

*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/7408>

Klaus Havelund · Jan Peleska  
Bill Roscoe · Erik de Vink (Eds.)

# Formal Methods

22nd International Symposium, FM 2018

Held as Part of the Federated Logic Conference, FloC 2018

Oxford, UK, July 15–17, 2018

Proceedings

*Editors*

Klaus Havelund   
NASA Jet Propulsion Laboratory  
Pasadena, CA  
USA

Jan Peleska   
University of Bremen  
Bremen  
Germany

Bill Roscoe  
University of Oxford  
Oxford  
UK

Erik de Vink  
Eindhoven University of Technology  
Eindhoven  
The Netherlands

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-95581-0            ISBN 978-3-319-95582-7 (eBook)  
<https://doi.org/10.1007/978-3-319-95582-7>

Library of Congress Control Number: 2018947575

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer International Publishing AG, part of Springer Nature 2018  
Chapter “Formal Specification and Verification of Dynamic Parametrized Architectures” is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>). For further details see license information in the chapter.

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 the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

FM 2018 was held in Oxford as part of FloC during July 15–17, with additional workshops on July 14 and during 18–19. It was a great pleasure to return to one of the spiritual homes of Formal Methods. This was the 22nd of a series stretching back to 1987. We are delighted to present its proceedings, once again published by Springer. FM is a core event for the formal methods community and brings together researchers working on both more theoretical aspects and industrial practice. Once again we had an Industry Day, or I-Day.

In all, there were 110 submitted papers for the main conference of which 35 were accepted, an acceptance rate of 32%. Kim G. Larsen, Annabelle McIver, and Leonardo de Moura gave invited talks. For I-Day, nine presenters were invited to share insights about applications of formal methods in industry.

Seven workshops were associated with FM this year: F-IDE, Overture, QAPL, AVoCS, REFINE, TLA+, and VaVas.

We offer our sincere thanks to all who helped make the conference a success and assisted with the preparation of these proceedings. This includes the FM committee chaired by Ana Cavalcanti, the FloC Organizing Committee led by Moshe Vardi, Daniel Kroening, and Marta Kwiatkowska, as well as the staff and volunteers who supported this event. Naturally, we also thank the Program Committee members and others who put so much effort into ensuring the quality of the program, as well as all authors who submitted papers.

FLoC had many sponsors including Oxford University Computer Science Department, Springer, and Diffblue. We thank them all.

June 2018

Erik de Vink  
Jan Peleska  
Bill Roscoe  
Klaus Havelund

# Organization

## Program Chairs

Jan Peleska                      University of Bremen, Germany  
Bill Roscoe                      University of Oxford, UK

## Workshop Chairs

Maurice ter Beek              CNR/ISTI, Italy  
Helen Treharne                University of Surrey, UK

## Industry Day Chairs

Klaus Havelund                NASA Jet Propulsion Laboratory, USA  
Jan Peleska                      University of Bremen, Germany  
Ralf Pinger                        Siemens, Germany

## Doctoral Symposium Chairs

Eerke Boiten                    De Montfort University, UK  
Fatiha Zaïdi                      Université Paris-Sud XI, France

## Organizing Committee

Erik de Vink                      Eindhoven University of Technology, The Netherlands  
    (General Chair)  
Mahmoud Talebi (Website)    Eindhoven University of Technology, The Netherlands

## Program Committee

Bernhard K. Aichernig        TU Graz, Austria  
Joerg Brauer                      Verified Systems International GmbH, Germany  
Ana Cavalcanti                University of York, UK  
Frank De Boer                    CWI, The Netherlands  
John Fitzgerald                Newcastle University, UK  
Martin Fraenzle                Carl von Ossietzky Universität Oldenburg, Germany  
Vijay Ganesh                    University of Waterloo, Canada  
Diego Garbervetsky            University of Buenos Aires, Argentina  
Dimitra Giannakopoulou    NASA Ames Research Center, USA  
Thomas Gibson-Robinson    University of Oxford, UK  
Stefania Gnesi                    ISTI-CNR, Italy

