Lecture Notes in Computer Science 10321

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

Editorial Board

David Hutchison
Lancaster University, Lancaster, UK
Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA
Josef Kittler
University of Surrey, Guildford, UK
Jon M. Kleinberg
Cornell University, Ithaca, NY, USA
Friedemann Mattern
ETH Zurich, Zurich, Switzerland
John C. Mitchell
Stanford University, Stanford, CA, USA
Moni Naor
Weizmann Institute of Science, Rehovot, Israel
C. Pandu Rangan
Indian Institute of Technology, Madras, India
Bernhard Steffen
TU Dortmund University, Dortmund, Germany
Demetri Terzopoulos
University of California, Los Angeles, CA, USA
Doug Tygar
University of California, Berkeley, CA, USA
Gerhard Weikum
Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at http://www.springer.com/series/7408

Ahmed Bouajjani · Alexandra Silva (Eds.)

Formal Techniques for Distributed Objects, Components, and Systems

37th IFIP WG 6.1 International Conference, FORTE 2017
Held as Part of the 12th International Federated Conference on Distributed Computing Techniques, DisCoTec 2017
Neuchâtel, Switzerland, June 19–22, 2017
Proceedings

Springer

Editors
Ahmed Bouajjani
University Paris Diderot
Paris
France

Alexandra Silva
University College London
London
UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-60224-0 ISBN 978-3-319-60225-7 (eBook)
DOI 10.1007/978-3-319-60225-7

Library of Congress Control Number: 2017943019

LNCS Sublibrary: SL2 – Programming and Software Engineering

© IFIP International Federation for Information Processing 2017
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, 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.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

The 12th International Federated Conference on Distributed Computing Techniques (DisCoTec) took place in Neuchâtel, Switzerland, during June 19–22, 2017. It was organized by the Institute of Computer Science of the University of Neuchâtel.

The DisCoTec series is one of the major events sponsored by the International Federation for Information Processing (IFIP). It comprises three conferences:

- COORDINATION, the IFIP WG6.1 International Conference on Coordination Models and Languages
- DAIS, the IFIP WG6.1 International Conference on Distributed Applications and Interoperable Systems
- FORTE, the IFIP WG6.1 International Conference on Formal Techniques for Distributed Objects, Components and Systems

Together, these conferences cover a broad spectrum of distributed computing subjects, ranging from theoretical foundations and formal description techniques to systems research issues.

Each day of the federated event began with a plenary speaker nominated by one of the conferences. The three invited speakers were Prof. Giovanna Di Marzo Serugendo (UniGE, Switzerland), Dr. Marko Vukolić (IBM Research, Switzerland), and Dr. Rupak Majumdar (MPI, Germany).

Associated with the federated event were also three satellite events that took place during June 21–22, 2017:

- The 10th Workshop on Interaction and Concurrency Experience (ICE)
- The 4th Workshop on Security in Highly Connected IT Systems (SHCIS)
- The EBSIS-sponsored session on Dependability and Interoperability with Event-Based Systems (DIEBS)

Sincere thanks go to the chairs and members of the Program and Steering Committees of the aforementioned conferences and workshops for their highly appreciated efforts. The organization of DisCoTec 2017 was only possible thanks to the dedicated work of the Organizing Committee, including Ivan Lanese (publicity chair), Romain Rouvoy (workshop chair), Peter Kropf (finance chair), and Aurélien Havet (webmaster), as well as all the students and colleagues who volunteered their time to help. Finally, many thanks go to IFIP WG6.1 for sponsoring this event, Springer's *Lecture Notes in Computer Science* for their support and sponsorship, and EasyChair for providing the reviewing infrastructure.

April 2017

Pascal Felber
Valerio Schiavoni

Preface

This volume contains the papers presented at FORTE 2017, the 37th IFIP International Conference on Formal Techniques for Distributed Objects, Components and Systems. This conference was organized as part of the 12th International Federated Conference on Distributed Computing Techniques (DisCoTec) and was held during June 19–22, 2017, in Neuchâtel (Switzerland).

The FORTE conference series represents a forum for fundamental research on theory, models, tools, and applications for distributed systems. The conference encourages contributions that combine theory and practice, and that exploit formal methods and theoretical foundations to present novel solutions to problems arising from the development of distributed systems. FORTE covers distributed computing models and formal specification, testing, and verification methods. The application domains include all kinds of application-level distributed systems, telecommunication services, Internet, embedded, and real-time systems, as well as networking and communication security and reliability.

After careful deliberations, the Program Committee selected 17 papers for presentation, of which three are short papers and one is a tool paper. In addition to these papers, this volume contains an abstract of the invited talk by an outstanding researcher, Rupak Majumdar (Max Planck Institute for Software Systems, Kaiserslautern, Germany), on "Systematic Testing for Asynchronous Programs." We warmly thank him for his participation. We also thank all the authors for their submissions, their willingness to continue improving their papers, and their presentations!

Conferences like FORTE rely on the willingness of experts to serve in the Program Committee; their professionalism and their helpfulness were exemplary. We thank the members of the Program Committee and all the external reviewers for their excellent work. We would like also to thank the general chair, Pascal Felber (University of Neuchâtel, Switzerland), and the support of the Organizing Committee chaired by Valerio Schiavoni (University of Neuchâtel, Switzerland), and the publicity chair, Ivan Lanese (University of Bologna, Italy). We also thank the members of the Steering Committee for their helpful advice. For the work of the Program Committee and the compilation of the proceedings, the EasyChair system was employed; it freed us from many technical matters and allowed us to focus on the program, for which we are grateful.

