Lecture Notes in Computer Science 859
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Thomas F. Melham Juanito Camilleri (Eds.)

Higher Order Logic Theorem Proving and Its Applications

7th International Workshop
Valletta, Malta, September 19-22, 1994
Proceedings

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 69 80, Vincenz-Priessnitz-Straße 1, D-76131 Karlsruhe, Germany

Juris Hartmanis
Department of Computer Science, Cornell University
4130 Upson Hall, Ithaka, NY 14853, USA

Jan van Leeuwen
Department of Computer Science, Utrecht University
Padualaan 14, 3584 CH Utrecht, The Netherlands

Volume Editors

Thomas F. Melham
Department of Computing Science, University of Glasgow
17 Lilybank Gardens, Glasgow, Scotland, G12 8QQ

Juanito Camilleri
Department of Computer Studies, University of Malta
University Heights, Msida, Malta

CR Subject Classification (1991): F.4.1, I.2.2-3

ISBN 3-540-58450-1 Springer-Verlag Berlin Heidelberg New York

CIP data applied for

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 1994
Printed in Germany

Typesetting: Camera-ready by author
SPIN: 10479015 45/3140-543210 - Printed on acid-free paper

Preface

This volume is the proceedings of the international workshop on *Higher Order Logic Theorem Proving and its Applications*, held at the Foundation for International Studies in the University of Malta during 19–22 September 1994. The workshop is the seventh in a series of annual meetings that began in 1988 with a small user group meeting for the HOL theorem prover and has since grown into a full-scale international workshop. Although the main subject of these meetings is still the HOL system, the focus has widened over the years to include the application, design, and theory of any mechanized proof system for higher order logic.

The forty-two papers submitted were mostly of a 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 at the workshop; all these papers appear in this proceedings. The workshop has a strong tradition of providing an open venue for the discussion and sharing of preliminary results, particularly those of students; a further twelve submissions were therefore accepted for informal presentation in a poster session.

The workshop organizers were especially pleased that Professor N. G. de Bruijn, Dr. Thomas Forster, and Dr. Keith Hanna accepted invitations to be guest speakers at the workshop. All three invited speakers also very kindly produced written contributions for inclusion in this proceedings.

We wish to thank the Bank of Valletta, Malta, who generously provided financial support for the workshop. We also gratefully acknowledge the support of the University of Malta, our host for the workshop, and of the Computing Science Department at Glasgow University. Jackie Attard Montalto and Yasmeen Staff gave invaluable assistance in matters of local organization.

Tom Melham
Juanito Camilleri

Conference Organization

Programme Chair
Dr. Thomas Melham
Dept. of Computing Science
University of Glasgow
17 Lilybank Gardens
Glasgow, Scotland, G12 8QQ
e-mail: `tfm@dcs.glasgow.ac.uk`

Workshop Chair
Dr. Juanito Camilleri
Dept. of Computer Science & AI
University of Malta
University Heights
Tal-Qroqq, Malta
e-mail: `juan@unimt.mt`

Programme Committee

By providing detailed and thoughtful reviews of the papers, the programme committee made a significant contribution to the quality of both the conference programme and this proceedings.

Flemming Andersen (TDR)
Richard Boulton (Cambridge)
Shui-Kai Chin (Syracuse)
Elsa Gunter (AT&T)
John Herbert (SRI)
Jeffrey Joyce (UBC)
Gilles Kahn (INRIA)
Ramayya Kumar (FZI)
Tim Leonard (DEC)
Karl Levitt (UC Davis)
Paul Loewenstein (SUN)
Tom Melham (Glasgow)
Tom Schubert (Portland State)
David Shepherd (INMOS)
Phil Windley (BYU)
Joakim von Wright (Åbo Akademi)

Additional Reviewers

The programme committee gratefully acknowledges the constructive assistance of the following additional reviewers:

Jim Alves-Foss, Penny Anderson, Myla Archer, Gregory Benson, Michael Butler, Rachel Cardell-Oliver, Anand Chavan, Paul Curzon, Nancy Day, Michael Donat, Gilles Dowek, Bill Findlay, Jens Godskesen, Mike Gordon, Cordelia Hall, Mark Heckman, Shahid Ikram, Jang-Dae Kim, Jens Kristensen, Finn Kristoffersen, Juin-Yeu Lu, Chet Murthy, Monica Nesi, Karsten Nyblad, Jørgen Nørgaard, Kim Dam Petersen, Jimmi Pettersson, Rob Shaw, Helene Wong, Cui Zhang, Zheng Zhu.

Contents

LCF Examples in HOL
Sten Agerholm 1

A Graphical Tool for Proving UNITY Progress
Flemming Andersen, Kim Dam Petersen, and Jimmi S. Pettersson 17

Reasoning About a Class of Linear Systems of Equations in HOL
Catia M. Angelo, Luc Claesen, and Hugo De Man 33

Towards a HOL Theory of Memory
J-P. Bodeveix, M. Filali, and P. Roche 49

Providing Tractable Security Analyses in HOL
Stephen H. Brackin 65

Invited paper:
Highlighting the Lambda-free Fragment of Automath
N.G. de Bruijn 81

First-Order Automation for Higher-Order-Logic Theorem Proving
Holger Busch 97

Symbolic Animation as a Proof Tool
Juanito Camilleri and Vincent Zammit 113

Datatypes in L2
Nick Chapman, Simon Finn, and Michael P. Fourman 128

A Formal Theory of Undirected Graphs in Higher-Order Logic
Ching-Tsun Chou 144

Mechanical Verification of Distributed Algorithms in Higher-Order Logic
Ching-Tsun Chou 158

Tracking Design Changes with Formal Verification
Paul Curzon 177

Invited paper:
Weak Systems of Set Theory Related to HOL
Thomas Forster 193

Interval-Semantic Component Models and the Efficient Verification of Transaction-Level Circuit Behavior
David A. Fura and Arun K. Somani 205

An Interpretation of NODEN in HOL
Brian T. Graham 221

Invited paper:
Reasoning about Real Circuits
Keith Hanna 235

Binary Decision Diagrams as a HOL Derived Rule
John Harrison 254

Trustworthy Tools for Trustworthy Programs: A Verified Verification Condition Generator
Peter V. Homeier and David F. Martin 269

S : A Machine Readable Specification Notation Based on Higher Order Logic
J. Joyce, N. Day, and M. Donat 285

An Engineering Approach to Formal Digital System Design
Mats Larsson 300

Generating Designs Using an Algorithmic Register Transfer Language with Formal Semantics
Juin-Yeu Lu and Shiu-Kai Chin 316

A HOL Formalisation of the Temporal Logic of Actions
Thomas Långbacka 332

Studying the ML Module System in HOL
Savi Maharaj and Elsa Gunter 346

Towards a Mechanically Supported and Compositional Calculus to Design Distributed Algorithms
I.S.W.B. Prasetya 362

Simplifying Deep Embedding: A Formalised Code Generator
Ralf Reetz and Thomas Kropf 378

Automating Verification by Functional Abstraction at the System Level
Klaus Schneider, Ramayya Kumar, and Thomas Kropf 391

A Parameterized Proof Manager
Konrad Slind 407

Implementational Issues for Verifying RISC-Pipeline Conflicts in HOL
Sofiène Tahar and Ramayya Kumar 424

Specifying Instruction-Set Architectures in HOL: A Primer
Phillip J. Windley 440

Representing Higher Order Logic Proofs in HOL
J. von Wright 456