Klaus Havelund	NASA Jet Propulsion Laboratory, USA
Anne E. Haxthausen	Technical University of Denmark, Denmark
Ian J. Hayes	The University of Queensland, Australia
Constance Heitmeyer	Naval Research Laboratory, USA
Jozef Hooman	TNO-ESI and Radboud University Nijmegen, The Netherlands
Laura Humphrey	Air Force Research Laboratory, USA
Fuyuki Ishikawa	National Institute of Informatics, Japan
Einar Broch Johnsen	University of Oslo, Norway
Cliff Jones	Newcastle University, UK
Joost-Pieter Katoen	RWTH Aachen University, Germany
Gerwin Klein	NICTA and The University of New South Wales, Australia
Laura Kovacs	Chalmers University of Technology, Sweden
Peter Gorm Larsen	Aarhus University, Denmark
Yves Ledru	Université Grenoble Alpes, France
Rustan Leino	Amazon Web Services, USA
Elizabeth Leonard	Naval Research Laboratory, USA
Martin Leucker	University of Lübeck, Germany
Michael Leuschel	University of Düsseldorf, Germany
Zhiming Liu	Southwest University, China
Tiziana Margaria	University of Limerick and Lero, Ireland
Mieke Massink	ISTI-CNR, Italy
Annabelle McIver	Macquarie University, Australia
Dominique Mery	Université de Lorraine, LORIA, France
Mohammad Reza Mousavi	University of Leicester, UK
Peter Müller	ETH Zurich, Switzerland
Colin O'Halloran	D-RisQ Software Systems, UK
Jose Oliveira	University of Minho, Portugal
Olaf Owe	University of Oslo, Norway
Sam Owre	SRI International, USA
Jan Peleska	TZI, University of Bremen, Germany
Alexandre Petrenko	CRIM, Canada
Anna Philippou	University of Cyprus, Cyprus
Ralf Pinger	Siemens, Germany
Elvinia Riccobene	University of Milan, Italy
Bill Roscoe	University of Oxford, UK
Grigore Rosu	University of Illinois at Urbana-Champaign, USA
Augusto Sampaio	Federal University of Pernambuco, Brazil
Gerardo Schneider	Chalmers University of Technology, Sweden
Natasha Sharygina	University of Lugano, Switzerland
Ana Sokolova	University of Salzburg, Austria
Jun Sun	Singapore University of Technology and Design, Singapore
Stefano Tonetta	FBK-irst, Italy
Farn Wang	National Taiwan University, Taiwan

Heike Wehrheim	University of Paderborn, Germany
Michael Whalen	University of Minnesota, USA
Jim Woodcock	University of York, UK
Hüsni Yenigün	Sabancı University, Turkey
Fatiha Zaidi	Université Paris-Sud, France
Gianluigi Zavattaro	University of Bologna, Italy

## Additional Reviewers

Abbyaneh, Alireza	Fantechi, Alessandro	Longuet, Delphine
Agogino, Adrian	Fava, Daniel	Lucanu, Dorel
Aldini, Alessandro	Ferrère, Thomas	Macedo, Hugo Daniel
Antignac, Thibaud	Foltzer, Adam	Macedo, Nuno
Antonino, Pedro	Foster, Simon	Madeira, Alexandre
Araujo, Hugo	Gazda, Maciej	Marescotti, Matteo
Arcaïni, Paolo	Ghasemi, Mahsa	Markin, Grigory
Archer, Myla	Ghassabani, Elaheh	Matheja, Christoph
Asadi, Sepideh	Gomez-Zamalloa, Miguel	Mathur, Umang
Astrauskas, Vytautas	Govind, Hari	Mauro, Jacopo
Avellaneda, Florent	Günther, Henning	Mazzanti, Franco
Basile, Davide	Hagemann, Willem	Meinicke, Larissa
Baxter, James	Henrio, Ludovic	Merz, Stephan
Berger, Philipp	Holzer, Andreas	Monahan, Rosemary
Blich, Martin	Hyvärinen, Antti	Mota, Alexandre
Bodeveix, Jean-Paul	Höfner, Peter	Neubauer, Felix
Boudjadar, Jalil	Jaafar, Fehmi	Nguena-Timo, Omer
Braghin, Chiara	Junges, Sebastian	Nguyen, Huu Nghia
Bugariu, Alexandra	Katis, Andreas	Noll, Thomas
Byun, Taejoon	Khakpour, Narges	Oortwijn, Wytse
Carvalho, Gustavo	Kharraz, Karam	Palmskog, Karl
Castaño, Rodrigo	Kiesl, Benjamin	Pardo, Raúl
Chen, Taolue	Kotelnikov, Evgenii	Pauck, Felix
Chen, Yu-Ting	Kouzapas, Dimitrios	Pedro, André
Chen, Zhenbang	Krings, Sebastian	Pena, Lucas
Chimento, Jesus Mauricio	Kulik, Tomas	Proenca, Jose
Ciancia, Vincenzo	König, Jürgen	Qu, Hongyang
Ciolek, Daniel	Laarman, Alfons	Robillard, Simon
Colvin, Robert	Latella, Diego	Scheffel, Torben
de Gouw, Stijn	Legunsen, Owolabi	Schmidt, Joshua
Dodds, Mike	Lester, Martin Mariusz	Schmitz, Malte
Ehlers, Rüdiger	Li, Guangyuan	Schneider, David
Eilers, Marco	Li, Ian	Schoepe, Daniel
Even-Mendoza, Karine	Liang, Jimmy	Scott, Joe
Fages, François	Liu, Si	Sewell, Thomas



