Lecture Notes in Computer Science 10886

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

Editorial Board

David Hutchison, UK
Josef Kittler, UK
Friedemann Mattern, Switzerland
Moni Naor, Israel
Bernhard Steffen, Germany
Doug Tygar, USA
Takeo Kanade, USA
Jon M. Kleinberg, USA
John C. Mitchell, USA
C. Pandu Rangan, India
Demetri Terzopoulos, USA
Gerhard Weikum, Germany

Formal Methods

Subline of Lectures Notes in Computer Science

Subline Series Editors

Ana Cavalcanti, University of York, UK
Marie-Claude Gaudel, Université de Paris-Sud, France

Subline Advisory Board

Manfred Broy, TU Munich, Germany
Annabelle McIver, Macquarie University, Sydney, NSW, Australia
Peter Müller, ETH Zurich, Switzerland
Erik de Vink, Eindhoven University of Technology, The Netherlands
Pamela Zave, AT&T Laboratories Research, Bedminster, NJ, USA
More information about this series at http://www.springer.com/series/7407
Message from the STAF Organizers

Software Technologies: Applications and Foundations (STAF) is a federation of leading conferences on software technologies. It provides a loose umbrella organization with a Steering Committee that ensures continuity. The STAF federated event takes place annually. The participating conferences and workshops may vary from year to year, but they all focus on foundational and practical advances in software technology. The conferences address all aspects of software technology, from object-oriented design, testing, mathematical approaches to modeling and verification, transformation, model-driven engineering, aspect-oriented techniques, and tools. STAF was created in 2013 as a follow-up to the TOOLS conference series that played a key role in the deployment of object-oriented technologies. TOOLS was created in 1988 by Jean Bézivin and Bertrand Meyer and STAF 2018 can be considered its 30th birthday.

STAF 2018 took place in Toulouse, France, during June 25–29, 2018, and hosted: five conferences ECMFA 2018, ICGT 2018, ICMT 2018, SEFM 2018, TAP 2018, and the Transformation Tool Contest TTC 2018; eight workshops and associated events. STAF 2018 featured seven internationally renowned keynote speakers, welcomed participants from all around the world, and had the pleasure to host a talk by the founders of the TOOLS conference, Jean Bézivin and Bertrand Meyer.

The STAF 2018 Organizing Committee would like to thank (a) all participants for submitting papers and attending the event, (b) the Program Committees and Steering Committees of all the individual conferences and satellite events for their hard work, (c) the keynote speakers for their thoughtful, insightful, and inspiring talks, and (d) the École Nationale Supérieure d'Electrotechnique, Electronique, Hydraulique et Télécommunications (ENSEEIHT), the Institut National Polytechnique de Toulouse (Toulouse INP), the Institut de Recherche en Informatique de Toulouse (IRIT), the région Occitanie, and all sponsors for their support. A special thanks goes to all the members of the Software and System Reliability Department of the IRIT Laboratory and the members of the INP-Act SAIC, dealing with all the foreseen and unforeseen work to prepare a memorable event.

Marc Pantel
Jean-Michel Bruel
Message from the SEFM Program Chairs

This volume contains the papers presented at SEFM 2018, the 16th International Conference on Software Engineering and Formal Methods, held June 27–29 in Toulouse, France. SEFM 2018 was collocated with STAF 2018.

The SEFM conference aims to bring together leading researchers and practitioners from academia, industry, and government, to advance the state of the art in formal methods, to facilitate their uptake in the software industry, and to encourage their integration within practical software engineering methods and tools. The topics of interest for submission included the following aspects of software engineering and formal methods:

- New frontiers in software architecture: self-adaptive, service-oriented, and cloud computing systems; component-based, object-based, and multi-agent systems; real-time, hybrid, and embedded systems; reconfigurable systems
- Software verification and testing: model checking and theorem proving; verification and validation; probabilistic verification and synthesis; testing
- Software development methods: requirement analysis, modeling, specification, and design; light-weight and scalable formal methods
- Application and technology transfer: case studies, best practices, and experience reports; tool integration
- Security and safety: security and mobility; safety-critical, fault-tolerant, and secure systems; software certification
- Design principles: domain-specific languages, type theory, abstraction, and refinement

SEFM 2018 solicited full research papers describing original research results, case studies and tools, and short papers on new ideas and work in progress, describing new approaches, techniques, and/or tools that are not fully validated yet. We received 58 submissions from 25 different countries. Each submission was reviewed by at least three Program Committee members. We accepted 17 regular papers, with an acceptance rate of 29%. The program also featured two remarkable invited talks:

- Mark Harman (Facebook and University College London): “We Need a Testability Transformation Semantics”

Our first words of thanks go to the Program Committee members and to the external reviewers, who carried out thorough and careful reviews and enabled the assembly of this high-quality work. We thank the authors for their submissions, and for their collaboration in further improving their papers. A special word of thanks goes to our invited speakers, Mark Harman and Andrzej Wasowski, for accepting our invitation and for their very stimulating contributions. We also thank the local Organizing
Committee of STAF 2018, who largely contributed to the success of this event. We also thank the developers and maintainers of the EasyChair conference management system, which was of great help in handling the paper submission, reviewing, discussion, and assembly of the proceedings. Finally, we are most grateful to Alexander Knüppel, who provided invaluable help in the preparation of the conference website and proceedings.

