Lecture Notes in Computer Science 5520

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

Alfred Kobsa
University of California, Irvine, CA, 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
Microsoft Research, Cambridge, MA, USA

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

Doug Tygar
University of California, Berkeley, CA, USA

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

Ana Bove Luís Soares Barbosa
Alberto Pardo Jorge Sousa Pinto (Eds.)

Language Engineering and Rigorous Software Development

International LerNet ALFA Summer School 2008
Piriapolis, Uruguay, February 24 - March 1, 2008
Revised Tutorial Lectures

Springer

Volume Editors

Ana Bove
Chalmers University of Technology
Department of Computer Science and Engineering
412 96 Göteborg, Sweden
E-mail: bove@chalmers.se

Luís Soares Barbosa
Universidade do Minho, Departamento de Informática
Campus de Gualtar, 4700-320 Braga, Portugal
E-mail: lsb@di.uminho.pt

Alberto Pardo
Universidad de la República
Facultad de Ingeniería, Instituto de Computación
Julio Herrera y Reissig 565 - Piso 5, 11300 Montevideo, Uruguay
E-mail: pardo@fing.edu.uy

Jorge Sousa Pinto
Universidade do Minho, Departamento de Informática
Campus de Gualtar, 4700-320 Braga, Portugal
E-mail: jsp@di.uminho.pt

Library of Congress Control Number: 2009930949

CR Subject Classification (1998): D.2, D.3, I.6, F.3, K.6.3

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743
ISBN-10 3-642-03152-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-03152-6 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.com

© Springer-Verlag Berlin Heidelberg 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12716449 06/3180 5 4 3 2 1 0

Preface

This volume contains the lecture notes from the courses offered at the International Summer School on Language Engineering and Rigorous Software Development, held in Piriápolis, Uruguay, from February 25 to March 1, 2008.

The aim of the school was the dissemination of advanced scientific knowledge in the areas of programming languages and rigorous methods for software development. The school was oriented to computer science graduate students and researchers, with an interest in formal techniques for the design and construction of software systems as well as programming languages.

The school was organized in the context of the LERnet (Language Engineering and Rigorous Software Development) project. LERnet is a project of the ALFA programme of the European Commission for co-operation between higher education institutions of the European Union and Latin America. The institutions that participate in the LERnet project are the following:

- Chalmers Tekniska Högskola, Sweden
- Institut National de la Recherche en Informatique et Automatique (INRIA), France
- Universidad de Castilla-La Mancha, Spain
- Universidad Católica de Santiago del Estero, Argentina
- Universidad EAFIT, Colombia
- Universidade Federal de Minas Gerais, Brazil
- Universidade do Minho, Portugal
- Universidad Nacional de San Luis, Argentina
- Universidad Politécnica de Valencia, Spain
- Universidad de la República, Uruguay
- Universiteit Utrecht, The Netherlands

The project oversees the mobility of PhD students from Latin America to the European Union and vice versa for a period of up to 18 months, to pursue research activities in the scope of their PhD projects. LERnet has funded the mobility of 21 doctorate students who thus had the opportunity to develop part of their work integrated in top teams in the area of their respective projects. This summer school was organized as a complementary activity of LERnet, and as such it included a student workshop where the grantholders had the opportunity to present, discuss, and obtain feedback on the progress of their work.

The relevance of the material contained in this volume reflects the increasing importance of programming language-based methods for reasoning about properties of software. Type systems play a prominent role among such methods, being as they are fundamental ingredients of programming languages and proof assistants. Types can also be used for establishing properties of software, such as information flow security. These proceedings include the lecture notes of three

courses on type theory: an introductory tutorial by Herman Geuvers, a course on type-based termination by Gilles Barthe, Benjamim Grégoire and Colin Riba, and a practical introduction to dependent types by Ana Bove and Peter Dybjer.

Type theory as used in the Coq proof assistant is also the basis for Yves Bertot's encoding in Coq of a static analyzer based on abstract interpretation, a semantics-based method. His study shows how a tool of undeniable practical interest can be formally understood and reasoned about. A different kind of encoding is used in the tutorial on combinator parsing by Doaitse Swierstra, which shows the advantages of embedding domain-specific languages into a programming language with a powerful type system and well-studied semantics.

A study by J.N. Oliveira of extended static checking using a point-free transform completes the volume. This is a novel approach to the treatment of the proof obligations generated when reasoning about properties of software. The approach advocates the use of algebraic methods to complement the more traditional use of logic.

Together these contributions will be an invaluable tool for graduate students and researchers looking forward to keeping up to date with the latest developments in rigorous approaches to software development.

We thank Adriana Carvalho and all the members of her team at the Bureau of International Relations at Minho, who were responsible for managing the project, including the participation of the project's grantholders in the event.

Finally, we would also like to express our gratitude to the school's sponsors, and thank the members of the Local Organizing Committee for the seamless organization and very enjoyable setting in which the school took place.

January 2009

Ana Bove
Luis Soares Barbosa
Alberto Pardo
Jorge Sousa Pinto

Organization

The LerNet Summer School was organised by the Universidad de la República, Uruguay.

Program Chair

Jorge Sousa Pinto	Minho University, Portugal

Scientific Committee

Ana Bove	Chalmers University, Sweden
Luis Soares Barbosa	Minho University, Portugal
Alberto Pardo	Universidad de la República, Uruguay
Jorge Sousa Pinto	Minho University, Portugal

Organizing Committee

Ana Bove	Chalmers University, Sweden
Carlos Luna	Universidad de la República, Uruguay
Alberto Pardo	Universidad de la República, Uruguay
Luis Sierra	Universidad de la República, Uruguay

Referees

A. Abel
R. Backhouse
Y. Bertot
C. Camarão
P. Dybjer
M. Florido
H. Geuvers
P. Gorm Larsen
C. McBride
C. Riba

Sponsoring Institutions

PEDECIBA (Programa de Desarrollo de las Ciencias Básicas, Uruguay)
CSIC (Comisión Sectorial de Investigación Científica, Universidad de la República)
TATA Consultancy Services
Microsoft Uruguay

Table of Contents

Introduction to Type Theory 1
Herman Geuvers

Dependent Types at Work 57
Ana Bove and Peter Dybjer

A Tutorial on Type-Based Termination 100
Gilles Barthe, Benjamin Grégoire, and Colin Riba

Structural Abstract Interpretation: A Formal Study Using Coq 153
Yves Bertot

Extended Static Checking by Calculation Using the Pointfree Transform 195
José N. Oliveira

Combinator Parsing: A Short Tutorial 252
S. Doaitse Swierstra

Author Index 301