Sharma, Arnab  
Singh, Neeraj  
Steffen, Martin  
Stewart, Danielle  
Stolz, Volker  
Stumpf, Johanna Beate  
Swaminathan, Mani  
Syeda, Hira  
Tabaei, Mitra  
Taha, Safouan

Ter Beek, Maurice H.  
Ter-Gabrielyan, Arshavir  
Thoma, Daniel  
Thorstensen, Evgenij  
Thule, Casper  
Toews, Manuel  
Tribastone, Mirco  
Tschaikowski, Max  
Tveito, Lars  
van Glabbeek, Rob

Voisin, Frederic  
Winter, Kirsten  
Yakovlev, Alex  
Ye, Kangfeng  
Yovine, Sergio  
Zeyda, Frank  
Zhao, Liang  
Zoppi, Edgardo  
Zulkoski, Ed

# Contents

## Invited Papers

Processing Text for Privacy: An Information Flow Perspective . . . . .	3
<i>Natasha Fernandes, Mark Dras, and Annabelle McIver</i>	
20 Years of <i>Real</i> Real Time Model Validation . . . . .	22
<i>Kim Guldstrand Larsen, Florian Lorber, and Brian Nielsen</i>	

## FM 2018 Main Conference

Deadlock Detection for Actor-Based Coroutines . . . . .	39
<i>Keyvan Azadbakht, Frank S. de Boer, and Erik de Vink</i>	
An Algebraic Approach for Reasoning About Information Flow . . . . .	55
<i>Arthur Américo, Mário S. Alvim, and Annabelle McIver</i>	
Towards ‘Verifying’ a Water Treatment System . . . . .	73
<i>Jingyi Wang, Jun Sun, Yifan Jia, Shengchao Qin, and Zhiwu Xu</i>	
FSM Inference from Long Traces . . . . .	93
<i>Florent Avellaneda and Alexandre Petrenko</i>	
A Weakness Measure for GR(1) Formulae . . . . .	110
<i>Davide Giacomo Cavezza, Dalal Alrajeh, and András György</i>	
Producing Explanations for Rich Logics. . . . .	129
<i>Simon Busard and Charles Pecheur</i>	
The Compound Interest in Relaxing Punctuality . . . . .	147
<i>Thomas Ferrère</i>	
IPL: An Integration Property Language for Multi-model Cyber-physical Systems . . . . .	165
<i>Ivan Ruchkin, Joshua Sunshine, Grant Iraci, Bradley Schmerl, and David Garlan</i>	
Timed Epistemic Knowledge Bases for Social Networks . . . . .	185
<i>Raúl Pardo, César Sánchez, and Gerardo Schneider</i>	
Optimal and Robust Controller Synthesis: Using Energy Timed Automata with Uncertainty . . . . .	203
<i>Giovanni Bacci, Patricia Bouyer, Uli Fahrenberg, Kim Guldstrand Larsen, Nicolas Markey, and Pierre-Alain Reynier</i>	

Encoding Fairness in a Synchronous Concurrent Program Algebra . . . . .	222
<i>Ian J. Hayes and Larissa A. Meinicke</i>	
A Wide-Spectrum Language for Verification of Programs on Weak Memory Models . . . . .	240
<i>Robert J. Colvin and Graeme Smith</i>	
Operational Semantics of a Weak Memory Model with Channel Synchronization . . . . .	258
<i>Daniel Schnetzer Fava, Martin Steffen, and Volker Stolz</i>	
Stepwise Development and Model Checking of a Distributed Interlocking System - Using RAISE . . . . .	277
<i>Signe Geisler and Anne E. Haxthausen</i>	
Resource-Aware Design for Reliable Autonomous Applications with Multiple Periods . . . . .	294
<i>Rongjie Yan, Di Zhu, Fan Zhang, Yiqi Lv, Junjie Yang, and Kai Huang</i>	
Verifying Auto-generated C Code from Simulink: An Experience Report in the Automotive Domain . . . . .	312
<i>Philipp Berger, Joost-Pieter Katoen, Erika Ábrahám, Md Tawhid Bin Waez, and Thomas Rambow</i>	
QFLan: A Tool for the Quantitative Analysis of Highly Reconfigurable Systems . . . . .	329
<i>Andrea Vandin, Maurice H. ter Beek, Axel Legay, and Alberto Lluch Lafuente</i>	
Modular Verification of Programs with Effects and Effect Handlers in Coq . . .	338
<i>Thomas Letan, Yann Régis-Gianas, Pierre Chifflier, and Guillaume Hiet</i>	
Combining Tools for Optimization and Analysis of Floating-Point Computations . . . . .	355
<i>Heiko Becker, Pavel Panchekha, Eva Darulova, and Zachary Tatlock</i>	
A Formally Verified Floating-Point Implementation of the Compact Position Reporting Algorithm . . . . .	364
<i>Laura Titolo, Mariano M. Moscato, César A. Muñoz, Aaron Dutle, and François Bobot</i>	
Formal Verification of Automotive Simulink Controller Models: Empirical Technical Challenges, Evaluation and Recommendations . . . . .	382
<i>Johanna Nellen, Thomas Rambow, Md Tawhid Bin Waez, Erika Ábrahám, and Joost-Pieter Katoen</i>	
Multi-robot LTL Planning Under Uncertainty . . . . .	399
<i>Claudio Menghi, Sergio Garcia, Patrizio Pelliccione, and Jana Tumova</i>	

