

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 Zürich, Zürich, 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>

Susanne Graf · Mahesh Viswanathan (Eds.)

Formal Techniques for Distributed Objects, Components, and Systems

35th IFIP WG 6.1 International Conference, FORTE 2015
Held as Part of the 10th International Federated Conference
on Distributed Computing Techniques, DisCoTec 2015
Grenoble, France, June 2–4, 2015
Proceedings

Editors

Susanne Graf
Université Grenoble Alpes / VERIMAG
Grenoble
France

Mahesh Viswanathan
University of Illinois at Urbana-Champaign
Urbana, Illinois
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-19194-2 ISBN 978-3-319-19195-9 (eBook)
DOI 10.1007/978-3-319-19195-9

Library of Congress Control Number: 2015939161

LNCS Sublibrary: SL2 – Programming and Software Engineering

Springer Cham Heidelberg New York Dordrecht London

© IFIP International Federation for Information Processing 2015

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.

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media
(www.springer.com)

Foreword

The 10th International Federated Conference on Distributed Computing Techniques (DisCoTec) took place in Montbonnot, near Grenoble, France, during June 2–5, 2015. It was hosted and organized by INRIA, the French National Research Institute in Computer Science and Control. 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 keynote speaker nominated by one of the conferences. The three invited speakers were Alois Ferscha (Johannes Kepler Universität, Linz, Austria), Leslie Lamport (Microsoft Research, USA), and Willy Zwaenepoel (EPFL, Lausanne, Switzerland).

Associated with the federated event were also three satellite workshops, that took place on June 5, 2015:

- The 2nd International Workshop on Formal Reasoning in Distributed Algorithms (FRIDA), with a keynote speech by Leslie Lamport (Microsoft Research, USA).
- The 8th International Workshop on Interaction and Concurrency Experience (ICE), with keynote lectures by Jade Alglave (University College London, UK) and Steve Ross-Talbot (ZDLC, Cognizant Technology Solutions, London, UK).
- The 2nd International Workshop on Meta Models for Process Languages (MeMo).

Sincere thanks go to the chairs and members of the Program and Steering Committees of the involved conferences and workshops for their highly appreciated efforts. Organizing DisCoTec was only possible thanks to the dedicated work of the Organizing Committee from INRIA Grenoble-Rhône-Alpes, including Sophie Azzaro, Vanessa Peregrin, Martine Consigny, Alain Kersaudy, Sophie Quinton, Jean-Bernard Stefani, and the excellent support from Catherine Nuel and the people at Insight Outside. Finally, many thanks go to IFIP WG6.1 for sponsoring this event, and to INRIA Grenoble-Rhône-Alpes and its Director Patrick Gros for their support and sponsorship.

Alain Girault
DisCoTec 2015 General Chair

DisCoTec Steering Committee

Farhad Arbab	CWI, Amsterdam, The Netherlands
Rocco De Nicola	IMT Lucca, Italy
Kurt Geihs	University of Kassel, Germany
Michele Loreti	University of Florence, Italy
Elie Najm	Telecom ParisTech, France (Chair)
Rui Oliveira	University of Minho, Portugal
Jean-Bernard Stefani	Inria Grenoble - Rhône-Alpes, France
Uwe Nestmann	Technical University of Berlin, Germany

Preface

This volume contains the proceedings of FORTE 2015, the 35th IFIP International Conference on Formal Techniques for Distributed Objects, Components and Systems. This conference was organized as part of the 10th International Federated Conference on Distributed Computing Techniques (DisCoTec) and was held in Grenoble, France between June 2–4, 2015.

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.

We received a total of 53 full paper submissions for review. Each submission was reviewed by at least three members of the Program Committee. Based on high-quality reviews, and a thorough (electronic) discussion by the Program Committee, we selected 15 papers for presentation at the conference and for publication in this volume.

Leslie Lamport (Microsoft Research) was keynote speaker of FORTE 2015. Leslie received the Turing Award in 2013. He is known for his seminal contributions in distributed systems. He has developed algorithms, formal models, and verification methods for distributed systems. Leslie's keynote lecture was on Temporal Logic of Actions.

We would like to thank all those who contributed to the success of FORTE 2015: the authors, for submitting high-quality work to FORTE 2015; the Program Committee and the external reviewers, for providing constructive, high-quality reviews, an efficient discussion, and a fair selection of papers; the invited speaker for an inspiring talk; and, of course, all the attendees of FORTE 2015. We are also grateful to the DisCoTec General Chair, Alain Girault, Organization Chair, Jean-Bernard Stefani, and all members of their local organization team. The EasyChair conference management system facilitated PC discussions, and the preparation of these proceedings. Thank You.

