Lecture Notes in Computer Science 6255

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

Ana Cavalcanti David Deharbe
Marie-Claude Gaudel Jim Woodcock (Eds.)

Theoretical Aspects of Computing – ICTAC 2010

7th International Colloquium
Natal, Rio Grande do Norte, Brazil
September 1-3, 2010
Proceedings

Springer

Volume Editors

Ana Cavalcanti
University of York, Department of Computer Science
York YO10 5DD, United Kingdom
E-mail: ana.cavalcanti@cs.york.ac.uk

David Deharbe
Universidade Federal do Rio Grande do Norte
Departamento de Informática e Matemática Aplicada
Lagoa Nova 59072-970 Natal-RN, Brazil
E-mail: deharbe@gmail.com

Marie-Claude Gaudel
Université de Paris-Sud, LRI
91405, Orsay Cedex, France
E-mail: mcg@lri.fr

Jim Woodcock
University of York, Department of Computer Science
York YO10 5DD, United Kingdom
E-mail: jim@cs.york.ac.uk

Library of Congress Control Number: 2010932035

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

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

ISSN 0302-9743
ISBN-10 3-642-14807-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-14807-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

The now well-established series of International Colloquia on Theoretical Aspects of Computing (ICTAC) brings together practitioners and researchers from academia, industry and government to present research results, and exchange experience and ideas. Beyond these scholarly goals, another main purpose is to promote cooperation in research and education between participants and their institutions, from developing and industrial countries.

This volume contains the papers presented at ICTAC 2010. It was held during September 1–3 in the city of Natal, Rio Grande do Norte, Brazil.

There were 68 submissions by authors from 24 countries all around the world. Each submission was reviewed by at least three, and on average four, Program Committee members and external reviewers. After extensive discussions, they decided to accept the 23 (regular) papers presented here. Authors of a selection of these papers were invited to submit an extended version of their work to a special issue of the *Theoretical Computer Science* journal.

Seven of the papers were part of a special track including one paper on "Formal Aspects of Software Testing", and six on the "Grand Challenge in Verified Software." The special track was jointly organized by Marie-Claude Gaudel, from the Université de Paris-Sud, and Jim Woodcock, from the University of York.

The program also included invited talks. Ian Hayes, from the University of Queensland, Australia, was the FME lecturer. This volume includes his invited paper on a program algebra for sequential programs. We gratefully acknowledge the support of Formal Methods Europe in making the participation of Ian Hayes possible. A second invited paper is by Paulo Borba, from the Universidade Federal de Pernambuco, Brazil. His paper describes a refinement theory for software product lines. Stephan Merz, from INRIA, gave an invited talk on a proof assistant for TLA$^+$; the abstract for his talk is also presented here. Wolfram Schulte, from Microsoft Research, gave a talk on verification of C programs.

ICTAC 2010 was organized jointly by the Universidade Federal do Rio Grande do Norte, Brazil, and the University of York, UK. EasyChair was used to manage the submissions, their reviewing, and the proceedings production.

We are grateful to all members of the Program and Organizing Committees, and to all referees for their hard work. The support and encouragement of the Steering Committee were invaluable assets.

Finally, we would like to thank all the authors of the invited and submitted papers, and all the participants of the conference. They are the main focus of the whole event. We hope they enjoyed it.

September 2010

Ana Cavalcanti
David Déharbe

Conference Organization

Steering Committee

John Fitzgerald
Martin Leucker
Zhiming Liu (Chair)
Tobias Nipkow
Augusto Sampaio
Natarajan Shankar
Jim Woodcock

Program Chairs

Ana Cavalcanti
David Déharbe

Special Track Chairs

Marie-Claude Gaudel
Jim Woodcock

Program Committee

Bernhard Aichernig
Jonathan Bowen
Michael Butler
Antonio Cerone
John Fitzgerald
Pascal Fontaine
Lindsay Groves
Robert Hierons
Maciej Koutny
Martin Leucker
Patrícia Machado
Marius Minea
Tobias Nipkow
Paritosh Pandya
Anders Ravn
Markus Roggenbach
Bernhard Schätz
Emil Sekerinski

Keijiro Araki
Christiano Braga
Andrew Butterfield
Jim Davies
Wan Fokkink
Marcelo Frias
Michael Hansen
Moonzoo Kim
Pascale Le Gall
Zhiming Liu
Ali Mili
Michael Mislove
José Nuno Oliveira
Alberto Pardo
Leila Ribeiro
Augusto Sampaio
Gerhard Schellhorn
Natarajan Shankar

Marjan Sirjani
Dang Van Hung
Helmut Veith
Martin Wirsing
Husnu Yenigun
Jin Song Dong
Dániel Varró
Ji Wang
Burkhart Wolff
Naijun Zhan

