Lecture Notes in Computer Science 7498

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

Rohit Gheyi David Naumann (Eds.)

Formal Methods: Foundations and Applications

15th Brazilian Symposium, SBMF 2012
Natal, Brazil, September 23-28, 2012
Proceedings

Springer

Volume Editors

Rohit Gheyi
Universidade Federal de Campina Grande
Departamento de Sistemas e Computação
Aprigio Veloso, 882
Campina Grande 58429 900, PB, Brazil
E-mail: rohit@dsc.ufcg.edu.br

David Naumann
Stevens Institute of Technology
Department of Computer Science
Hoboken, NJ 07030, USA
E-mail: naumann@cs.stevens.edu

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-33295-1 e-ISBN 978-3-642-33296-8
DOI 10.1007/978-3-642-33296-8
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012946266

CR Subject Classification (1998): D.2.4-5, D.2, F.3.1, F.4.1-2, D.3, K.6

LNCS Sublibrary: SL 2 – Programming and Software Engineering

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 2012: the 15th Brazilian Symposium on Formal Methods. The conference was held in the city of Natal, Brazil, colocated with CBSoft 2012, the Third Brazilian Conference on Software: Theory and Practice.

The conference program included two invited talks, given by John Rushby (SRI International, USA) and Wolfram Schulte (Microsoft Research, USA).

A total of 14 research papers were presented at the conference and are included in this volume; they were selected from 29 submissions. The submissions came from 12 countries: Argentina, Brazil, Canada, China, France, Germany, Morroco, Portugal, Swiss, Uruguay, the UK, and the USA. There was also a special track for short papers, which are published as a technical report.

The deliberations of the Program Committee and the preparation of these proceedings were handled by EasyChair, which indeed made our lives much easier.

We are grateful to the Program Committee, and the additional reviewers, for their hard work in evaluating submissions and suggesting improvements. SBMF 2012 was organized by Departamento de Informática e Matemática Aplicada da Universidade Federal do Rio Grande do Norte (DIMAP/UFRN) under the auspices of the Brazilian Computer Society (SBC). We are very thankful of the organizer of this year's conference, David Deharbe (UFRN), and we are specially thankful to CBSoft2012 organizers Nélio Cacho (DIMAP/UFRN), Frederico Lopes (DIMAP/UFRN), and Gibeon Aquino (DIMAP/UFRN), who arranged everything and made the conference run smoothly.

The conference was sponsored by the following organizations, which we thank for their generous support:

- CNPq, the Brazilian Scientific and Technological Research Council
- CAPES, the Brazilian Higher Education Funding Council
- Microsoft Research
- Universidade Federal do Rio Grande do Norte

July 2012

Rohit Gheyi
David Naumann

Organization

Steering Committee

Jim Davies	University of Oxford, UK
Rohit Gheyi	UFCG, Brazil (Co-chair)
Juliano Iyoda	UFPE, Brazil
Carroll Morgan	University of New South Wales, UK
David Naumann	Stevens Institute of Technology, USA (Co-chair)
Marcel Oliveira	UFRN, Brazil
Adenilso Simao	ICMC/USP, Brazil
Jim Woodcock	University of York, UK

Program Chairs

Rohit Gheyi	UFCG, Brazil
David Naumann	Stevens Institute of Technology, USA

Program Committee

Aline Andrade	UFBA, Brazil
Luis Barbosa	Universidade do Minho, Portugal
Roberto Bigonha	UFMG, Brazil
Christiano Braga	UFF, Brazil
Michael Butler	University of Southampton, UK
Andrew Butterfield	Trinity College Dublin, Ireland
Ana Cavalcanti	University of York, UK
Márcio Cornélio	UFPE, Brazil
Andrea Corradini	Università di Pisa, Italy
Jim Davies	University of Oxford, UK
David Deharbe	UFRN, Brazil
Ewen Denney	SGT/NASA Ames, USA
Clare Dixon	University of Liverpool, UK
Jorge Figueiredo	UFCG, Brazil
Rohit Gheyi	UFCG, Brazil
John Harrison	Intel Corporation, USA
Rolf Hennicker	Ludwig-Maximilians-Universität München, Germany
Juliano Iyoda	UFPE, Brazil
Zhiming Liu	UNU-IIST, China
Gerald Luettgen	University of Bamberg, Germany

