

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

For further volumes:

<http://www.springer.com/series/558>

Farhad Arbab Marjan Sirjani (Eds.)

Fundamentals of Software Engineering

5th International Conference, FSEN 2013
Tehran, Iran, April 24-26, 2013
Revised Selected Papers



Springer

Volume Editors

Farhad Arbab

CWI Amsterdam, The Netherlands

E-mail: Farhad.Arbab@cwi.nl

Marjan Sirjani

Reykjavik University, Iceland

E-mail: marjan@ru.is

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-40212-8

e-ISBN 978-3-642-40213-5

DOI 10.1007/978-3-642-40213-5

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2013946950

CR Subject Classification (1998): F.3, D.2, F.1, D.4, F.4, C.2, J.7

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© IFIP International Federation for Information Processing 2013

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The present volume contains the proceedings of the 5th IPM International Conference on Fundamentals of Software Engineering (FSEN), held in Tehran, Iran, April 24–26, 2013. FSEN 2013 was organized by the School of Computer Science at the Institute for Research in Fundamental Sciences (IPM) in Iran, in cooperation with the ACM SIGSOFT and IFIP WG 2.2.

The topics of interest in FSEN span all aspects of formal methods, especially those related to advancing the application of formal methods in software industry and promoting their integration with practical engineering techniques. The Program Committee (PC) of FSEN 2013 consisted of 50 top researchers from 37 different academic institutes in 17 countries. We received 65 submissions from 33 countries, out of which the PC accepted 17 regular papers for the conference program. Each submission was reviewed by at least three independent referees, for its quality, originality, contribution, clarity of presentation, and its relevance to the conference topics.

Three distinguished keynote speakers delivered their lectures at FSEN 2013. Jose Meseguer gave a talk on “Symbolic Formal Methods: Combining the Power of Rewriting, Narrowing, SMT Solving and Model Checking.” Holger Hermanns spoke on “Stochastic, Hybrid and Real-Time Systems: From Foundations to Applications with Modest.” Wolfgang Reisig presented “Service-Oriented Computing: Forthcoming Challenges.”

We thank the Institute for Research in Fundamental Sciences (IPM), Tehran, Iran, for their financial support and local organization of FSEN 2013. We thank the members of the PC for their time, effort, and contributions to making FSEN a quality conference. We thank Hossein Hojjat for his help in preparing this volume. Last but not least, our thanks go to our authors and conference participants, without whose submissions and participation FSEN would not have been possible.

June 2013

Farhad Arbab
Marjan Sirjani

Contents

Unbounded Allocation in Bounded Heaps	1
<i>Jurriaan Rot, Frank de Boer, and Marcello Bonsangue</i>	
On the Complexity of Adding Convergence.	17
<i>Alex Klinkhamer and Ali Ebnenasir</i>	
Deadlock Checking by Data Race Detection	34
<i>Ka I Pun, Martin Steffen, and Volker Stolz</i>	
Delta Modeling and Model Checking of Product Families.	51
<i>Hamideh Sabouri and Ramtin Khosravi</i>	
Lending Petri Nets and Contracts	66
<i>Massimo Bartoletti, Tiziana Cimoli, and G. Michele Pinna</i>	
On Efficiency Preorders.	83
<i>Manish Gaur and S. Arun-Kumar</i>	
Compiling Cooperative Task Management to Continuations.	95
<i>Keiko Nakata and Andri Saar</i>	
Extending UPPAAL for the Modeling and Verification of Dynamic Real-Time Systems	111
<i>Abdeljalil Boudjadar, Frits Vaandrager, Jean-Paul Bodeveix, and Mamoun Filali</i>	
Efficient Operational Semantics for EB^3 for Verification of Temporal Properties	133
<i>Dimitris Vekris and Catalin Dima</i>	
Interval Soundness of Resource-Constrained Workflow Nets: Decidability and Repair	150
<i>Elham Ramezani, Natalia Sidorova, and Christian Stahl</i>	
Statistical Model Checking of a Clock Synchronization Protocol for Sensor Networks.	168
<i>Luca Battisti, Damiano Macedonio, and Massimo Merro</i>	
A New Representation of Two-Dimensional Patterns and Applications to Interactive Programming	183
<i>Iulia Teodora Banu-Demergian, Ciprian Ionut Paduraru, and Gheorghe Stefanescu</i>	

