

## Founding Editors

Gerhard Goos

*Karlsruhe Institute of Technology, Karlsruhe, Germany*

Juris Hartmanis

*Cornell University, Ithaca, NY, USA*

## Editorial Board Members

Elisa Bertino

*Purdue University, West Lafayette, IN, USA*

Wen Gao

*Peking University, Beijing, China*

Bernhard Steffen 

*TU Dortmund University, Dortmund, Germany*

Gerhard Woeginger 

*RWTH Aachen, Aachen, Germany*

Moti Yung

*Columbia University, New York, NY, USA*

More information about this series at <http://www.springer.com/series/7408>


Emil Sekerinski · Nelma Moreira ·  
José N. Oliveira et al. (Eds.)


# Formal Methods


FM 2019 International Workshops

Porto, Portugal, October 7–11, 2019  
Revised Selected Papers, Part II

*Editors*

Emil Sekerinski   
McMaster University  
Hamilton, ON, Canada

Nelma Moreira   
University of Porto  
Porto, Portugal

José N. Oliveira   
University of Minho  
Braga, Portugal

Workshop Editors *see next page*

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-54996-1              ISBN 978-3-030-54997-8 (eBook)  
<https://doi.org/10.1007/978-3-030-54997-8>

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer Nature Switzerland AG 2020

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, expressed 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.

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

## Workshop Editors

### AFFORD

Daniel Ratiu  
Argo Ai  
Munich, Germany  
dratiu@argo.ai

### DataMOD

Riccardo Guidotti  
University of Pisa  
Pisa, Italy  
riccardo.guidotti@di.unipi.it

### FMAS

Marie Farrell  
University of Liverpool  
Liverpool, UK  
marie.farrell@liverpool.ac.uk

Matt Luckcuck  
University of Liverpool  
Liverpool, UK  
m.luckcuck@liverpool.ac.uk

### FMBC

Diego Marmsoler  
University of Exeter  
Exeter, UK  
d.marmsoler@exeter.ac.uk

### FMIS

José Campos  
University of Minho  
Braga, Portugal  
jose.campos@di.uminho.pt


### HFM

Troy Astarte  
University of Newcastle  
Newcastle upon Tyne, UK  
t.astarte@ncl.ac.uk

### NSAD

Laure Gonnord  
Claude Bernard University  
Lyon, France  
laure.gonnord@ens-lyon.fr

### OpenCert

Antonio Cerone   
Nazarbayev University  
Nur-Sultan, Kazakhstan  
antonio.cerone@nu.edu.kz

### Overture

Luis Diogo Couto  
Forcepoint  
Ireland  
ldcouto@gmail.com

### Refine

Brijesh Dongol  
University of Surrey  
Guildford, UK  
b.dongol@surrey.ac.uk

### RPLA

Martin Kutrib  
University of Giessen  
Giessen, Germany  
kutrib@informatik.uni-gies-  
sen.de

### SASB

Pedro Monteiro  
University of Lisbon  
Lisbon, Portugal  
pedro.tiago.monteiro@tec-  
nico.ulisboa.pt

### TAPAS

David Delmas  
Airbus Operations S.A.S.  
Toulouse, France  
david.delmas@lip6.fr

# Preface

The Third World Congress on Formal Methods (FM 2019) took place during October 7–11, 2019, in Porto, Portugal. The congress comprised nine conferences: the 23rd International Symposium on Formal Methods (FM 2019); the 29th International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR 2019); the 13th International Conference on Mathematics of Program Construction (MPC 2019); the 21st International Symposium on Principles and Practice of Declarative Programming (PPDP 2019); the 19th International Conference on Runtime Verification (RV 2019); the 26th International Static Analysis Symposium (SAS 2019); the 13th International Conference on Tests and Proofs (TAP 2019); the 7th International Symposium on Unifying Theories of Programming (UTP 2019); and the 13th International Conference on Verification and Evaluation of Computer and Communication Systems (VECoS 2019). The conference also included a Doctoral Symposium, an Industry Day, 2 festschrifts, 16 workshops, and 5 tutorials. In total there were 630 registered participants from 43 countries, 381 presentations from 821 authors, 44 invited speakers, and 13 tool exhibitors. The 16 workshops emerged out of 18 workshop proposals. Three workshops, the Second International Workshop on Dynamic Logic, New Trends and Applications (DaLi 2019), the Third International Workshop and Tutorial on Formal Methods Teaching (FMTea 2019), and the 5th Workshop on Formal Integrated Development Environment (F-IDE 2019), had their proceedings published separately. This two-volume book consists of the proceedings of the other 13 workshops.