June 2015

Susanne Graf
Mahesh Viswanathan

Organization

Program Committee Chairs

Susanne Graf	VERIMAG & CNRS, Grenoble, France
Mahesh Viswanathan	University of Illinois at Urbana-Champaign, USA

Program Committee Members

Erika Abraham	RWTH Aachen University, Germany
Luca Aceto	Reykjavik University, Iceland
S. Akshay	IIT Bombay, India
Paul Attie	American University of Beirut, Lebanon
Rohit Chadha	University of Missouri, USA
Rance Cleaveland	University of Maryland, USA
Frank de Boer	CWI, Amsterdam, The Netherlands
Borzoo Bonakdarpour	McMaster University, Ontario, Canada
Michele Boreale	Università degli Studi di Firenze, Italy
Stephanie Delaune	CNRS & ENS Cachan, France
Wan Fokkink	Vrije Universiteit Amsterdam, The Netherlands
Gregor Goessler	Inria Grenoble, France
Gerard Holzmann	Jet Propulsion Laboratory, Pasadena, CA, USA
Alan Jeffrey	Alcatel-Lucent Bell Labs, USA
Petr Kuznetsov	Telecom ParisTech, France
Ivan Lanese	University of Bologna/INRIA, Italy
Kim Larsen	University of Aalborg, Denmark
Antonia Lopes	University of Lisbon, Portugal
Stephan Merz	LORIA & INRIA Nancy, France
Catuscia Palamidessi	INRIA Saclay, France
Alan Schmitt	IRISA & INRIA Rennes, France

Steering Committee

Erika Abraham	RWTH Aachen, Germany
Dirk Beyer	University of Passau, Germany
Michele Boreale	Università degli Studi di Firenze, Italy
Einar Broch Johnsen	University of Oslo, Norway
Frank de Boer	CWI, Amsterdam, The Netherlands
Holger Giese	University of Potsdam, Germany
Catuscia Palamidessi	INRIA, Saclay, France
Grigore Rosu	University of Illinois at Urbana-Champaign, USA
Jean-Bernard Stefani	INRIA, Grenoble, France (Chair)
Heike Wehrheim	University of Paderborn, Germany

Additional Reviewers

Agrawal, Shreya
Astefanoaei, Lacramioara
Azadbakht, Keyvan
Bauer, Matthew
Bettini, Lorenzo
Bezirgiannis, Nikolaos
Bracciali, Andrea
Bresolin, Davide
Castellani, Ilaria
Corzilius, Florian
Dalsgaard, Andreas Engelbredt
Dang, Thao
Della Monica, Dario
Demangeon, Romain
Denielou, Pierre-Malo
Di Giusto, Cinzia
Dokter, Kasper
Enea, Constantin
Fehnker, Ansgar
Foshammer, Louise
Francalanza, Adrian
Franco, Juliana
Griffith, Dennis
Guha, Shibashis
Henrio, Ludovic
Herbreteau, Frédéric
Hirsch, Martin
Höfner, Peter
Jongmans, Sung-Shik T.Q.
Kemper, Stephanie
Kini, Dileep
Laurent, Mounier

Lenglet, Sergueï
Loreti, Michele
Mandel, Louis
Marques, Eduardo R.B.
Martins, Francisco
Massink, Mieke
Mateescu, Radu
Mezzina, Claudio Antares
Najm, Elie
Ober, Iulian
Padovani, Luca
Peressotti, Marco
Pessaux, François
Phawade, Ramchandra
Poulsen, Danny Bøgsted
Prisacariu, Cristian
Pérez, Jorge A.
Quinton, Sophie
Ravi, Srivatsan
Reniers, Michel
Rezine, Ahmed
S. Krishna
Sangnier, Arnaud
Serbanescu, Vlad Nicolae
Sirjani, Marjan
Tapia Tarifa, Silvia Lizeth
Tiezzi, Francesco
Trivedi, Ashutosh
Valencia, Frank
Wognsen, Erik Ramsgaard
Xue, Bingtian

Contents

Ensuring Properties of Distributed Systems

Types for Deadlock-Free Higher-Order Programs	3
<i>Luca Padovani and Luca Novara</i>	
On Partial Order Semantics for SAT/SMT-Based Symbolic Encodings of Weak Memory Concurrency	19
<i>Alex Horn and Daniel Kroening</i>	
A Strategy for Automatic Verification of Stabilization of Distributed Algorithms	35
<i>Ritwika Ghosh and Sayan Mitra</i>	
Faster Linearizability Checking Via P -Compositionality	50
<i>Alex Horn and Daniel Kroening</i>	
Translation Validation for Synchronous Data-Flow Specification in the SIGNAL Compiler	66
<i>Van Chan Ngo, Jean-Pierre Talpin, and Thierry Gautier</i>	

Formal Models of Concurrent and Distributed Systems

Dynamic Causality in Event Structures	83
<i>Youssef Arbach, David Karcher, Kirstin Peters, and Uwe Nestmann</i>	
Loop Freedom in AODVv2	98
<i>Kedar S. Namjoshi and Richard J. Trefler</i>	
Code Mobility Meets Self-organisation: A Higher-Order Calculus of Computational Fields.	113
<i>Ferruccio Damiani, Mirko Viroli, Danilo Pianini, and Jacob Beal</i>	

Real Time Systems

Timely Dataflow: A Model	131
<i>Martín Abadi and Michael Isard</i>	
Difference Bound Constraint Abstraction for Timed Automata Reachability Checking	146
<i>Weifeng Wang and Li Jiao</i>	

Compliance and Subtyping in Timed Session Types 161
*Massimo Bartoletti, Tiziana Cimoli, Maurizio Murgia,
Alessandro Sebastian Podda, and Livio Pompianu*

Security

Type Checking Privacy Policies in the π -calculus 181
Dimitrios Kouzapas and Anna Philippou

Extending Testing Automata to All LTL 196
Ala Eddine Ben Salem

Efficient Verification Techniques

Simple Isolation for an Actor Abstract Machine 213
Benoit Claudel, Quentin Sabah, and Jean-Bernard Stefani

Sliced Path Prefixes: An Effective Method to Enable
Refinement Selection 228
Dirk Beyer, Stefan Löwe, and Philipp Wendler

Author Index 245