Push-Down Automata with Gap-Order Constraints	199
<i>Parosh Aziz Abdulla, Mohamed Faouzi Atig, Giorgio Delzanno, and Andreas Podelski</i>	
Model Checking MANETs with Arbitrary Mobility	217
<i>Fatemeh Ghassemi, Saeide Ahmadi, Wan Fokkink, and Ali Movaghar</i>	
Validating SCTP Simultaneous Open Procedure	233
<i>Somsak Vanit-Anunchai</i>	
Improving Time Bounded Reachability Computations in Interactive Markov Chains	250
<i>Hassan Hatefi and Holger Hermanns</i>	
Checking Compatibility of Web Services Behaviorally	267
<i>Kais Klai and Hanen Ochi</i>	
Author Index	283

Organization

General Chair

Hamid Sarbazi-azad IPM, Iran; Sharif University of Technology, Iran

Steering Committee

Farhad Arbab CWI, The Netherlands; Leiden University,
The Netherlands
Christel Baier University of Dresden, Germany
Frank de Boer CWI, The Netherlands; Leiden University,
The Netherlands
Ali Movaghar IPM, Iran; Sharif University of Technology, Iran
Hamid Sarbazi-azad IPM, Iran; Sharif University of Technology, Iran
Marjan Sirjani Reykjavik University, Iceland
Jan Rutten CWI, The Netherlands; Radboud University
Nijmegen, The Netherlands

Program Chairs

Farhad Arbab CWI, The Netherlands; Leiden University,
The Netherlands
Marjan Sirjani Reykjavik University, Iceland

Program Committee

Mohammad Abdollahi Iran University of Science and Technology, Iran
Azgomi University of Illinois at Urbana-Champaign, USA
Gul Agha University of Groningen, The Netherlands
Marco Aiello CWI and Leiden University, The Netherlands
Farhad Arbab Technical University of Dresden, Germany
Christel Baier University of Amsterdam, The Netherlands
Jan Bergstra Università degli Studi di Verona, Italy
Maria Paola Bonacina University of Waterloo, Canada
Borzoo Bonakdarpour Leiden University, The Netherlands
Marcello Bonsangue University of Bologna, Italy
Mario Bravetti University of Southampton, UK
Michael Butler CWI and Leiden University, The Netherlands
Frank De Boer

Erik De Vink	Technische Universiteit Eindhoven, The Netherlands
Klaus Dräger	Oxford University, UK
Wan Fokkink	Vrije Universiteit Amsterdam, The Netherlands
Lars-Ake Fredlund	Universidad Politécnica de Madrid, Spain
Masahiro Fujita	University of Tokyo, Japan
Maurizio Gabbrielli	University of Bologna, Italy
Fatemeh Ghassemi	University of Tehran, Iran
Carlo Ghezzi	Politecnico di Milano, Italy
Jan Friso Groote	Eindhoven University of Technology, The Netherlands
Radu Grosu	Stony Brook University, USA
Hassan Haghghi	Shahid Beheshti University, Iran
Mohammad Izadi	Sharif University of Technology, Iran
Mohammad Mahdi Jaghoori	CWI, The Netherlands
Einar Broch Johnsen	University of Oslo, Norway
Joost-Pieter Katoen	RWTH Aachen, Germany
Narges Khakpour	KTH, Sweden
Ramtin Khosravi	University of Tehran, Iran
Joost Kok	Leiden University, The Netherlands
Kim Larsen	Aalborg University, Denmark
Zhiming Liu	United Nations University—International Institute for Software Technology, Macao
Sun Meng	Peking University, China
Hassan Mirian-Hosseiniabadi	Sharif University of Technology, Iran
Ugo Montanari	Università di Pisa, Italy
Peter Mosses	Swansea University, UK
Mohammadreza Mousavi	Eindhoven University of Technology, The Netherlands
Ali Movaghar	Sharif University of Technology, Iran
Peter Olveczky	University of Oslo, Norway
Hiren D. Patel	University of Waterloo, Canada
Jose Proenca	Katholieke Universiteit Leuven, Belgium
Philipp Ruemmer	Uppsala University, Sweden
Jan Rutten	CWI and Radboud University Nijmegen, The Netherlands
Gwen Salaün	Grenoble INP—INRIA—LIG, France
Cesar Sanchez	IMDEA Software Institute, Spain
Davide Sangiorgi	University of Bologna, Italy
Wendelin Serwe	INRIA Rhône-Alpes/VASY, France
Marjan Sirjani	Reykjavik University, Iceland
Carolyn Talcott	SRI International, USA
Tayssir Touili	LIAFA, CNRS and University Paris Diderot, France