## *Volume 1:*

### **AFFORD 2019**

The Third Workshop on Practical Formal Verification for Software Dependability

### **DataMod 2019**

The 8th International Symposium From Data to Models and Back

### **FMAS 2019**

The First Formal Methods for Autonomous Systems Workshop

### **FMBC 2019**

The First Workshop on Formal Methods for Blockchains

### **FMIS 2019**

The 8th International Workshop on Formal Methods for Interactive Systems

## *Volume 2:*

### **HFM 2019**

The First History of Formal Methods Workshop

### **NSAD 2019**

The 8th International Workshop on Numerical and Symbolic Abstract Domains

**OpenCERT 2019**

The 9th International Workshop on Open Community Approaches to Education, Research and Technology

**Overture 2019**

The 17th Overture Workshop

**Refine 2019**

The 19th Refinement Workshop

**RPLA 2019**

The First International Workshop on Reversibility in Programming, Languages, and Automata

**SASB 2019**

The 10th International Workshop on Static Analysis and Systems Biology

**TAPAS 2019**

The 10th Workshop on Tools for Automatic Program Analysis

The diversity of the workshop themes reflects the evolution that formal methods of software development have taken since the first World Congress on Formal Methods in 1999 (Toulouse, France) and the second in 2009 (Eindhoven, The Netherlands). Each workshop has its unique history and style that was left up to the workshop organizers to maintain. We are pleased to have four workshops for the first time: FMAS, FMBC, HFM, and RPLA. In total, 123 papers were accepted after a first round of reviewing for the presentation at FM 2019. Of those, 108 were submitted for a second round of reviewing after the congress and 68 selected for inclusion in these proceedings. The workshop organizers ensured that all papers received at least three reviews. Nine invited abstracts, two invited papers, and one workshop summary are included as well.

We are grateful to the workshop authors, the workshop organizers, the Program and Organizing Committee members of the workshops, the local organizers, the sponsors of the congress, and everyone else involved in the 34 events of the congress for the concerted effort in putting together such a rich program.

Finally, we thank Springer for their immediate willingness to publish the collected FM 2019 workshop proceedings in the LNCS series and their support in the editing process.

May 2020

Emil Sekerinski  
Nelma Moreira  
José N. Oliveira

# Organization

## General Chair

José N. Oliveira                      University of Minho, INESC TEC, Portugal

## Program Chairs

Maurice H. ter Beek                      ISTI-CNR, Italy  
Annabelle McIver                      Macquarie University, Australia

## Industry Day Chairs

Joe Kiniry                      Galois Inc., USA  
Thierry Lecomte                      ClearSy, France

## Doctoral Symposium Chairs

Alexandra Silva                      University College London, UK  
Antónia Lopes                      University of Lisbon, Portugal

## Journal First Track Chair

Augusto Sampaio                      Federal University of Pernambuco, Brazil

## Workshop and Tutorial Chairs

Emil Sekerinski                      McMaster University, Canada  
Nelma Moreira                      University of Porto, Portugal

## Organizing Committee

Luís Soares Barbosa                      University of Minho, INESC TEC, Portugal  
José Creissac Campos                      University of Minho, INESC TEC, Portugal  
João Pascoal Faria                      University of Porto, INESC TEC, Portugal  
Sara Fernandes                      University of Minho, INESC TEC, Portugal  
Luís Neves                      Critical Software, Portugal  
Ana Paiva                      University of Porto, INESC TEC, Portugal



## **Local Organizers**

Catarina Fernandes	University of Minho, INESC TEC, Portugal
Paula Rodrigues	INESC TEC, Portugal
Ana Rita Costa	INESC TEC, Portugal

## **Web Team**

Francisco Neves	University of Minho, INESC TEC, Portugal
Rogério Pontes	University of Minho, INESC TEC, Portugal
Paula Rodrigues	INESC TEC, Portugal

## **FME Board**

Ana Cavalcanti	University of York, UK
Lars-Henrik Eriksson	Uppsala University, Sweden
Stefania Gnesi	ISTI-CNR, Italy
Einar Broch Johnsen	University of Oslo, Norway
Nico Plat	Thanos, The Netherlands

