

Lecture Notes in Computer Science

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

1479

Jim Grundy Malcolm Newey (Eds.)

Theorem Proving in Higher Order Logics

11th International Conference, TPHOLs '98
Canberra, Australia
September 27 – October 1, 1998
Proceedings



Springer

Series Editors

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

Volume Editors

Jim Grundy
Malcolm Newey
The Australian National University, Department of Computer Science
Canberra ACT 0200, Australia
E-mail: {Jim.Grundy,Malcolm.Newey}@anu.edu.au

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

**Theorem proving in higher order logics : 11th international conference ; proceedings / TPHOLs '98, Canberra, Australia, September 27 - October 2, 1998 / Jim Grundy ; Malcolm Newey (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1998 (Lecture notes in computer science ; Vol. 1479)
ISBN 3-540-64987-5**

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

ISSN 0302-9743

ISBN 3-540-64987-5 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 1998
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10638740 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

This volume contains the proceedings of *The 11th International Conference on Theorem Proving in Higher Order Logics* (TPHOLs'98), which was held in Canberra at The Australian National University, between September 27 and October 2, 1998. Each of the fifty-two papers submitted as completed research contributions was refereed by at least three reviewers appointed by the program committee. Because of the limited space in the program and proceedings, only twenty-six could be accepted for publication in this volume. The competition was tough, and many good papers were unsuccessful.

TPHOLs'98 continues the tradition of its predecessors in providing a venue for the presentation of work in progress, where researchers invite discussion of preliminary results by means of a short talk, a display at a poster session, and inclusion of a paper in a supplementary proceedings. For TPHOLs'98, the supplementary proceedings takes the form of a book entitled *Theorem Proving in Higher Order Logics: Emerging Trends, 1998* and published by the Computer Science Department of The Australian National University,

The invited speakers for TPHOLs'98 were Tobias Nipkow and Joakim von Wright; the organizers were delighted that both accepted the invitation and provided original papers for inclusion in the proceedings. Professor Nipkow plays a leading role in the Isabelle community, while Dr. von Wright is noted for his contributions both to theorem proving in higher order logics and to the area of program refinement. This is particularly pertinent since TPHOLs'98 was run in federation with *The 1998 International Refinement Workshop and Formal Methods Pacific* (IRW/FMP'98).

Although the TPHOLs conferences have their genesis in HOL Users Meetings, recent years have seen a high rate of contribution from the other major groups, particularly the user communities of Coq, Isabelle, LAMBDA, LEGO, NuPrl, and PVS. Since 1993 the proceedings have been published by Springer as Volumes 780, 859, 971, 1125, 1275, and 1479 of *Lecture Notes in Computer Science*. More history of TPHOLs can be found with further information about the 1998 event at <http://cs.anu.edu.au/TPHOLs98/>.

The conference was sponsored by the Computer Science Department of The Australian National University (ANU), Intel, the Defence Science and Technology Organisation (DSTO), The Australian Research Council, and ACSys (the Cooperative Research Centre for Advanced Computational Systems). The financial support of these groups is gratefully acknowledged.

Canberra, September 1998

Jim Grundy and Malcolm Newey

Conference Organisation

Jim Grundy (ANU)
Malcolm Newey (ANU)

Program Committee

Mark Aagaard (Intel)	Paul Jackson (Edinburgh)
Sten Agerholm (IFAD)	Sara Kalvala (Warwick)
David Basin (Freiburg)	Thomas Kropf (Karlsruhe)
Richard Boulton (Edinburgh)	Tim Leonard (Compaq)
Albert Camilleri (HP)	Paul Loewenstein (Sun)
Tony Cant (DSTO)	Tom Melham (Glasgow)
Robert Constable (Cornell)	Paul Miner (NASA)
Gilles Dowek (INRIA)	Malcolm Newey (ANU)
Amy Felty (Bell Labs)	Sam Owre (SRI)
Mike Gordon (Cambridge)	Christine Paulin-Mohring (LRI)
Jim Grundy (ANU)	Lawrence Paulson (Cambridge)
Elsa Gunter (Bell Labs)	Laurent Théry (INRIA)
Joshua Guttman (Mitre)	Phil Windley (Brigham Young)
John Harrison (Intel)	Wai Wong (Hong Kong Baptist)

Invited Speakers

Tobias Nipkow (TU München)
Jockum von Wright (Åbo Akademi)

