

# Lecture Notes in Computer Science

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

2758

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Hong Kong*

*London*

*Milan*

*Paris*

*Tokyo*

David Basin  
Burkhart Wolff (Eds.)

# Theorem Proving in Higher Order Logics

16 International Conference, TPHOLs 2003  
Rome, Italy, September 8-12, 2003  
Proceedings



Springer

## Series Editors

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

## Volume Editors

David Basin  
ETH Zentrum  
CH-8092 Zürich, Switzerland  
E-mail: basin@inf.ethz.ch

Burkhard Wolff  
Albert-Ludwigs-University Freiburg  
D-79110 Freiburg, Germany  
E-mail: wolff@informatik.uni-freiburg.de

## Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek  
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;  
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

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

ISSN 0302-9743

ISBN 3-540-40664-6 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 New York  
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2003  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP Berlin GmbH  
Printed on acid-free paper      SPIN: 10930755      06/3142      5 4 3 2 1 0

# Preface

This volume constitutes the proceedings of the *16th International Conference on Theorem Proving in Higher Order Logics* (TPHOLs 2003) held September 8–12, 2003 in Rome, Italy. TPHOLs covers all aspects of theorem proving in higher order logics as well as related topics in theorem proving and verification.

TPHOLs 2003 was co-located with *TABLEAUX*, the International Conference on Automated Reasoning with Analytic Tableaux and Related Methods, and with *CalcuIemus*, the Symposium on the Integration of Symbolic Computation and Mechanized Reasoning.

There were 50 papers submitted to TPHOLs 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 tradition, TPHOLs 2003 also offered a venue for the presentation of work in progress, where researchers invite discussion by means of a brief preliminary talk and then discuss their work at a poster session. A supplementary proceedings containing associated papers for work in progress was published by the computer science department at the Universität Freiburg.

The organizers are grateful to Jean-Raymond Abrial, Patrick Lincoln, and Dale Miller for agreeing to give invited talks at TPHOLs 2003.

The TPHOLs conference traditionally changes continent 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-Verlag Lecture Notes in Computer Science series:

|                |      |                  |      |
|----------------|------|------------------|------|
| 1993 (Canada)  | 780  | 1998 (Australia) | 1479 |
| 1994 (Malta)   | 859  | 1999 (France)    | 1690 |
| 1995 (USA)     | 971  | 2000 (USA)       | 1869 |
| 1996 (Finland) | 1125 | 2001 (UK)        | 2152 |
| 1997 (USA)     | 1275 | 2002 (USA)       | 2410 |

We would like to thank members of both the Freiburg and Zürich groups for their help in organizing the program. In particular, Achim Brucker, Barbara Geiser, and Paul Hankes Drielsma. We would also like to express our thanks to Marta Cialdea Mayer and her team for coordinating the local arrangements in Rome.

Finally, we thank our sponsors: Intel, ITT, ETH Zürich, and the Universität Freiburg. We also gratefully acknowledge the use of computing equipment from Università Roma III.

May 2003

David Basin, Burkhart Wolff  
TPHOLs 2003 Program Chairs

## Program Committee

|                           |   |
|---------------------------|---|
| Mark Aagaard              | University of Waterloo, Canada          |
| David Basin               | ETH Zürich, Switzerland                 |
| Yves Bertot               | INRIA Sophia Antipolis, France          |
| Alan Bundy                | University of Edinburgh, UK             |
| Victor Carreno            | NASA Langley, USA                       |
| Iliano Cervesato          | ITT Industries, Inc., USA               |
| Thierry Coquand           | Chalmers University, Göteborg, Sweden   |
| Peter Dybjer              | Chalmers University, Göteborg, Sweden   |
| Amy Felty                 | University of Ottawa, Canada            |
| Jean-Christophe Filliâtre | Université Paris Sud, France            |
| Mike Gordon               | University of Cambridge, UK             |
| Jim Grundy                | Intel Inc., USA                         |
| Elsa Gunter               | NJIT, USA                               |
| John Harrison             | Intel Inc., USA                         |
| Douglas Howe              | Carleton University, Canada             |
| Paul Jackson              | University of Edinburgh, UK             |
| Bart Jacobs               | University of Nijmegen, The Netherlands |
| Sara Kalvala              | University of Warwick, UK               |
| Thomas Kropf              | Bosch, Germany                          |
| Tom Melham                | Oxford University, UK                   |
| César Muñoz               | National Institute of Aerospace, USA    |
| Tobias Nipkow             | Technische Universität München, Germany |
| Sam Owre                  | SRI, USA                                |
| Christine Paulin-Mohring  | Université Paris Sud, France            |
| Lawrence Paulson          | University of Cambridge, UK             |
| Frank Pfenning            | Carnegie Mellon University, USA         |
| Wolfgang Reif             | Universität Augsburg, Germany           |
| Konrad Slind              | University of Utah, USA                 |
| Sofiene Tahar             | Concordia University, Canada            |
| Burkhart Wolff            | Universität Freiburg, Germany           |