June 2018

Einar Broch Johnsen
Ina Schaefer
Organization

Steering Committee

Manfred Broy
Radu Calinescu
Antonio Cerone
Alessandro Cimatti
Rocco De Nicola
Mike Hinchey
Paddy Krishnan
Eva Khn
Zhiming Liu
Gwen Salan
Marjan Sirjani

Technische Universität, Munich, Germany
University of York, UK
Nazarbayev University, Kazakhstan
FBK, Italy
IMT School for Advanced Studies Lucca, Italy
Lero, The Irish Software Engineering Research Centre, Ireland
Oracle Labs, Australia
TU Wien, Austria
Southwest University, China
Grenoble INP, Inria, LIG, France
Malardalen University, Sweden

Program Chairs

Einar Broch Johnsen
Ina Schaefer

University of Oslo, Norway
Technische Universität Braunschweig, Germany

Program Committee

Erika Abraham
Elvira Albert
Ade Azurat
Luis Barbosa
Dirk Beyer
Marcello Bonsangue
Jonathan Bowen
Mario Bravetti
Einar Broch Johnsen
Ana Cavalcanti
Alessandro Cimatti
Ferruccio Damiani
Frank De Boer
Rocco De Nicola
John Derrick
Anke Dittmar
George Eleftherakis
José Luiz Fiadeiro
Carlo A. Furia

RWTH Aachen University, Germany
Universidad Complutense de Madrid, Spain
Fasilkom UI, Indonesia
University of Minho, Portugal
LMU Munich, Germany
Leiden University, The Netherlands
London South Bank University, UK
University of Bologna, Italy
University of Oslo, Norway
University of York, UK
FBK-irst, Italy
Università di Torino, Italy
CWI, The Netherlands
School for Advanced Studies Lucca, Italy
University of Sheffield, UK
University of Rostock, Germany
The University of Sheffield, UK
Royal Holloway, University of London, UK
Chalmers University of Technology, Sweden
Philipp Haller  
KTH Royal Institute of Technology, Sweden

