Theorem Proving in Higher Order Logics

20th International Conference, TPHOLs 2007
Kaiserslautern, Germany, September 10-13, 2007
Proceedings
Preface

This volume constitutes the proceedings of the 20th International Conference on Theorem Proving in Higher-Order Logics (TPHOLs 2007) held September 10–13, 2007 in Kaiserslautern, Germany. TPHOLs covers all aspects of theorem proving in higher-order logics as well as related topics in theorem proving and verification.

There were 52 submissions, and each submission was refereed by at least 4 reviewers, who had been selected by the program committee. Of these submissions, 26 were accepted for presentation at the conference and publication in this volume. In keeping with tradition, TPHOLs 2007 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 University of Kaiserslautern. The organizers are grateful to Constance Heitmeyer (Naval Research Laboratory), Xavier Leroy (INRIA Rocquencourt) and Peter Liggesmeyer (Fraunhofer IESE) for agreeing to give invited talks at TPHOLs 2007.

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

<table>
<thead>
<tr>
<th>Year</th>
<th>Location</th>
<th>LNCS Number</th>
<th>Year</th>
<th>Location</th>
<th>LNCS Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1993</td>
<td>Vancouver</td>
<td>LNCS 780</td>
<td>2000</td>
<td>Portland</td>
<td>LNCS 1869</td>
</tr>
<tr>
<td>1994</td>
<td>Valletta</td>
<td>LNCS 859</td>
<td>2001</td>
<td>Edinburgh</td>
<td>LNCS 2152</td>
</tr>
<tr>
<td>1995</td>
<td>Aspen Grove</td>
<td>LNCS 971</td>
<td>2002</td>
<td>Hampton</td>
<td>LNCS 2410</td>
</tr>
<tr>
<td>1996</td>
<td>Turku</td>
<td>LNCS 1125</td>
<td>2003</td>
<td>Rome</td>
<td>LNCS 2758</td>
</tr>
<tr>
<td>1997</td>
<td>Murray Hill</td>
<td>LNCS 1275</td>
<td>2004</td>
<td>Park City</td>
<td>LNCS 3223</td>
</tr>
<tr>
<td>1998</td>
<td>Canberra</td>
<td>LNCS 1479</td>
<td>2005</td>
<td>Oxford</td>
<td>LNCS 3603</td>
</tr>
<tr>
<td>1999</td>
<td>Nice</td>
<td>LNCS 1690</td>
<td>2006</td>
<td>Seattle</td>
<td>LNCS 4130</td>
</tr>
</tbody>
</table>

We would like to thank our sponsors: Fraunhofer IESE (Institute of Experimental Software Engineering), DASMOD (Dependable Adaptive Systems and Mathematical Modeling) Cluster, and DFKI (German Research Center for Artificial Intelligence).

July 2007

Klaus Schneider
Jens Brandt
Conference Organization

Program Chairs
Klaus Schneider
Jens Brandt

Program Committee
Mark Aagaard
Yves Bertot
Ching-Tsun Chou
Thierry Coquand
Amy Felty
Jean-Christophe Filliatre
Ganesh Gopalakrishnan
Mike Gordon
Jim Grundy
Elsa Gunter
John Harrison
Jason Hickey
Peter Homeier
Joe Hurd
Paul Jackson
Thomas Kropf
John Matthews
Tom Melham
Cesar Munoz
Tobias Nipkow
Sam Owre
Christine Paulin-Mohring
Lawrence Paulson
Klaus Schneider
Konrad Slind
Sofiene Tahar
Burkhart Wolff

External Reviewers
Behzad Akbarpour
Ulrich Berger
Stefan Berghofer
Pierre Castéran
Pierre Corbineau
Amjad Gawanmeh
Florian Haftmann
Osman Hasan
Nathan Linger
Claude Marche
Jia Meng
Paul Miner
John O’Leary
Sam Owre
Tom Ridge
Norbert Schirmer
Natarajan Shankar
Alan Smaill
Mark-Oliver Stehr
Christian Urban
Makarius Wenzel
Yu Yang
Mohamed Zaki
# Table of Contents

On the Utility of Formal Methods in the Development and Certification of Software (Invited Talk) .......................... 1  
*Constance L. Heitmeyer*

*Peter Liggesmeyer*

Separation Logic for Small-Step Cminor ........................................ 5  
*Andrew W. Appel and Sandrine Blazy*

Formalising Java’s Data Race Free Guarantee ............................... 22  
*David Aspinall and Jaroslav Ševčík*

Finding Lexicographic Orders for Termination Proofs in Isabelle/HOL  ........................................................................ 38  
*Lukas Bulwahn, Alexander Krauss, and Tobias Nipkow*

Formalising Generalised Substitutions ......................................... 54  
*Jeremy E. Dawson*

Extracting Purely Functional Contents from Logical Inductive Types  ... 70  
*David Delahaye, Catherine Dubois, and Jean-Frédéric Étienne*

A Modular Formalisation of Finite Group Theory .......................... 86  
*Georges Gonthier, Assia Mahboubi, Laurence Rideau, Enrico Tassi, and Laurent Théry*

Verifying Nonlinear Real Formulas Via Sums of Squares ................ 102  
*John Harrison*

Verification of Expectation Properties for Discrete Random Variables  
in HOL ...................................................................................... 119  
*Osman Hasan and Sofiène Tahar*

A Formally Verified Prover for the ALC Description Logic ............... 135  
*José-Antonio Alonso, Joaquín Borrego-Díaz, María-José Hidalgo, Francisco-Jesus Martín-Mateos, and José-Luis Ruiz-Reina*

Proof Pearl: The Termination Analysis of TERMINATOR .................. 151  
*Joe Hurd*

Improving the Usability of HOL Through Controlled Automation Tactics .......................................................... 157  
*Eunsuk Kang and Mark D. Aagaard*
Verified Decision Procedures on Context-Free Grammars
Yasuhiko Minamide
173

Using XCAP to Certify Realistic Systems Code: Machine Context Management
Zhaozhong Ni, Dachuan Yu, and Zhong Shao
189

Proof Pearl: De Bruijn Terms Really Do Work
Michael Norrish and René Vestergaard
207

Proof Pearl: Looping Around the Orbit
Steven Obua
223

Source-Level Proof Reconstruction for Interactive Theorem Proving
Lawrence C. Paulson and Kong Woei Susanto
232

Proof Pearl: The Power of Higher-Order Encodings in the Logical Framework LF
Brigitte Pientka
246

Automatically Translating Type and Function Definitions from HOL to ACL2
James Reynolds
262

Operational Reasoning for Concurrent Caml Programs and Weak Memory Models
Tom Ridge
278

Proof Pearl: Wellfounded Induction on the Ordinals Up to $\varepsilon_0$
Matt Kaufmann and Konrad Slind
294

A Monad-Based Modeling and Verification Toolbox with Application to Security Protocols
Christoph Sprenger and David Basin
302

Primality Proving with Elliptic Curves
Laurent Théry and Guillaume Hanrot
319

HOL2P - A System of Classical Higher Order Logic with Second Order Polymorphism
Norbert Völker
334

Building Formal Method Tools in the Isabelle/Isar Framework
Makarius Wenzel and Burkhart Wolff
352

Simple Types in Type Theory: Deep and Shallow Encodings
François Garillot and Benjamin Werner
368

Mizar’s Soft Type System
Freek Wiedijk
383

Author Index
401