Local Organization

Hamidreza Shahrabi IPM, Iran

Proceedings Manager

Hossein Hojjat EPFL, Switzerland

Additional Reviewers

Attiogbe, Christian	Jongmans, Sung-Shik T. Q.
Bacci, Giovanni	Khamespanah, Ehsan
Balliu, Musard	Khiri, Johan
Basold, Henning	Kokash, Natallia
Bentea, Lucian	Lampka, Kai
Berg, Manuela	Lisser, Bert
Bulanov, Pavel	Lluch Lafuente, Alberto
Buscemi, Marzia	Macedo, Hugo
Chen, Zhenbang	Madeira, Alexandre
Churchill, Martin	Mauro, Jacopo
Corradini, Andrea	Mousavi, Mohammad Reza
Cranen, Sjoerd	Mukkamala, Raghava Rao
Dalla Preda, Mila	Nizamic, Faris
de Gouw, Stijn	Parkinson, Matthew
Dubslaff, Clemens	Patrignani, Marco
Echenim, Mnacho	Qamar, Nafees
Emerencia, Ando	Roohi, Nima
Faber, Johannes	Salehi Fathabadi, Asieh
Fox, Anthony	Sharma, Arpit
Fu, Hongfei	Snook, Colin
Gadducci, Fabio	Soleimanifard, Siavash
Gerakios, Prodromos	Srba, Jiri
Ghassemi, Fatemeh	Subotic, Pavle
Guan, Nan	Tanhaei, Mohammd
Guanciaie, Roberto	Timmer, Mark
Hafez Qorani, Saleh	Torrini, Paolo
Harkjær Møller, Mikael	Wang, Shuling
Helpa, Christopher	Warriach, Ehsan
Helvensteijn, Michiel	Wu, Stephen
Höftberger, Oliver	Yautsiukhin, Artsiom
Isakovic, Haris	Ye, Lina

**Invited Talks
(Abstracts)**

Symbolic Formal Methods: Combining the Power of Rewriting, Narrowing, SMT Solving and Model Checking

Jose Meseguer

University of Illinois at Urbana-Champaign, Urbana, USA

Symbolic techniques that represent possibly infinite sets of states by symbolic constraints and support decision or semi-decision procedures based on such constraints have become essential to automate large parts of the verification effort and make verification much more scalable. They include: (i) SMT solving; (ii) rewriting- and unification-based techniques, including rewriting and narrowing modulo theories; and (iii) automata-based model checking techniques, which describe infinite sets of states and/or system traces symbolically by various kinds of automata. However, a key problem limiting the applicability of current symbolic techniques is lack of, or limited support for, extensibility. That is, although certain classes of systems can be formalized in ways that allow the application of specific symbolic analysis techniques, many other systems of interest fall outside the scope of such techniques. There is a real need to extend and combine the power of symbolic analysis techniques to cover a much wider class of systems. The talk will present some recent advances towards the goal of combined, extensible symbolic formal methods within the context of rewriting logic and Maude.

Stochastic, Hybrid and Real-Time Systems: From Foundations to Applications with Modest

Holger Hermanns

Saarland University–Computer Science,
Saarbrücken, Germany

Our reliance on complex safety-critical or economically vital systems such as networked automation systems or “smart” power grids increases at an everaccelerating pace. The necessity to study the reliability and performance of these systems is evident, but purely functional models and properties are insufficient in many cases. This has led to the development of integrative approaches that combine probabilities, real-time aspects and continuous dynamics with formal verification.

