

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

New York University, NY, 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

Jean-Christophe Filliâtre
Christine Paulin-Mohring
Benjamin Werner (Eds.)

Types for Proofs and Programs

International Workshop, TYPES 2004
Jouy-en-Josas, France, December 15-18, 2004
Revised Selected Papers



Springer

Volume Editors

Jean-Christophe Filliâtre
Christine Paulin-Mohring
LRI, Inria Futurs, LIX, Université Paris Sud
LRI Bât 490, 91405 Orsay Cedex, France
E-mail: {jean-christophe.filliatre,christine.paulin}@lri.fr

Benjamin Werner
Inria Futurs, LIX, LRI, Laboratoire d'Informatique (LIX)
École Polytechnique
91128 Palaiseau Cedex, France
E-mail: werner@lix.polytechnique.fr

Library of Congress Control Number: 2005938814

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 3-540-31428-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-31428-8 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 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11617990 06/3142 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 from December 15 to 18, 2004, in Jouy en Josas, France.

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 proposed more than 50 presentations. Out of 33 post-workshop 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 93 Nijmegen, The Netherlands, LNCS 806

TYPES 94 Båstad, Sweden, LNCS 996

TYPES 95 Torino, Italy, LNCS 1158

TYPES 96 Aussois, France, LNCS 1512

TYPES 98 Kloster Irsee, Germany, LNCS 1657

TYPES 2000 Durham, United Kingdom, LNCS 2277

TYPES 2002 Berg en Dal, The Netherlands, LNCS 2646

TYPES 2003 Torino, Italy, LNCS 3085

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

We are very grateful to INRIA for supporting the TYPES meeting. We especially want to thank Catherine Girard and Catherine Moreau (organization), Chantal Girodon (registration) and Laurent Steff (technical support). Hugo Herbelin was in charge of the programme in the organizing committee. Finally, Marie-Carol Lopes took care of the organization of the post-workshop proceedings and carefully prepared the final composition of the volume.

November 2005

Jean-Christophe Filliâtre
Christine Paulin-Mohring
Benjamin Werner

Organization

Referees

P. Aczel	N. Gambino	D. Miller
M. Baaz	H. Geuvers	A. Miquel
C. Ballarin	B. Grégoire	J-F. Monin
B. Barras	P. Hancock	Z. Petric
S. Berardi	D. Hendricks	D. Pichardie
S. Berghofer	O. Hermant	R. Pollack
Y. Bertot	J. Hickey	L. Pottier
F. Blanqui	F. Honsell	C. Raffalli
S. Boulmé	G. Klein	E. Ritter
A. Bove	S. Kremer	C. Sacerdoti Coen
V. Capretta	Z. Luo	P. Sobocinski
T. Coquand	A. Mahboubi	B. Spitters
L. Cruz-Filipe	R. Matthes	M. Strecker
J. Despeyroux	M. Mayero	L. Thery
P. Di Gianantonio	C. McBride	F. Wiedjick
L. Dixon	P-A. Melliès	K. Wirt
G. Dowek	M. Miculan	R. Zumkeller
N. Gahni	R. Milewski	

Table of Contents

Formalized Metatheory with Terms Represented by an Indexed Family of Types <i>Robin Adams</i>	1
A Content Based Mathematical Search Engine: Whelp <i>Andrea Asperti, Ferruccio Guidi, Claudio Sacerdoti Coen, Enrico Tassi, Stefano Zacchiroli</i>	17
A Machine-Checked Formalization of the Random Oracle Model <i>Gilles Barthe, Sabrina Tarento</i>	33
Extracting a Normalization Algorithm in Isabelle/HOL <i>Stefan Berghofer</i>	50
A Structured Approach to Proving Compiler Optimizations Based on Dataflow Analysis <i>Yves Bertot, Benjamin Grégoire, Xavier Leroy</i>	66
Formalising Bitonic Sort in Type Theory <i>Ana Bove, Thierry Coquand</i>	82
A Semi-reflexive Tactic for (Sub-)Equational Reasoning <i>Claudio Sacerdoti Coen</i>	98
A Uniform and Certified Approach for Two Static Analyses <i>Solange Coupet-Grimal, William Delobel</i>	115
Solving Two Problems in General Topology Via Types <i>Adam Grabowski</i>	138
A Tool for Automated Theorem Proving in Agda <i>Fredrik Lindblad, Marcin Benke</i>	154
Surreal Numbers in Coq <i>Lionel Elie Mamane</i>	170
A Few Constructions on Constructors <i>Conor McBride, Healfdene Goguen, James McKinna</i>	186
Tactic-Based Optimized Compilation of Functional Programs <i>Thomas Meyer, Burkhart Wolff</i>	201

Interfaces as Games, Programs as Strategies <i>Markus Michelbrink</i>	215
λ Z: Zermelo's Set Theory as a PTS with 4 Sorts <i>Alexandre Miquel</i>	232
Exploring the Regular Tree Types <i>Peter Morris, Thorsten Altenkirch, Conor McBride</i>	252
On Constructive Existence <i>Michel Parigot</i>	268
Author Index	275