## Contents – Part II

### **HFM 2019 - History of Formal Methods Workshop**

Flow Diagrams, Assertions, and Formal Methods . . . . .	15
<i>Mark Priestley</i>	
The School of Squiggol: A History of the Bird–Meertens Formalism. . . . .	35
<i>Jeremy Gibbons</i>	
Reasoning About Shared-Variable Concurrency: Interactions Between Research Threads . . . . .	54
<i>Cliff B. Jones</i>	
Specification with Class: A Brief History of Object-Z . . . . .	73
<i>Graeme Smith and David J. Duke</i>	
Formal Specifications and Software Testing, a Fruitful Convergence . . . . .	87
<i>Marie-Claude Gaudel</i>	
From Manuscripts to Programming Languages: An Archivist Perspective. . . .	95
<i>Alexandra Vidal, Ana Sandra Meneses, and António Sousa</i>	
What Have Formal Methods Ever Done for Us? An Audience Discussion . . .	103
<i>Troy Kaighin Astarte</i>	

### **NSAD 2019 - 8th Workshop on Numerical and Symbolic Abstract Domains**

Combination of Boxes and Polyhedra Abstractions for Constraint Solving . . .	119
<i>Ghiles Ziat, Alexandre Maréchal, Marie Pelleau, Antoine Miné, and Charlotte Truchet</i>	
An Abstract Domain for Objects in Dynamic Programming Languages . . . . .	136
<i>Vincenzo Arceri, Michele Pasqua, and Isabella Mastroeni</i>	

### **OpenCERT 2019 - 9th International Workshop on Open Community Approaches to Education, Research and Technology**

A Survey of Learning Methods in Open Source Software . . . . .	157
<i>Aidarbek Suleimenov, Assiya Khuzyakhmetova, and Antonio Cerone</i>	

A Calculus of Chaos in Stochastic Compilation: Engineering in the Cause of Mathematics . . . . .	167
<i>Peter T. Breuer and Simon J. Pickin</i>	
Runtime Verification of Linux Kernel Security Module . . . . .	185
<i>Denis Efremov and Ilya Shchepetkov</i>	
Open and Interactive Learning Resources for Algorithmic Problem Solving . . . . .	200
<i>João F. Ferreira and Alexandra Mendes</i>	
Challenges Faced by Students in an Open Source Software Undergraduate Course . . . . .	209
<i>Dias Issa</i>	
Open Source Software as a Learning Tool for Computer Science Students . . .	224
<i>Assiya Khuzyakhmetova and Aidarbek Suleimenov</i>	
<b>Overture 2019 - 17th Overture Workshop</b>	
Exploring Human Behaviour in Cyber-Physical Systems with Multi-modelling and Co-simulation . . . . .	237
<i>Ken Pierce, Carl Gamble, David Golightly, and Roberto Palacín</i>	
Migrating the INTO-CPS Application to the Cloud . . . . .	254
<i>Hugo Daniel Macedo, Mikkel Bayard Rasmussen, Casper Thule, and Peter Gorm Larsen</i>	
Towards a Static Check of FMUs in VDM-SL . . . . .	272
<i>Nick Battle, Casper Thule, Cláudio Gomes, Hugo Daniel Macedo, and Peter Gorm Larsen</i>	
ViennaDoc: An Animatable and Testable Specification Documentation Tool . . . . .	289
<i>Tomohiro Oda, Keijiro Araki, Yasuhiro Yamamoto, Kumiyo Nakakoji, Hiroshi Sako, Han-Myung Chang, and Peter Gorm Larsen</i>	
<b>Refine 2019 - 19th Refinement Workshop</b>	
A Map of Asynchronous Communication Models . . . . .	307
<i>Florent Chevrou, Aurélie Hurault, Shin Nakajima, and Philippe Quéinnec</i>	
An Abstract Semantics of Speculative Execution for Reasoning About Security Vulnerabilities . . . . .	323
<i>Robert J. Colvin and Kirsten Winter</i>	