April 2017

Ahmed Bouajjani
Alexandra Silva

Organization

Program Committee

Elvira Albert	Complutense University of Madrid, Spain
Luis Barbosa	Universidade do Minho, Portugal
Gilles Barthe	IMDEA Software Institute, Spain
Borzoo Bonakdarpour	McMaster University, Canada
Ahmed Bouajjani	IRIF, University of Paris Diderot, France
Franck Cassez	Macquarie University, Australia
Hana Chockler	King's College London, UK
Pedro D'Argenio	Universidad Nacional de Córdoba - CONICET, Argentina
Frank De Boer	CWI, The Netherlands
Mariangiola Dezani-Ciancaglini	Università di Torino, Italy
Cezara Dragoi	IST, Austria
Michael Emmi	Bell Labs, Nokia, USA
Carla Ferreira	CITI/DI/FCT/UNL, Portugal
Bart Jacobs	Katholieke Universiteit Leuven, Belgium
Sophia Knight	Uppsala University, Sweden
Annabelle McIver	Macquarie University, Australia
Stephan Merz	Inria Nancy, France
Stefan Milius	FAU Erlangen, Germany
Catuscia Palamidessi	Inria, France
Corina Pasareanu	CMU/NASA Ames Research Center, USA
Anna Philippou	University of Cyprus
Sanjiva Prasad	Indian Institute of Technology Delhi, India
Alexandra Silva	University College London, UK
Ana Sokolova	University of Salzburg, Austria
Marielle Stoelinga	University of Twente, The Netherlands

Additional Reviewers

Åman Pohjola, Johannes	Göthel, Thomas
Bacci, Giovanni	Isabel, Miguel
Brett, Noel	Jakšić, Svetlana
Chen, Tzu-Chun	Jensen, Peter Gjøl
Coppo, Mario	Klin, Bartek
Dodds, Mike	Kouzapas, Dimitrios
Gerhold, Marcus	Köpf, Boris
Gutkovas, Ramūnas	Lee, Matias David

Lienhardt, Michael
Luckow, Kasper
Madeira, Alexandre
Mamouras, Konstantinos
Maubert, Bastien
Meijer, Jeroen
Montenegro, Manuel
Monti, Raúl E.
Mousavi, Mohammadreza
Pang, Jun
Petrisan, Daniela
Proenca, Jose
Sammartino, Matteo
Schivo, Stefano
Schlatte, Rudolf
Siddique, Umair
Toninho, Bernardo

Systematic Testing for Asynchronous Programs (Invited Talk)

Rupak Majumdar

MPI-SWS, Kaiserslautern, Germany

Asynchronous programming is a generic term for concurrent programming with cooperative task management and shows up in many different applications. For example, many programming models for the web, smartphone and cloud-backed applications, server applications, and embedded systems implement programming in this style. In all these scenarios, while programs can be very efficient, the manual management of resources and asynchronous procedures can make programming quite difficult. The natural control flow of a task is obscured and the programmer must ensure correct behavior for all possible orderings of external events. Specifically, the global state of the program can change between the time an asynchronous procedure is posted and the time the scheduler picks and runs it.

In this talk, I will describe algorithmic analysis techniques for systematic testing of asynchronous programs. I will talk about formal models for asynchronous programs and verification and systematic testing techniques for these models. The results will use connections between asynchronous programs and classical concurrency models such as Petri nets, partial order reductions for asynchronous programs, as well as combinatorial constructions of small test suites with formal guarantees of coverage.

Contents

Session Types for Link Failures 1
Manuel Adameit, Kirstin Peters, and Uwe Nestmann

Learning-Based Compositional Parameter Synthesis for Event-Recording Automata 17
Étienne André and Shang-Wei Lin

Modularising Opacity Verification for Hybrid Transactional Memory 33
Alasdair Armstrong and Brijesh Dongol

Proving Opacity via Linearizability: A Sound and Complete Method. 50
Alasdair Armstrong, Brijesh Dongol, and Simon Doherty

On Futures for Streaming Data in ABS (Short Paper) 67
Keyvan Azadbakht, Nikolaos Bezirgiannis, and Frank S. de Boer

Session-Based Concurrency, Reactively 74
Mauricio Cano, Jaime Arias, and Jorge A. Pérez

Procedural Choreographic Programming. 92
Luís Cruz-Filipe and Fabrizio Montesi

An Observational Approach to Defining Linearizability on Weak Memory Models 108
John Derrick and Graeme Smith

Applying a Dependency Mechanism for Voting Protocol Models Using Event-B 124
J. Paul Gibson, Souad Kherroubi, and Dominique Méry

Weak Simulation Quasimetric in a Gossip Scenario. 139
Ruggero Lanotte, Massimo Merro, and Simone Tini

Reasoning About Distributed Secrets 156
Nicolás Bordenabe, Annabelle McIver, Carroll Morgan, and Tahiry Rabehaja

Classical Higher-Order Processes (Short Paper). 171
Fabrizio Montesi

Weak Nominal Modal Logic 179
Joachim Parrow, Tjark Weber, Johannes Borgström, and Lars-Henrik Eriksson

Type Inference of Simulink Hierarchical Block Diagrams in Isabelle 194
Viorel Preoteasa, Iulia Dragomir, and Stavros Tripakis

Creating Büchi Automata for Multi-valued Model Checking 210
Stefan J.J. Vijzelaar and Wan J. Fokkink

Privacy Assessment Using Static Taint Analysis (Tool Paper) 225
Marcel von Maltitz, Cornelius Diekmann, and Georg Carle

EPTL - A Temporal Logic for Weakly Consistent Systems (Short Paper) 236
Mathias Weber, Annette Bieniusa, and Arnd Poetzsch-Heffter

Author Index 243