## Sponsoring Organizations



## Additional Referees

Sabine Glesner  
 Martin Wildmoser  
 Joakim von Wright  
 Gerwin Klein  
 Bruno Dutertre  
 Alfons Geser  
 Otmane Ait-Mohamed  
 Mohamed Layouni  
 Ali Habibi  
 Amjad Gawanmeh  
 Paul Curzon  
 Helen Lowe  
 Tom Ridge  
 Graham Steel

Daniel Winterstein  
 Dominik Haneberg  
 Michael Balser  
 Claudio Castellini  
 Christoph Duelli  
 Gerhard Schellhorn  
 Andreas Thums  
 Jean Duprat  
 Jan von Plato  
 Makoto Takeyama  
 Nicolas Oury  
 Ashish Tiwari  
 Harald Ruess

# Table of Contents

## Invited Talk I

|   |   |
|---|---|
| Click'n Prove: Interactive Proofs within Set Theory ..... | 1 |
| <i>Jean-Raymond Abrial, Dominique Cansell</i>             |   |

## Hardware and Assembler Languages

|  |    |
|--|----|
| Formal Specification and Verification of ARM6 .....  | 25 |
| <i>Anthony Fox</i>                                   |    |
| A Programming Logic for Java Bytecode Programs ..... | 41 |
| <i>Claire L. Quigley</i>                             |    |
| Verified Bytecode Subroutines .....                  | 55 |
| <i>Gerwin Klein, Martin Wildmoser</i>                |    |

## Proof Automation I

|  |     |
|--|-----|
| Complete Integer Decision Procedures as Derived Rules in HOL ..... | 71  |
| <i>Michael Norrish</i>   |     |
| Changing Data Representation within the Coq System .....           | 87  |
| <i>Nicolas Magaud</i>  |     |
| Applications of Polytypism in Theorem Proving .....                | 103 |
| <i>Konrad Slind, Joe Hurd</i>                                      |     |

## Proof Automation II

|   |     |
|---|-----|
| A Coverage Checking Algorithm for LF .....  | 120 |
| <i>Carsten Schürmann, Frank Pfenning</i>  |     |
| Automatic Generation of Generalization Lemmas for Proving Properties<br>of Tail-Recursive Definitions ..... | 136 |
| <i>Deepak Kapur, Nikita A. Sakhanenko</i>   |     |

## Tool Combination

|   |     |
|---|-----|
| Embedding of Systems of Affine Recurrence Equations in Coq .....                  | 155 |
| <i>David Cachera, David Pichardie</i>   |     |
| Programming a Symbolic Model Checker in a Fully Expansive<br>Theorem Prover ..... | 171 |
| <i>Hasan Amjad</i>  |     |



|  |     |
|--|-----|
| Combining Testing and Proving in Dependent Type Theory ..... | 188 |
| <i>Peter Dybjer, Qiao Haiyan, Makoto Takeyama</i>            |     |

## Invited Talk II

|  |     |
|--|-----|
| Reasoning about Proof Search Specifications: An Abstract ..... | 204 |
| <i>Dale Miller</i>   |     |

## Logic Extensions

|   |     |
|---|-----|
| Program Extraction from Large Proof Developments .....                | 205 |
| <i>Luís Cruz-Filipe, Bas Spitters</i>                                 |     |
| First Order Logic with Domain Conditions .....                        | 221 |
| <i>Freek Wiedijk, Jan Zwanenburg</i>                                  |     |
| Extending Higher-Order Unification to Support Proof Irrelevance ..... | 238 |
| <i>Jason Reed</i>   |     |

## Advances in Theorem Prover Technology

|   |     |
|---|-----|
| Inductive Invariants for Nested Recursion .....   | 253 |
| <i>Sava Krstić, John Matthews</i>   |     |
| Implementing Modules in the Coq System.....   | 270 |
| <i>Jacek Chrząszcz</i>  |     |
| MetaPRL – A Modular Logical Environment.....  | 287 |
| <i>Jason Hickey, Aleksey Nogin, Robert L. Constable, Brian E. Aydemir,</i><br><i>Eli Barzilay, Yegor Bryukhov, Richard Eaton, Adam Granicz,</i><br><i>Alexei Kopylov, Christoph Kreitz, Vladimir N. Krupski,</i><br><i>Lori Lorigo, Stephan Schmitt, Carl Witty, Xin Yu</i> |     |

## Mathematical Theories

|  |     |
|--|-----|
| Proving Pearl: Knuth’s Algorithm for Prime Numbers ..... | 304 |
| <i>Laurent Théry</i>                                     |     |
| Formalizing Hilbert’s Grundlagen in Isabelle/Isar .....  | 319 |
| <i>Laura I. Meikle, Jacques D. Fleuriot</i>              |     |

## Security

|  |     |
|--|-----|
| Using Coq to Verify Java Card™ Applet Isolation Properties ..... | 335 |
| <i>June Andronick, Boutheina Chetali, Olivier Ly</i>             |     |
| Verifying Second-Level Security Protocols .....                  | 352 |
| <i>Giampaolo Bella, Cristiano Longo, Lawrence C Paulson</i>      |     |

|                    |     |
|--------------------|-----|
| Author Index ..... | 367 |
|--------------------|-----|