Weakening Correctness and Linearizability for Concurrent Objects on Multicore Processors . . . . .	342
<i>Graeme Smith and Lindsay Groves</i>	
Towards a Method for the Decomposition by Refinement in Event-B . . . . .	358
<i>Kenza Kraibi, Rahma Ben Ayed, Joris Rehm, Simon Collart-Dutilleul, Philippe Bon, and Dorian Petit</i>	
Transformations for Generating Type Refinements . . . . .	371
<i>Douglas R. Smith and Stephen J. Westfold</i>	
Comparing Correctness-by-Construction with Post-Hoc Verification—A Qualitative User Study . . . . .	388
<i>Tobias Runge, Thomas Thüm, Loek Cleophas, Ina Schaefer, and Bruce W. Watson</i>	
<b>RPLA 2019 - Workshop on Reversibility in Programming, Languages, and Automata</b>	
Reversible Programs Have Reversible Semantics . . . . .	413
<i>Robert Glück, Robin Kaarsgaard, and Tetsuo Yokoyama</i>	
Two-Way Quantum and Classical Automata with Advice for Online Minimization Problems . . . . .	428
<i>Kamil Khadiev and Aliya Khadieva</i>	
Quotients and Atoms of Reversible Languages . . . . .	443
<i>Hellis Tamm</i>	
<b>SASB 2019 - 10th International Workshop on Static Analysis and Systems Biology</b>	
Bayesian Verification of Chemical Reaction Networks . . . . .	461
<i>Gareth W. Molyneux, Viraj B. Wijesuriya, and Alessandro Abate</i>	
Nested Event Representation for Automated Assembly of Cell Signaling Network Models . . . . .	480
<i>Evan W. Becker, Kara N. Bocan, and Natasa Miskov-Zivanov</i>	
<b>TAPAS 2019 - 10th Workshop on Tools for Automatic Program Analysis</b>	
PrideMM: Second Order Model Checking for Memory Consistency Models . . . . .	507
<i>Simon Cooksey, Sarah Harris, Mark Batty, Radu Grigore, and Mikoláš Janota</i>	

<b>FkCC: The Farkas Calculator</b> . . . . .	526
<i>Christophe Alias</i>	
<b>Handling Heap Data Structures in Backward Symbolic Execution</b> . . . . .	537
<i>Robert Husák, Jan Kofroň, and Filip Zavoral</i>	
<b>AUTHCHECK: Program-State Analysis for Access-Control Vulnerabilities</b> . . . . .	557
<i>Goran Piskachev, Tobias Petrasch, Johannes Späth, and Eric Bodden</i>	
<b>Author Index</b> . . . . .	573

# Contents – Part I

## **AFFORD 2019 - 3rd Workshop on Practical Formal Verification for Software Dependability**

Experiences with Streamlining Formal Methods Tools . . . . .	5
<i>Paolo Masci</i>	
The Bourgeois Gentleman, Engineering and Formal Methods . . . . .	12
<i>Thierry Lecomte</i>	
SEB-CG: Code Generation Tool with Algorithmic Refinement Support for Event-B . . . . .	19
<i>Mohammadsadegh Dalvandi, Michael Butler, and Asieh Salehi Fathabadi</i>	
Compiling C and C++ Programs for Dynamic White-Box Analysis. . . . .	30
<i>Zuzana Baranová and Petr Ročkal</i>	
Model Checking in a Development Workflow: A Study on a Concurrent C++ Hash Table . . . . .	46
<i>Petr Ročkal</i>	
Addressing Usability in a Formal Development Environment . . . . .	61
<i>Paolo Arcaini, Silvia Bonfanti, Angelo Gargantini, Elvinia Riccobene, and Patrizia Scandurra</i>	
Formal Modelling and Verification as Rigorous Review Technology: An Inspiration from INSPEX . . . . .	77
<i>Richard Banach, Joseph Razavi, Olivier Debicki, and Suzanne Lesecq</i>	

## **DataMod 2019 - 8th International Symposium From Data to Models and Back**

Validation of a Simulation Algorithm for Safety-Critical Human Multitasking . . . . .	99
<i>Giovanna Broccia, Paolo Milazzo, Cristina Belviso, and Carmen Berrocal Montiel</i>	
An Ontology-Based Approach to Support Formal Verification of Concurrent Systems. . . . .	114
<i>Natalia Garanina, Igor Anureev, Elena Sidorova, Dmitry Koznov, Vladimir Zyubin, and Sergei Gorlatch</i>	