Patricia Machado	UFCG, Brazil
Tiago Massoni	UFCG, Brazil
Ana Melo	USP, Brazil
Stephan Merz	INRIA Lorraine, France
Alvaro Moreira	UFRGS, Brazil
Anamaria Moreira	UFRN, Brazil
Carroll Morgan	University of New South Wales, UK
Alexandre Mota	UFPE, Brazil
Arnaldo Moura	Unicamp, Brazil
David Naumann	Stevens Institute of Technology, USA
Daltro Nunes	UFRGS, Brazil
Jose Oliveira	Universidade do Minho, Portugal
Marcel Oliveira	UFRN, Brazil
Alberto Pardo	Universidad de la República, Uruguay
Alexandre Petrenko	CRIM, Canada
Leila Ribeiro	UFRGS, Brazil
Augusto Sampaio	UFPE, Brazil
Leila Silva	UFS, Brazil
Adenilso Simao	ICMC/USP, Brazil
Heike Wehrheim	University of Paderborn, Germany

Additional Reviewers

Almeida, José
Barbosa, Paulo
Costa, Umberto
de Vink, Erik
Duarte, Lucio
Dury, Arnaud
Rosa, Cristián
Sierra, Luis
Silva, Paulo
Sun, Meng
Wang, Hao

Table of Contents

The Versatile Synchronous Observer 1
John Rushby

Thirteen Years of Automated Code Analysis at Microsoft 2
Wolfram Schulte

Model Checking Propositional Deontic Temporal Logic via a μ-Calculus Characterization 3
Araceli Acosta, Cecilia Kilmurray, Pablo F. Castro, and Nazareno M. Aguirre

An Approach Using the B Method to Formal Verification of PLC Programs in an Industrial Setting 19
Haniel Barbosa and David Déharbe

Palytoxin Inhibits the Sodium-Potassium Pump – An Investigation of an Electrophysiological Model Using Probabilistic Model Checking 35
Fernando A.F. Braz, Jader S. Cruz, Alessandra C. Faria-Campos, and Sérgio V.A. Campos

BETA: A B Based Testing Approach 51
Ernesto C.B. de Matos and Anamaria Martins Moreira

A Process Algebra Based Strategy for Generating Test Vectors from SCR Specifications 67
Gustavo Carvalho, Diogo Falcão, Alexandre Mota, and Augusto Sampaio

Specification Patterns for Properties over Reachable States of Graph Grammars 83
Simone André da Costa Cavalheiro, Luciana Foss, and Leila Ribeiro

Compositionality and Refinement in Model-Driven Engineering 99
Jim Davies, Jeremy Gibbons, David Milward, and James Welch

Identifying Hardware Failures Systematically 115
André Didier and Alexandre Mota

Investigating Time Properties of Interrupt-Driven Programs 131
Yanhong Huang, Yongxin Zhao, Jianqi Shi, Huibiao Zhu, and Shengchao Qin

Specifying and Verifying Declarative Fluent Temporal Logic Properties of Workflows 147
Germán Regis, Nicolás Ricci, Nazareno M. Aguirre, and Tom Maibaum

Composition of Model Transformations: A Categorical Framework 163
Christoph Schulz, Michael Löwe, and Harald König

Verification Rules for Exception Handling in Eiffel 179
Emil Sekerinski and Tian Zhang

A Sound Reduction of Persistent-Sets for Deadlock Detection in MPI Applications 194
Subodh Sharma, Ganesh Gopalakrishnan, and Greg Bronevetsky

Alternating-Time Temporal Logic in the Calculus of (Co)Inductive Constructions 210
Dante Zanarini, Carlos Luna, and Luis Sierra

Author Index 227