Additional Reviewers

Abdelwaheb Ayari	Rajev Goré	Peter Robinson
Robert Beers	Trent Larson	Shankar
Yves Bertot	Patrick Lincoln	Rob Shaw
Michael Butler	Chuchang Liu	John Slaney
Ricky Butler	Brendan Mahony	Srivas
Victor Carreño	Andrew Martin	Mark Staples
David Cyrluk	Monica Nesi	Myra VanInwegen
Joelle Despeyroux	Michael Norrish	Luca Viganò
Ben DiVito	Maris Ozols	Jockum von Wright
Katherine Eastaughffe	Randy Pollack	Jon Whittle
Andy Gordon		Burkhart Wolff

Contents

Invited Papers

Verified Lexical Analysis	1
<i>Tobias Nipkow</i>	
Extending Window Inference	17
<i>Joakim von Wright</i>	

Refereed Papers

Program Abstraction in a Higher-Order Logic Framework	33
<i>Marco Benini, Sara Kalvala, and Dirk Nowotka</i>	
The Village Telephone System: A Case Study in Formal Software Engineering	49
<i>Karthikeyan Bhargavan, Carl A. Gunter, Elsa L. Gunter, Michael Jackson, Davor Obradovic, and Pamela Zave</i>	
Generating Embeddings from Denotational Descriptions	67
<i>Richard J. Boulton</i>	
An Interface between CLAM and HOL	87
<i>Richard Boulton, Konrad Slind, Alan Bundy, and Mike Gordon</i>	
Classical Propositional Decidability via Nuprl Proof Extraction	105
<i>James L. Caldwell</i>	
A Comparison of PVS and Isabelle/HOL	123
<i>David Griffioen and Marieke Huisman</i>	
Adding External Decision Procedures to HOL90 Securely	143
<i>Elsa L. Gunter</i>	
Formalizing Basic First Order Model Theory	153
<i>John Harrison</i>	
Formalizing Dijkstra	171
<i>John Harrison</i>	
Mechanical Verification of Total Correctness through Diversion Verification Conditions	189
<i>Peter V. Homeier and David F. Martin</i>	
A Type Annotation Scheme for Nuprl	207
<i>Douglas J. Howe</i>	
Verifying a Garbage Collection Algorithm	225
<i>Paul B. Jackson</i>	

HOT: A Concurrent Automated Theorem Prover Based on Higher-Order Tableaux	245
<i>Karsten Konrad</i>	
Free Variables and Subexpressions in Higher-Order Meta Logic	263
<i>Chuck Liang</i>	
An LPO-based Termination Ordering for Higher-Order Terms without λ -abstraction	277
<i>Maxim Lifantsev and Leo Bachmair</i>	
Proving Isomorphism of First-Order Logic Proof Systems in HOL	295
<i>Anna Mikhajlova and Joakim von Wright</i>	
Exploiting Parallelism in Interactive Theorem Provers	315
<i>Roderick Moten</i>	
I/O Automata and Beyond: Temporal Logic and Abstraction in Isabelle	331
<i>Olaf Müller</i>	
Object-Oriented Verification Based on Record Subtyping in Higher-Order Logic	349
<i>Wolfgang Naraschewski and Markus Wenzel</i>	
On the Effectiveness of Theorem Proving Guided Discovery of Formal Assertions for a Register Allocator in a High-Level Synthesis System	367
<i>Naren Narasimhan and Ranga Vemuri</i>	
Co-inductive Axiomatization of a Synchronous Language	387
<i>David Nowak, Jean-René Beauvais, and Jean-Pierre Talpin</i>	
Formal Specification and Theorem Proving Breakthroughs in Geometric Modeling	401
<i>François Puitg and Jean-François Dufourd</i>	
A Tool for Data Refinement	423
<i>Rimvydas Rukšėnas and Joakim von Wright</i>	
Mechanizing Relevant Logics with HOL	443
<i>Hajime Sawamura and Daisaku Asanuma</i>	
Case Studies in Meta-Level Theorem Proving	461
<i>Friedrich W. von Henke, Stephan Pfab, Holger Pfeifer, and Harald Rueß</i>	
Formalization of Graph Search Algorithms and Its Applications	479
<i>Mitsuharu Yamamoto, Koichi Takahashi, Masami Hagiya, Shin-ya Nishizaki, and Tetsuo Tamai</i>	
Author Index	497