How to Look Next? A Data-Driven Approach for Scanpath Prediction . . . . .	131
<i>Giuseppe Boccignone, Vittorio Cuculo, and Alessandro D’Amelio</i>	
“Know Thyself” How Personal Music Tastes Shape the Last.Fm Online Social Network. . . . .	146
<i>Riccardo Guidotti and Giulio Rossetti</i>	
Gender Recognition in the Wild with Small Sample Size - A Dictionary Learning Approach . . . . .	162
<i>Alessandro D’Amelio, Vittorio Cuculo, and Sathya Bursic</i>	
An Instrumented Mobile Language Learning Application for the Analysis of Usability and Learning. . . . .	170
<i>Aigerim Aibassova, Antonio Cerone, and Mukhtar Tashkenbayev</i>	
Analysis and Visualization of Performance Indicators in University Admission Tests . . . . .	186
<i>Michela Natilli, Daniele Fadda, Salvatore Rinzivillo, Dino Pedreschi, and Federica Licari</i>	
Anomaly Detection from Log Files Using Unsupervised Deep Learning . . . . .	200
<i>Sathya Bursic, Vittorio Cuculo, and Alessandro D’Amelio</i>	
<b>FMAS 2019 - 1st Formal Methods for Autonomous Systems Workshop</b>	
Formalisation and Implementation of Road Junction Rules on an Autonomous Vehicle Modelled as an Agent . . . . .	217
<i>Gleifer Vaz Alves, Louise Dennis, and Michael Fisher</i>	
CriSGen: Constraint-Based Generation of Critical Scenarios for Autonomous Vehicles. . . . .	233
<i>Andreas Nonnengart, Matthias Klusch, and Christian Müller</i>	
Verification of Fair Controllers for Urban Traffic Manoeuvres at Intersections . . . . .	249
<i>Christopher Bischopink and Maïke Schwammberger</i>	
Temporal Logic Semantics for Teleo-Reactive Robotic Agent Programs. . . . .	265
<i>Keith Clark, Brijesh Dongol, and Peter Robinson</i>	
A Mission Definition, Verification and Validation Architecture. . . . .	281
<i>Louis Viard, Laurent Ciarletta, and Pierre-Etienne Moreau</i>	
<b>FMBC 2019 - 1st Workshop on Formal Methods for Blockchains</b>	
Smart Contracts: Application Scenarios for Deductive Program Verification . . . . .	293
<i>Bernhard Beckert, Jonas Schiffel, and Mattias Ulbrich</i>	

Deductive Proof of Industrial Smart Contracts Using Why3 . . . . .	299
<i>Zeinab Nehai and François Bobot</i>	
Verifying Smart Contracts with Cubicle . . . . .	312
<i>Sylvain Conchon, Alexandrina Korneva, and Fatiha Zaidi</i>	
Call Me Back, I Have a Type Invariant . . . . .	325
<i>M. Anthony Aiello, Johannes Kanig, and Taro Kurita</i>	
Statistical Model Checking of RANDAO’s Resilience to Pre-computed Reveal Strategies. . . . .	337
<i>Musab A. Alturki and Grigore Roşu</i>	
A Distributed Blockchain Model of Selfish Mining . . . . .	350
<i>Dennis Eijkel and Ansgar Fehnker</i>	
Towards a Verified Model of the Algorand Consensus Protocol in Coq . . . . .	362
<i>Musab A. Alturki, Jing Chen, Victor Luchangco, Brandon Moore, Karl Palmiskog, Lucas Peña, and Grigore Roşu</i>	
Mi-Cho-Coq, a Framework for Certifying Tezos Smart Contracts . . . . .	368
<i>Bruno Bernardo, Raphaël Cauderlier, Zhenlei Hu, Basile Pesin, and Julien Tesson</i>	
Smart Contract Interactions in Coq . . . . .	380
<i>Jakob Botsch Nielsen and Bas Spitters</i>	
Formal Specification of a Security Framework for Smart Contracts . . . . .	392
<i>Mikhail Mandrykin, Jake O’Shannessy, Jacob Payne, and Ilya Shchepetkov</i>	
<b>FMIS 2019 - 8th Formal Methods for Interactive Systems Workshop</b>	
Examples of the Application of Formal Methods to Interactive Systems. . . . .	409
<i>Michael D. Harrison</i>	
Modelling Human Reasoning in Practical Behavioural Contexts Using Real-Time Maude . . . . .	424
<i>Antonio Cerone and Peter Csaba Ölveczky</i>	
A Survey of Papers from Formal Methods for Interactive Systems (FMIS) Workshops . . . . .	443
<i>Pascal Béger, Sebastien Leriche, and Daniel Prun</i>	
Formal Modelling of Safety-Critical Interactive Devices Using Coloured Petri Nets. . . . .	465
<i>Sapna Jaidka, Steve Reeves, and Judy Bowen</i>	



<b>Model-Based Testing of Post-WIMP Interactions Using Object Oriented Petri-Nets</b> . . . . .	486
<i>Alexandre Canny, David Navarre, José Creissac Campos, and Philippe Palanque</i>	
<b>Fortune Nets for Fortunettes: Formal, Petri Nets-Based, Engineering of Feedforward for GUI Widgets</b> . . . . .	503
<i>David Navarre, Philippe Palanque, Sven Coppers, Kris Luyten, and Davy Vanacken</i>	
<b>Author Index</b> . . . . .	521