Lecture Notes in Computer Science 6527

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

Jim Davies Leila Silva Adenilso Simao (Eds.)

Formal Methods: Foundations and Applications

13th Brazilian Symposium on Formal Methods, SBMF 2010
Natal, Brazil, November 8-11, 2010
Revised Selected Papers

Springer

Volume Editors

Jim Davies
Oxford University, Department of Computer Science
Oxford OX1 3QD, UK
E-mail: Jim.Davies@comlab.ox.ac.uk

Leila Silva
Universidade Federal de Sergipe
Departamento de Ciência da Computação e Estatística
CEP 49100-000, Aracaju, SE, Brazil
E-mail: lmas@ufs.br

Adenilso Simao
Avenida Trabalhador São-Carlense, 400 Centro
13566-590, São Carlos, SP, Brazil
E-mail: adenilso@icmc.usp.br

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-19828-1 e-ISBN 978-3-642-19829-8
DOI 10.1007/978-3-642-19829-8
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011922662

CR Subject Classification (1998): D.2.4, D.2, F.3, D.3, D.1, K.6, F.4

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© Springer-Verlag Berlin Heidelberg 2011
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 papers presented at SBMF 2010: the 13th Brazilian Symposium on Formal Methods, organized during the week of November 8, 2010. The conference was held, for the second time, in the city of Natal, Rio Grande do Norte, Brazil, co-located with ICTSS 2010, the 22nd IFIP International Conference on Testing Software and Systems, and SAST 2010, the Brazilian Workshop on Systematic and Automated Software Testing.

The conference programme included three invited talks, given by Constance Heitmeyer (Naval Research Lab, USA), Bill Roscoe (University of Oxford, UK) and David Naumann (Stevens Institute of Technology, USA). It also included two workshops: *Using BOOGIE 2 in the Verification of Spec# Programs*, organized by K. Rustan M. Leino (Microsoft Research) and Rosemary Monahan (National University of Ireland), and *Workshop on B Dissemination (WOBD)*, chaired by Thierry Lecomte (ClearSy, France) on behalf of the DEPLOY project.

There was also an accompanying doctoral research symposium, with presentations from research students working on new developments in the theory and practice of formal methods, and a special session on the development of the formal methods curriculum.

Awards were made to: Wojciech Mostowski and Erik Poll, for the best paper, "Midlet Navigation Graphs in JML"; to Alexandra Silva, for the best paper presentation; to Giselle Reis, for the best doctoral presentation; to Tiago Massoni, for the best use of presentation technology; and to Rolf Hennicker, for the best contribution to the discussions that followed each author's presentation.

A total of 18 research papers were presented at the conference, selected from 55 submissions, and included in revised form in this volume. We are grateful to the Programme Committee, and the additional reviewers, for their hard work in evaluating submissions and suggesting improvements. The papers were presented, by their authors, in seven separate sessions; these sessions were well attended, and we are grateful to the many participants who made additional, thoughtful contributions between, during, and after the paper presentations.

We are grateful to the organizers of this year's conference, the Departamento de Informática e Matemática Aplicada of Rio Grande do Norte (UFRN) and the Brazilian Computer Society (SBC), and also to the sponsors: CNPq, the Brazilian Scientific and Technological Research Council; CAPES, the Brazilian Higher Education Funding Council; The Federal University of Rio Grande do Norte (UFRN); Miranda Computação e Comércio Ltda; SETIRN.

December 2010

Jim Davies
Leila Silva
Adenilso Simão

Organization

Programme Committee

Aline Andrade
David Aspinall
Luis Barbosa
Roberto Bigonha
Michael Butler
Andrew Butterfield
Ana Cavalcanti
Marcio Cornelio
Andrea Corradini
Jim Davies (Co-chair)
David Deharbe
Ewen Denney
Clare Dixon
Rohit Gheyi
Rolf Hennicker
Juliano Iyoda
Zhiming Liu
Gerald Luettgen
Patricia Machado
Ana de Melo
Stephan Merz
Alvaro Moreira
Anamaria Moreira
Carroll Morgan
Alexandre Mota
Arnaldo Moura
David Naumann
Daltro Jose Nunes
Jose Oliveira
Marcel Oliveira (Local Chair)
Alberto Pardo
Alexandre Petrenko
Montréal, Canada
Leila Ribeiro
Augusto Sampaio
Leila Silva (Co-chair)
Adenilso Simão (Co-chair)
Heike Wehrheim
Jim Woodcock

Additional Reviewers

Ludwig Adam
Renato Alexandre Silva
Wilkerson L. Andrade
Tigran Avanesov
Sebastian Bauer
Karine Birnfeld
Filippo Bonchi
Adilson Bonifácio
Florent Bouchy
Alexander Ditter
Arnaud Dury
Adriano Gomes
Bruno Gomes
Rolf Hennicker
Giovanny Lucero
Hugo Macedo
Charles Morisset
Regina Motz
Stan Rosenberg
Asieh Salehi Fathabadi
Paulo Salem da Silva
Luis Sierra
Volker Stolz
Ivan Tierno
Jan Tobias Muehlberg
Walter Vogler
Shuling Wang
James Welch
Mar Yah Said
Sanaz Yeganefard
Jiaqi Zhu

Table of Contents

Directed Model Checking for B: An Evaluation and New Techniques 1
Michael Leuschel and Jens Bendisposto

Midlet Navigation Graphs in JML 17
Wojciech Mostowski and Erik Poll

Runtime Verification for Generic Classes with ConGu2 33
Pedro Crispim, Antónia Lopes, and Vasco T. Vasconcelos

A High-Level Language for Modeling Algorithms and Their Properties 49
Sabina Akhtar, Stephan Merz, and Martin Quinson

A Formal Environment Model for Multi-Agent Systems 64
Paulo Salem da Silva and Ana C.V. de Melo

A Modal Interface Theory with Data Constraints 80
Sebastian S. Bauer, Rolf Hennicker, and Michel Bidoit

Synchronizing Model and Program Refactoring 96
Tiago Massoni, Rohit Gheyi, and Paulo Borba

A Type-Theoretic Framework for Certified Model Transformations 112
Daniel Calegari, Carlos Luna, Nora Szasz, and Álvaro Tasistro

Simulating Truly Concurrent CSP 128
Moritz Kleine and J.W. Sanders

Statistical Verification of Probabilistic Properties with Unbounded Until 144
Håkan L.S. Younes, Edmund M. Clarke, and Paolo Zuliani

Reasoning about Assignments in Recursive Data Structures 161
Alejandro Tamalet and Ken Madlener

Specification of a Localization Component Driven by a Goal-Based Approach: Some Lessons We Learned 177
Abderrahman Matoussi, Frédéric Gervais, and Régine Laleau

A Formal Framework for Specifying and Analyzing Logs as Electronic Evidence 194
Eduardo Mazza, Marie-Laure Potet, and Daniel Le Métayer

Formal Development of a Cardiac Pacemaker: From Specification to Code 210
Artur O. Gomes and Marcel V.M. Oliveira

A Decision Procedure for Bisimilarity of Generalized Regular Expressions 226
Marcello Bonsangue, Georgiana Caltais, Eugen-Ioan Goriac, Dorel Lucanu, Jan Rutten, and Alexandra Silva

Normalization of Linear Horn Clauses 242
Thomas Martin Gawlitza, Helmut Seidl, and Kumar Neeraj Verma

A Graph-Based Implementation for Mechanized Refinement Calculus of OO Programs 258
Zhiming Liu, Charles Morisset, and Shuling Wang

Automating Refinement of *Circus* Programs 274
Frank Zeyda and Ana Cavalcanti

Author Index 291