Today, formal quantitative modelling and analysis is supported by a wide range of tools and formalisms such as PRISM with probabilistic guarded commands, UPPAAL for graphical modelling and verification of timed automata, or hybrid system model checkers like PHAVER. This variety of different languages and tools, however, is a major obstacle for new users seeking to apply formal methods in their field of work.

To overcome these problems, the MODEST [4,6] modelling language and its underlying semantic model of stochastic hybrid automata (SHA) have been designed as an overarching formalism of which many well-known and extensively studied models such as Markov decision processes, probabilistic timed systems or hybrid automata are special cases. The construction and analysis of SHA models is supported by the MODEST TOOLSET [1], which supports analysis with a range of different methods. At the current stage, the following analysis components are available: `prohver` [6] handles probabilistic safety properties for SHA; `mcpta` performs model checking of probabilistic timed automata using PRISM; `mctau` [2] connects to UPPAAL for model checking of timed automata, for which it is more efficient than `mcpta`; and `modes` [3] performs statistical model checking and simulation of stochastic timed automata with an emphasis on the sound handling of nondeterministic models.

The MODEST TOOLSET has been used for a variety of applications with different levels of complexity and of expressiveness. These include *really cool* safety critical hard real-time wireless control applications for bicycles [5] as well

as high-speed trains [6], and innovative electric power grid control strategies [7]. The applications combine different abstraction and analysis techniques supported by the MODEST TOOLSET.

Joint work with Arnd Hartmanns, Saarland University

References

1. The Modest Toolset website, <http://www.modestchecker.net>
2. Bogdoll, J., David, A., Hartmanns, A., and Hermanns, H.: metau: Bridging the gap between Modest and UPPAAL. In: Donaldson, A., Parker, D. (eds.) SPIN 2012. LNCS, vol. 7385, pp. 227–233. Springer, Heidelberg (2012)
3. Bogdoll, J., Hartmanns, A., and Hermanns, H.: Simulation and statistical model checking for Modestly nondeterministic models. In: Schmitt, J.B. (ed.) MMB & DFT 2012. LNCS, vol. 7201, pp. 249–252. Springer, Heidelberg (2012)
4. Bohnenkamp, H.C., D’Argenio, P.R., Hermanns, H., and Katoen, J.-P.: MoDeST: A compositional modeling formalism for hard and softly timed systems. IEEE Transactions on Software Engineering 32(10), 812–830 (2006)
5. Graf, H.B., Hermanns, H., Kulshrestha, J., Peter, J., Vahldiek, A., and Vasudevan, A.: A verified wireless safety critical hard real-time design. In: WOWMOM, pp. 1–9. IEEE (2011)
6. Hahn, E.M., Hartmanns, A., Hermanns, H., and Katoen, J.-P.: A compositional modelling and analysis framework for stochastic hybrid systems. Formal Methods in System Design (2012)
7. Hartmanns, A., Hermanns, H., and Berrang, P.: A comparative analysis of decentralized power grid stabilization strategies. In: Winter Simulation Conference (2012)

Service Oriented Computing: Forthcoming Challenges

Wolfgang Reisig

Humboldt-Universität zu Berlin,
Berlin, Germany

Service-oriented Computing has established itself as a core paradigm of modern software architectures. Nevertheless, some obstacles prevent even more widespread use of service oriented architectures (SOAs). To overcome those obstacles, in particular the following questions have to be addressed:

1. SOAs are more and more implemented in the cloud. To what extent are the stakeholders affected by this change of technology?
2. It turned out useful to conceive not only software components, but also humans and technical systems as service providers and service requesters. How can a unified approach to SOA cope with this?
3. Basic notions such as correctness and equivalence are clear cut and undisputed for classical programs. Are there corresponding generally acceptable and manageable such notions for SOAs?
4. Quick assignment of needed data, software and hardware to services is inevitable for smoothly running SOAs. How can a small, flexible infrastructure guarantee this kind of elasticity?

Those questions cannot seriously be answered on an intuitive, informal level. It is inevitable to model services in a formal framework, with the decisive properties of the services be represented as properties of their formal models. The above questions are then addressed and faithfully solved in the framework of the formal models. To this end we suggest methods and principles of formally modeling and analyzing SOAs.