Klaus Havelund  
Jet Propulsion Laboratory, USA

Rob Hierons  
Brunel University, UK

Marieke Huisman  
University of Twente, The Netherlands

Paddy Krishnan  
Oracle, USA

Peter Gorm Larsen  
Aarhus University, Denmark

Kung-Kiu Lau  
The University of Manchester, UK

Martin Leucker  
University of Lübeck, Germany

Tiziana Margaria  
Lero, Ireland

Mercedes Merayo  
Universidad Complutense de Madrid, Spain

Shin Nakajima  
National Institute of Informatics, Japan

Viet Yen Nguyen  
Hypefactors, Denmark

Fernando Orejas  
Universitat Politècnica de Catalunya, Spain

Marc Pantel  
IRIT/INPT, Université de Toulouse, France

Anna Philippou  
University of Cyprus, Cyprus

Geguang Pu  
East China Normal University, China

Leila Ribeiro  
Universidade Federal do Rio Grande do Sul, Brazil

Philipp Ruemmer  
Uppsala University, Sweden

Bernhard Rumpe  
RWTH Aachen University, Germany

Gwen Salaün  
University of Grenoble Alpes, France

Augusto Sampaio  
Federal university of Pernambuco, Brazil

Cesar Sanchez  
IMDEA Software Institute

Ina Schaefer  
Technische Universität Braunschweig, Germany

Neeraj Singh  
INPT-ENSEEIHT/IRIT, University of Toulouse, France

Marjan Sirjani  
Malardalen University, Sweden; Reykjavik University, Iceland

Graeme Smith  
The University of Queensland, Australia

Bernhard Steffen  
Technische Universität Dortmund, Germany

Maurice H. Ter Beek  
ISTI-CNR, Pisa, Italy

Willem Visser  
Stellenbosch University, South Africa

Bruce Watson  
Stellenbosch University, South Africa

Heike Wehrheim  
University of Paderborn, Germany

Wang Yi  
Uppsala University, Sweden

Ingrid Chieh Yu  
University of Oslo, Norway

### Additional Reviewers

Abd Alrahman, Yehia  
Din, Crystal Chang

Arshad, Rehman  
Dokter, Kasper

Barbon, Gianluca  
Foster, Simon

Cardone, Felice  
Freitas, Fred

Convent, Lukas  
Galletta, Letterio

Correas Fernández, Jesús  
García, Miriam

Dangl, Matthias  
Giraudo, Mauro
Gordillo, Pablo
Gossen, Frederik
Inverso, Omar
Irfan, Ahmed
Isabel, Miguel
Jafari, Ali
Krishna, Ajay
Kulik, Tomas
Laarman, Alfons
Lamprecht, Anna-Lena
Lange, Felix Dino
Lemberger, Thomas
Lu, Yi
Macedo, Hugo Daniel
Markin, Grigory
Mauro, Jacopo
Micheli, Andrea
Mohaqeqi, Morteza
Nellen, Johanna
Netz, Lukas
Neves, Renato
Paolini, Luca
Pauck, Felix
Peng, Cong
Pérez, Jorge A.
Qian, Chen
Raco, Deni
Rüthing, Oliver
Sabouri, Hamideh
Sacerdoti Coen, Claudio
Santini, Francesco
Schupp, Stefan
Sharma, Arnab
Spagnolo, Giorgio O.
Stolz, Volker
Ta, Quang-Trung
Tapia Tarifa, Silvia Lizeth
Thoma, Daniel
Thomsen, Michael Kirkedal
Varga, Simon
von Wenckstern, Michael
Winter, Kirsten
Zhang, Ning
Contents

Invited Keynote

We Need a Testability Transformation Semantics .......................... 3

Mark Harman

Specification

From Software Specifications to Constraint Programming ............... 21

Stefan Hallerstedt, Miran Hasanagić, Sebastian Krings,
Peter Gorm Larsen, and Michael Leuschel

Automated Specification Extraction and Analysis with Spectractor ..... 37

Christoph Schulze, Rance Cleaveland, and Mikael Lindvall

Bridging the Gap Between Informal Requirements and Formal
Specifications Using Model Federation ...................................... 54

Fahad Rafique Golra, Fabien Dagnat, Jeanine Souquières, Imen Sayar,
and Sylvain Guerin

Concurrency

Program Verification for Exception Handling on Active Objects
Using Futures ................................................................. 73

Crystal Chang Din, Rudolf Schlatte, and Tzu-Chun Chen

Spread the Work: Multi-threaded Safety Analysis for Hybrid Systems . 89

Stefan Schupp and Erika Abrahám

FASTLANE Is Opaque – a Case Study in Mechanized Proofs of Opacity . 105

Gerhard Schellhorn, Monika Wedel, Oleg Travkin, Jürgen König,
and Heike Wehrheim

Program Analysis

Monte Carlo Tree Search for Finding Costly Paths in Programs .......... 123

Kasper Luckow, Corina S. Pășăreanu, and Willem Visser

A Cloud-Based Execution Framework for Program Analysis .......... 139

Daniel Balasubramanian, Dmitriy Kostyuchenko, Kasper Luckow,
Rody Kersten, and Gabor Karsai
Cross-Architecture Lifter Synthesis ................................. 155
  Rijnard van Tonder and Claire Le Goues

Model Checking and Runtime Verification

Counterexample Simplification for Liveness Property Violation ............ 173
  Gianluca Barbon, Vincent Leroy, and Gwen Salaïn

Online Enumeration of All Minimal Inductive Validity Cores ............... 189
  Jaroslav Bendík, Elaheh Ghassabani, Michael Whalen, and Ivana Černá

Prevent: A Predictive Run-Time Verification Framework Using
Statistical Learning .................................................................. 205
  Reza Babaee, Arie Gurfinkel, and Sebastian Fischmeister

Applications

Formal Verification of Platoon Control Strategies ............................ 223
  Adnan Rashid, Umair Siddique, and Osman Hasan

Exploring Properties of a Telecommunication Protocol with Message Delay
Using Interactive Theorem Prover ............................................. 239
  Catherine Dubois, Olga Grinchtein, Justin Pearson, and Mats Carlsson

Automated Validation of IoT Device Control Programs Through
Domain-Specific Model Generation ............................................ 254
  Yunja Choi

Shape Analysis and Reuse

Graph-Based Shape Analysis Beyond Context-Freeness ..................... 271
  Hannah Arndt, Christina Jansen, Christoph Matheja, and Thomas Noll

Facilitating Component Reusability in Embedded Systems with GPUs ...... 287
  Gabriel Campeanu

Author Index ........................................................................... 303