Local Organization

David Déharbe
Anamaria Moreira
Bartira Rocha
Marcel Oliveira
Martin Musicante

External Reviewers

Nazareno Aguirre
Luís Barbosa
Andreas Bauer
Jasmin Blanchette
Simon Bumler
Pablo Castro
John Colley
Simon Doherty
Bruno Dutertre
Zoltán Égel
Miguel Ferreira
Alexander Gruler
Julian Haselmayr
Andreas Holzer
Hans Hüttel
Elisabeth Jöbstl
Narges Khakpour
Yunho Kim
Willibald Krenn
Shigeru Kusakabe
Jiang Liu
Anh Luu
Hans van Maaren
Bruno Montalto
Florian Nafz
Carlos Olarte
Peter Ölveczky
Sam Owre
Miguel Palomino
Pekka Pihlajasaari
Wilkerson Andrade
Thomas Basuki
Mario Benevides
Harald Brandl
Emanuela Cartaxo
Zhenbang Chen
Nam Dang
Wei Dong
Andrew Edmunds
Ansgar Fehnker
Juan Galeotti
Dominik Haneberg
Pedro Henriques
Andras Horvath
Visar Januzaj
Vineet Kahlon
Ramtin Khosravi
András Kövi
Stefan Kugele
Christian Leuxner
Wanwei Liu
Issam Maamria
Hiroshi Mochio
Martin Musicante
Gethin Norman
Francisco Oliveira
Yoichi Omori
Federica Paci
Ngoc Pham
Jorge Pinto

Carlos Pombo
Abdolbaghi Rezazadeh
Hassen Saïdi
Sylvain Schmitz
Martin Steffen
Volker Stolz
Daniel Thoma
Hoang Truong
Saleem Vighio
Xu Wang
Tjark Weber
Shaojie Zhang
Yu Zhang
Liang Zhao
Florian Zuleger

Viorel Preoteasa
Hamideh Sabouri
Abhisekh Sankaran
Leila Silva
Kurt Stenzel
Michael Tautschnig
Bogdan Tofan
Marcos Viera
Shuling Wang
Zhaofei Wang
James Welch
Xian Zhang
Hengjun Zhao
Manchun Zheng

Table of Contents

Invited Papers and Abstract

Invariants and Well-Foundedness in Program Algebra 1
Ian J. Hayes

A Theory of Software Product Line Refinement 15
Paulo Borba, Leopoldo Teixeira, and Rohit Gheyi

The TLA$^+$ Proof System: Building a Heterogeneous Verification Platform 44
Kaustuv Chaudhuri, Damien Doligez, Leslie Lamport, and Stephan Merz

Grammars

Subtyping Algorithm of Regular Tree Grammars with Disjoint Production Rules 45
Lei Chen and Haiming Chen

Minimal Tree Language Extensions: A Keystone of XML Type Compatibility and Evolution 60
Jacques Chabin, Mirian Halfeld-Ferrari, Martin A. Musicante, and Pierre Réty

Tracking Down the Origins of Ambiguity in Context-Free Grammars 76
H.J.S. Basten

Semantics

Prioritized *slotted-Circus* 91
Paweł Gancarski and Andrew Butterfield

A Denotational Semantical Model for Orc Language 106
Qin Li, Huibiao Zhu, and Jifeng He

An Extended cCSP with Stable Failures Semantics 121
Zhenbang Chen and Zhiming Liu

Preference and Non-deterministic Choice 137
Bill Stoddart, Frank Zeyda, and Steve Dunne

Modelling

Material Flow Abstraction of Manufacturing Systems 153
Jewgenij Botaschanjan and Benjamin Hummel

Specification and Verification of a MPI Implementation for a MP-SoC 168
Umberto Souza da Costa, Ivan Soares de Medeiros Júnior, and Marcel Vinicius Medeiros Oliveira

Special Track: Formal Aspects of Software Testing and Grand Challenge in Verified Software

Testing of Abstract Components 184
Bilal Kanso, Marc Aiguier, Frédéric Boulanger, and Assia Touil

Scalable Distributed Concolic Testing: A Case Study on a Flash Storage Platform 199
Yunho Kim, Moonzoo Kim, and Nam Dang

Analyzing a Formal Specification of Mondex Using Model Checking 214
Reng Zeng and Xudong He

Formal Modelling of Separation Kernel Components 230
Andrius Velykis and Leo Freitas

Mechanized Verification with Sharing 245
Gregory Malecha and Greg Morrisett

Industrial-Strength Certified SAT Solving through Verified SAT Proof Checking 260
Ashish Darbari, Bernd Fischer, and João Marques-Silva

Dynamite 2.0: New Features Based on UnSAT-Core Extraction to Improve Verification of Software Requirements 275
Mariano M. Moscato, Carlos Gustavo López Pombo, and Marcelo Fabiùn Frias

Logics

Complete Calculi for Structured Specifications in Fork Algebra 290
Carlos Gustavo Lopez Pombo and Marcelo Fabiùn Frias

Towards Managing Dynamic Reconfiguration of Software Systems in a Categorical Setting 306
Pablo F. Castro, Nazareno M. Aguirre, Carlos Gustavo López Pombo, and Thomas S.E. Maibaum

Characterizing Locality (Encapsulation) with Bisimulation 322
Pablo F. Castro and Tom S.E. Maibaum

Justification Logic and History Based Computation 337
Francisco Bavera and Eduardo Bonelli

Algorithms and Types

A Class of Greedy Algorithms and Its Relation to Greedoids 352
Srinivas Nedunuri, Douglas R. Smith, and William R. Cook

On Arithmetic Computations with Hereditarily Finite Sets, Functions and Types 367
Paul Tarau

A Modality for Safe Resource Sharing and Code Reentrancy 382
Rui Shi, Dengping Zhu, and Hongwei Xi

Author Index 397