Lecture Notes in Computer Science 4502

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison
Lancaster University, UK

Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
University of Surrey, Guildford, UK

Jon M. Kleinberg
Cornell University, Ithaca, NY, USA

Friedemann Mattern
ETH Zurich, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
University of Dortmund, Germany

Madhu Sudan
Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Moshe Y. Vardi
Rice University, Houston, TX, USA

Gerhard Weikum
Max-Planck Institute of Computer Science, Saarbruecken, Germany

Thorsten Altenkirch Conor McBride (Eds.)

Types for Proofs and Programs

International Workshop, TYPES 2006
Nottingham, UK, April 18-21, 2006
Revised Selected Papers

Volume Editors

Thorsten Altenkirch
Conor McBride
University of Nottingham
School of Computer Science and Information Technology
Jubilee Campus, Wollaton Road, Nottingham NG8 1BB, UK
E-mail: {txa, ctm}@cs.nott.ac.uk

Library of Congress Control Number: 2007936170

CR Subject Classification (1998): F.3.1, F.4.1, D.3.3, I.2.3

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-74463-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-74463-4 Springer 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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12111886 06/3180 5 4 3 2 1 0

Preface

These proceedings contain a selection of refereed papers presented at or related to the Annual Workshop of the TYPES project (EU coordination action 510996), which was held April 18–21, 2006 at the University of Nottingham, UK.

The topic of this workshop was formal reasoning and computer programming based on type theory: languages and computerized tools for reasoning, and applications in several domains such as analysis of programming languages, certified software, formalization of mathematics and mathematics education.

The workshop was attended by more than 100 researchers and included more than 60 presentations. We also had the pleasure of three invited lectures, from Bart Jacobs (University of Nijmegen), Hongwei Xi (Boston University) and Simon Peyton Jones (Microsoft Research). Simon Peyton Jones spoke in a joint session with the workshop on Trends in Functional Programming (TFP), which was co-located with the TYPES conference.

From 29 submitted papers, 17 were selected after a reviewing process. The final decisions were made by the editors.

This workshop followed a series of meetings of the TYPES working group funded by the European Union (IST project 29001, ESPRIT Working Group 21900, ESPRIT BRA 6435). The proceedings of these workshop were published in the LNCS series:

TYPES 1993 Nijmegen, The Netherlands, LNCS 806
TYPES 1994 Båstad, Sweden, LNCS 996
TYPES 1995 Turin, Italy, LNCS 1158
TYPES 1996 Aussois, France, LNCS 1512
TYPES 1998 Kloster Irsee, Germany, LNCS 1657
TYPES 1999 Lökeborg, Sweden, LNCS 1956
TYPES 2000 Durham, UK, LNCS 2277
TYPES 2002 Berg en Dal, The Netherlands, LNCS 2646
TYPES 2003 Turin, Italy, LNCS 3085
TYPES 2004 Jouy-en-Josas, France, LNCS 3839

ESPRIT BRA 6453 was a continuation of ESPRIT Action 3245, Logical Frameworks: Design, Implementation and Experiments. Proceedings for annual meetings under that action were published by Cambridge University Press in the books *Logical Frameworks* and *Logical Environments*, edited by Gérard Huet and Gordon Plotkin.

We are grateful for the support of the School of Computer Science and Information Technology at the University of Nottingham in organizing the meeting. We should like to thank James Chapman, Wouter Swierstra and Peter Morris,

who helped with the administration and coordination of the meeting. We are also grateful to Peter Morris for help in the preparation of the volume.

March 2007

Thorsten Altenkirch
Conor McBride

Referees

A. Abel
P. Aczel
R. Adams
R. Atkey
S. van Bakel
C. Ballarin
S. Berardi
Y. Bertot
A. Bove
E. Brady
P. Callaghan
J. Carlstrom
J. Cheney
J. Chrząszcz
M. Coppo
J. Courant
C. Coquand
T. Coquand
R. Crole
R. Davies
J. Despeyroux
L. Dixon
G. Dowek
R. Dychhoff
M. Escardo
J-C. Filliâtre
M. Fluet
P. Fontaine
N. Gambino
H. Geuvers
N. Ghani
A. Gordon
B. Grégoire
P. Hancock
J. Harrison
M. Huisman
B. Jacobs
S. Jost
T. Kelsey
J. Lipton
Z. Luo
M.E. Maietti
J. McKinna
M. Miculan
A. Miquel
P. Morris
S. Negri
M. Oostdijk
R. Paterson
D. Pattinson
R. Pollack
T. Ridge
G. Sambin
T. Streicher
C. Urban
D. Walukiewicz-Chrząszcz
S. Weirich
A. Weiermann
B. Werner
F. Wiedijk

Table of Contents

Weyl's Predicative Classical Mathematics as a Logic-Enriched Type Theory 1
Robin Adams and Zhaohui Luo

Crafting a Proof Assistant 18
Andrea Asperti, Claudio Sacerdoti Coen, Enrico Tassi, and Stefano Zacchiroli

On Constructive Cut Admissibility in Deduction Modulo 33
Richard Bonichon and Olivier Hermant

Fast Reflexive Arithmetic Tactics the Linear Case and Beyond 48
Frédéric Besson

Combining de Bruijn Indices and Higher-Order Abstract Syntax in Coq 63
Venanzio Capretta and Amy P. Felty

Deciding Equality in the Constructor Theory 78
Pierre Corbineau

A Formalisation of a Dependently Typed Language as an Inductive-Recursive Family 93
Nils Anders Danielsson

Truth Values Algebras and Proof Normalization 110
Gilles Dowek

Curry-Style Types for Nominal Terms 125
Maribel Fernández and Murdoch J. Gabbay

(In)consistency of Extensions of Higher Order Logic and Type Theory 140
Herman Geuvers

Constructive Type Classes in Isabelle 160
Florian Haftmann and Makarius Wenzel

Zermelo's Well-Ordering Theorem in Type Theory 175
Danko Ilik

A Finite First-Order Theory of Classes 188
Florent Kirchner

Coinductive Correctness of Homographic and Quadratic Algorithms for Exact Real Numbers 203
Milad Niqui

Using Intersection Types for Cost-Analysis of Higher-Order Polymorphic Functional Programs 221
Hugo R. Simões, Kevin Hammond, Mário Florido, and Pedro Vasconcelos

Subset Coercions in Coq 237
Matthieu Sozeau

A Certified Distributed Security Logic for Authorizing Code 253
Nathan Whitehead

Author Index 269