Lecture Notes in Computer Science

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
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.


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
   Jurriaan Rot, Frank de Boer, and Marcello Bonsangue

On the Complexity of Adding Convergence ...................... 17
   Alex Klinkhamer and Ali Ebnenasir

Deadlock Checking by Data Race Detection ..................... 34
   Ka I Pun, Martin Steffen, and Volker Stolz

Delta Modeling and Model Checking of Product Families ....... 51
   Hamideh Sabouri and Ramtin Khosravi

Lending Petri Nets and Contracts ................................. 66
   Massimo Bartoletti, Tiziana Cimoli, and G. Michele Pinna

On Efficiency Preorders ........................................... 83
   Manish Gaur and S. Arun-Kumar

Compiling Cooperative Task Management to Continuations ....... 95
   Keiko Nakata and Andri Saar

Extending UPPAAL for the Modeling and Verification of Dynamic Real-Time Systems ................................. 111
   Abdeldjalil Boudjadar, Frits Vaandrager, Jean-Paul Bodeveix, and Mamoun Filali

Efficient Operational Semantics for $EB^3$ for Verification of Temporal Properties ................................. 133
   Dimitris Vekris and Catalin Dima

Interval Soundness of Resource-Constrained Workflow Nets:
Decidability and Repair ............................................. 150
   Elham Ramezani, Natalia Sidorova, and Christian Stahl

Statistical Model Checking of a Clock Synchronization Protocol for Sensor Networks ................................. 168
   Luca Battisti, Damiano Macedonio, and Massimo Merro

A New Representation of Two-Dimensional Patterns
and Applications to Interactive Programming .................. 183
   Iulia Teodora Banu-Demergian, Ciprian Ionut Paduraru, and Gheorghe Stefanescu
Push-Down Automata with Gap-Order Constraints ........................................ 199
Parosh Aziz Abdulla, Mohamed Faouzi Atig, Giorgio Delzanno,
and Andreas Podelski

Model Checking MANETs with Arbitrary Mobility .................................... 217
Fatemeh Ghassemi, Saeide Ahmadi, Wan Fokkink,
and Ali Movaghar

Validating SCTP Simultaneous Open Procedure ....................................... 233
Somsak Vanit-Anunchai

Improving Time Bounded Reachability Computations
in Interactive Markov Chains .................................................................... 250
Hassan Hatefi and Holger Hermanns

Checking Compatibility of Web Services Behaviorally ............................ 267
Kais Klai and Hanen Ochi

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

Hamidreza Shahrabi IPM, Iran

Proceedings Manager

Hossein Hojjat EPFL, Switzerland

Additional Reviewers

Attiogbe, Christian
Bacci, Giovanni
Balliu, Musard
Basold, Henning
Bentea, Lucian
Berg, Manuela
Bulanov, Pavel
Buscemi, Marzia
Chen, Zhenbang
Churchill, Martin
Corradini, Andrea
Cranen, Sjoerd
Dalla Preda, Mila
de Gouw, Stijn
Dubslaff, Clemens
Echenim, Mnacho
Emerencia, Ando
Faber, Johannes
Fox, Anthony
Fu, Hongfei
Gadducci, Fabio
Gerakios, Prodromos
Ghassemi, Fatemeh
Guan, Nan
Guanciale, Roberto
Hafez Qorani, Saleh
Harkjaer Møller, Mikael
Helpa, Christopher
Helvensteijn, Michiel
Höftberger, Oliver
Isakovic, Haris

Jongmans, Sung-Shik T. Q.
Khamespanah, Ehsan
Khiri, Johan
Kokash, Natallia
Lampka, Kai
Lisser, Bert
Lluch Lafuente, Alberto
Macedo, Hugo
Madeira, Alexandre
Mauro, Jacopo
Mousavi, Mohammad Reza
Mukkamala, Raghava Rao
Nizamic, Faris
Parkinson, Matthew
Patrignani, Marco
Qamar, Nafees
Roohi, Nima
Salehi Fathabadi, Asieh
Sharma, Arpit
Snook, Colin
Soleimanifard, Siavash
Srba, Jiri
Subotic, Pavle
Tanhaei, Mohammad
Timmer, Mark
Torrini, Paolo
Wang, Shuling
Warriach, Ehsan
Wu, Stephen
Yautsiukhin, Artsiom
Ye, Lina
Invited Talks
(Abstracts)
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, UPPAAAL 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 UPPAAAL 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

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.