Lecture Notes in Computer Science 7342

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
TU Dortmund University, 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 for Informatics, Saarbruecken, Germany

Jeremy Gibbons Pablo Nogueira (Eds.)

Mathematics of Program Construction

11th International Conference, MPC 2012
Madrid, Spain, June 25-27, 2012
Proceedings

Springer

Volume Editors

Jeremy Gibbons
Oxford University
Department of Computer Science
Wolfson Building, Parks Road, Oxford OX1 3QD, UK
E-mail: jeremy.gibbons@cs.ox.ac.uk

Pablo Nogueira
Universidad Politécnica de Madrid
Facultad de Informática, Campus de Montegancedo s/n
28660 Boadilla del Monte, Madrid, Spain
E-mail: pablo.nogueira@upm.es

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-31112-3 e-ISBN 978-3-642-31113-0
DOI 10.1007/978-3-642-31113-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012939357

CR Subject Classification (1998): F.3, D.2.4, D.1.1, F.4.1, D.3, F.4, G.2, D.1

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

© Springer-Verlag Berlin Heidelberg 2012
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.
The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the proceedings of MPC 2012, the 11th International Conference on the Mathematics of Program Construction. This conference series aims to promote the development of mathematical principles and techniques that are demonstrably practical and effective in the process of constructing computer programs, broadly interpreted. The focus is on techniques that combine precision with conciseness, enabling programs to be constructed by formal calculation.

The conference was held in Madrid, Spain, during June 25–27, 2012. The previous ten conferences were held in 1989 in Twente, The Netherlands (with proceedings published as LNCS 375); in 1992 in Oxford, UK (LNCS 669); in 1995 in Kloster Irsee, Germany (LNCS 947); in 1998 in Marstrand, Sweden (LNCS 1422); in 2000 in Ponte de Lima, Portugal (LNCS 1837); in 2002 in Dagstuhl, Germany (LNCS 2386); in 2004, in Stirling, UK (LNCS 3125); in 2006 in Kuressaare, Estonia (LNCS 4014); in 2008 in Marseille-Luminy, France (LNCS 5133); and in 2010 in Lac-Beauport, Canada (LNCS 6120).

There were 27 submissions—rather fewer than in previous years. Each submission was reviewed by at least four members of the Program Committee, with an additional review by one of the Program Chairs. The Program Committee selected 13 papers to appear at the conference. Of these 13 papers, 6 had an additional round of 'shepherding' by a member of the Program Committee in order to improve the presentation and tailor it for the MPC audience. There were also three invited talks at the conference; these are represented here by one paper and two abstracts.

The MPC conference series takes great pride in the thoroughness of its reviewing. We are very grateful to the members of the Program Committee and the external referees for their care and diligence in reviewing the submitted papers. The review process and compilation of the proceedings were greatly helped by Andrei Voronkov's EasyChair system, which we can highly recommend.

June 2012

Jeremy Gibbons
Pablo Nogueira

Organization

Program Committee

Ralph-Johan Back	Abo Akademi University, Finland
Roland Backhouse	University of Nottingham, UK
Eerke Boiten	University of Kent, UK
William R. Cook	University of Texas at Austin, USA
Jules Desharnais	Université Laval, Canada
Jeremy Gibbons	University of Oxford, UK
Lindsay Groves	Victoria University of Wellington, New Zealand
Ian J. Hayes	University of Queensland, Australia
Ralf Hinze	University of Oxford, UK
Graham Hutton	University of Nottingham, UK
Johan Jeuring	Open Universiteit Nederland and Universiteit Utrecht, The Netherlands
Christian Lengauer	University of Passau, Germany
Larissa Meinicke	University of Queensland, Australia
Carroll Morgan	University of New South Wales, Australia
Shin-Cheng Mu	Academia Sinica, Taiwan
Bernhard Möller	Institut für Informatik, Universität Augsburg, Germany
David Naumann	Stevens Institute of Technology, USA
Pablo Nogueira	Universidad Politécnica de Madrid, Spain
Jose Oliveira	Universidade do Minho, Portugal
Steve Reeves	The University of Waikato, New Zealand
Wouter Swierstra	Universiteit Utrecht, The Netherlands
Anya Tafliovich	University of Toronto Scarborough, Canada

Additional Reviewers

Paulo Sérgio Almeida	Roland Glueck	Nicolas Pouillard
Gilles Barthe	Stefan Hallerstede	Viorel Preoteasa
James Chapman	Ángel Herranz	Patrick Roocks
Juan Manuel Crespo	Wim Hesselink	Cesar Sanchez
Sharon Curtis	Martin Hofmann	Jeremy Siek
Han-Hing Dang	Peter Höfner	Ana Sokolova
Brijesh Dongol	Daniel James	Kim Solin
Steve Dunne	Mauro Jaskelioff	Tarmo Uustalu
Jonathan Edwards	Björn Lisper	Nicolas Wu
Joao Ferreira	Bruno Oliveira	Andreas Zelend

Local Organization

Pablo Nogueira (Chair)	Universidad Politécnica de Madrid
Ricardo Peña	Universidad Complutense de Madrid
Álvaro García Pérez	IMDEA Software Institute and Universidad Politécnica de Madrid
Manuel Montenegro	Universidad Complutense de Madrid

Host Institutions

- Universidad Complutense de Madrid.
- Universidad Politécnica de Madrid.

Acknowledgements

We are grateful to the Madrid Convention Bureau for their help and support in the organization of the conference. We are also grateful to the Spanish *Ministerio de Economía y Competitividad* for their financial support via Acción Complementaria TIN2011-16141-E.

Table of Contents

Invited Talks

Probabilistic Relational Hoare Logics for Computer-Aided Security Proofs 1
Gilles Barthe, Benjamin Grégoire, and Santiago Zanella Béguelin

The Laws of Programming Unify Process Calculi 7
Tony Hoare and Stephan van Staden

The Geometry of Synthesis: How to Make Hardware Out of Software (Abstract) 23
Dan R. Ghica

Security and Information Flow

Scheduler-Independent Declassification 25
Alexander Lux, Heiko Mantel, and Matthias Perner

Elementary Probability Theory in the Eindhoven Style 48
Carroll Morgan

Synchronous and Real-Time Systems

Scheduling and Buffer Sizing of n-Synchronous Systems: Typing of Ultimately Periodic Clocks in Lucy-n 74
Louis Mandel and Florence Plateau

Deriving Real-Time Action Systems Controllers from Multiscale System Specifications 102
Brijesh Dongol and Ian J. Hayes

Algorithms and Games

Calculating Graph Algorithms for Dominance and Shortest Path 132
Ilya Sergey, Jan Midtgaard, and Dave Clarke

First-Past-the-Post Games 157
Roland Backhouse

Program Calculi

Reverse Exchange for Concurrency and Local Reasoning 177
Han-Hing Dang and Bernhard Möller

Unifying Correctness Statements 198
Walter Guttmann

Tool Support

Dependently Typed Programming Based on Automated Theorem Proving 220
Alasdair Armstrong, Simon Foster, and Georg Struth

Algebras and Datatypes

An Algebraic Calculus of Database Preferences 241
Bernhard Möller, Patrick Roocks, and Markus Endres

Modular Tree Automata 263
Patrick Bahr

Categorical Functional Programming

Constructing Applicative Functors 300
Ross Paterson

Kan Extensions for Program Optimisation *Or:* Art and Dan Explain an Old Trick 324
Ralf Hinze

Author Index 363