Functions	363
<i>B. Reus</i>	
Function Definition in Higher Order Logic	381
<i>K. Slind</i>	
Higher Order Annotated Terms for Proof Search	399
<i>A. Smaill, I. Green</i>	
A Comparison of MDG and HOL for Hardware Verification	415
<i>S. Tahar, P. Curzon</i>	
A Mechanisation of Computability Theory in HOL	431
<i>V. Zammit</i>	
AUTHOR INDEX	447