Vector Barrier Certificates and Comparison Systems . . . . .	418
<i>Andrew Sogokon, Khalil Ghorbal, Yong Kiam Tan, and André Platzer</i>	
Timed Vacuity . . . . .	438
<i>Hana Chockler, Shibashis Guha, and Orna Kupferman</i>	
Falsification of Cyber-Physical Systems Using Deep Reinforcement Learning . . . . .	456
<i>Takumi Akazaki, Shuang Liu, Yoriyuki Yamagata, Yihai Duan, and Jianye Hao</i>	
Dynamic Symbolic Verification of MPI Programs . . . . .	466
<i>Dhriti Khanna, Subodh Sharma, César Rodríguez, and Rahul Purandare</i>	
To Compose, or Not to Compose, That Is the Question: An Analysis of Compositional State Space Generation . . . . .	485
<i>Sander de Putter and Anton Wijs</i>	
View Abstraction for Systems with Component Identities. . . . .	505
<i>Gavin Lowe</i>	
Compositional Reasoning for Shared-Variable Concurrent Programs . . . . .	523
<i>Fuyuan Zhang, Yongwang Zhao, David Sanán, Yang Liu, Alwen Tiu, Shang-Wei Lin, and Jun Sun</i>	
Statistical Model Checking of LLVM Code . . . . .	542
<i>Axel Legay, Dirk Nowotka, Danny Bøgsted Poulsen, and Louis-Marie Tranouez</i>	
SDN-Actors: Modeling and Verification of SDN Programs. . . . .	550
<i>Elvira Albert, Miguel Gómez-Zamalloa, Albert Rubio, Matteo Sammartino, and Alexandra Silva</i>	
CompoSAT: Specification-Guided Coverage for Model Finding . . . . .	568
<i>Sorawee Porncharoenwase, Tim Nelson, and Shriram Krishnamurthi</i>	
Approximate Partial Order Reduction . . . . .	588
<i>Chuchu Fan, Zhenqi Huang, and Sayan Mitra</i>	
A Lightweight Deadlock Analysis for Programs with Threads and Reentrant Locks . . . . .	608
<i>Cosimo Laneve</i>	
Formal Specification and Verification of Dynamic Parametrized Architectures . . . . .	625
<i>Alessandro Cimatti, Ivan Stojic, and Stefano Tonetta</i>	

**FM 2018 Industry Day**

From Formal Requirements to Highly Assured Software for Unmanned Aircraft Systems . . . . .	647
<i>César Muñoz, Anthony Narkawicz, and Aaron Dutle</i>	
Interlocking Design Automation Using Prover Trident . . . . .	653
<i>Arne Borälv</i>	
Model-Based Testing for Avionics Systems . . . . .	657
<i>Jörg Brauer and Uwe Schulze</i>	
On Software Safety, Security, and Abstract Interpretation . . . . .	662
<i>Daniel Kästner, Laurent Mauborgne, and Christian Ferdinand</i>	
Variant Analysis with QL . . . . .	666
<i>Pavel Avgustinov, Kevin Backhouse, and Man Yue Mo</i>	
Object-Oriented Security Proofs . . . . .	671
<i>Ernie Cohen</i>	
Z3 and SMT in Industrial R&D . . . . .	675
<i>Nikolaj Bjørner</i>	
Evidential and Continuous Integration of Software Verification Tools . . . . .	679
<i>Tewodros A. Beyene and Harald Ruess</i>	
Disruptive Innovations for the Development and the Deployment of Fault-Free Software . . . . .	686
<i>Thierry Lecomte</i>	
<b>Author Index</b> . . . . .	691