Lecture Notes in Computer Science 12232

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
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-giessen.de

**SASB**
Pedro Monteiro
University of Lisbon
Lisbon, Portugal
pedro.tiago.monteiro@tecnico.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 Symposium on Static Analysis (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  
Paula Rodrigues  
Ana Rita Costa  

**Web Team**

Francisco Neves  
Rogério Pontes  
Paula Rodrigues  

**FME Board**

Ana Cavalcanti  
Lars-Henrik Eriksson  
Stefania Gnesi  
Einar Broch Johnsen  
Nico Plat  

University of Minho, INESC TEC, Portugal  
INESC TEC, Portugal  

University of Minho, INESC TEC, Portugal  
INESC TEC, Portugal  

University of York, UK  
Uppsala University, Sweden  
ISTI-CNR, Italy  
University of Oslo, Norway  
Thanos, The Netherlands
Contents – Part I

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

Experiences with Streamlining Formal Methods Tools ............................ 5
*Paolo Masci*

The Bourgeois Gentleman, Engineering and Formal Methods ................. 12
*Thierry Lecomte*

SEB-CG: Code Generation Tool with Algorithmic Refinement Support for Event-B .......................................................... 19
*Mohammadsadegh Dalvandi, Michael Butler,*
*and Asieh Salehi Fathabadi*

Compiling C and C++ Programs for Dynamic White-Box Analysis .......... 30
*Zuzana Baranová and Petr Ročkai*

Model Checking in a Development Workflow: A Study on a Concurrent C++ Hash Table ......................................................... 46
*Petr Ročkai*

Addressing Usability in a Formal Development Environment .............. 61
*Paolo Arcaini, Silvia Bonfanti, Angelo Gargantini, Elvinia Riccobene,*
*and Patrizia Scandurra*

Formal Modelling and Verification as Rigorous Review Technology:
An Inspiration from INSPEX ...................................................... 77
*Richard Banach, Joseph Razavi, Olivier Debicki,* and *Suzanne Lesecq*

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

Validation of a Simulation Algorithm for Safety-Critical Human Multitasking ................................................................. 99
*Giovanna Broccia, Paolo Milazzo, Cristina Belviso,*
*and Carmen Berrocal Montiel*

An Ontology-Based Approach to Support Formal Verification of Concurrent Systems .................................................. 114
*Natalia Garanina, Igor Anureev, Elena Sidorova, Dmitry Koznov,*
*Vladimir Zyubin,* and *Sergei Gorlatch*
How to Look Next? A Data-Driven Approach for Scanpath Prediction

Giuseppe Boccignone, Vittorio Cuculo, and Alessandro D’Amelio

“Know Thyself” How Personal Music Tastes Shape the Last.Fm Online Social Network

Riccardo Guidotti and Giulio Rossetti

Gender Recognition in the Wild with Small Sample Size - A Dictionary Learning Approach

Alessandro D’Amelio, Vittorio Cuculo, and Sathya Bursic

An Instrumented Mobile Language Learning Application for the Analysis of Usability and Learning

Aigerim Aibassova, Antonio Cerone, and Mukhtar Tashkenbayev

Analysis and Visualization of Performance Indicators in University Admission Tests

Michela Natilli, Daniele Fadda, Salvatore Rinzivillo, Dino Pedreschi, and Federica Licari

Anomaly Detection from Log Files Using Unsupervised Deep Learning

Sathya Bursic, Vittorio Cuculo, and Alessandro D’Amelio

FMAS 2019 - 1st Formal Methods for Autonomous Systems Workshop

Formalisation and Implementation of Road Junction Rules on an Autonomous Vehicle Modelled as an Agent

Gleifer Vaz Alves, Louise Dennis, and Michael Fisher

CriSGen: Constraint-Based Generation of Critical Scenarios for Autonomous Vehicles

Andreas Nonnengart, Matthias Klusch, and Christian Müller

Verification of Fair Controllers for Urban Traffic Manoeuvres at Intersections

Christopher Bischopink and Maike Schwammberger

Temporal Logic Semantics for Teleo-Reactive Robotic Agent Programs

Keith Clark, Brijesh Dongol, and Peter Robinson

A Mission Definition, Verification and Validation Architecture

Louis Viard, Laurent Ciarletta, and Pierre-Etienne Moreau

FMBC 2019 - 1st Workshop on Formal Methods for Blockchains

Smart Contracts: Application Scenarios for Deductive Program Verification

Bernhard Beckert, Jonas Schiffl, and Mattias Ulbrich
Deductive Proof of Industrial Smart Contracts Using Why3 ................................. 299
Zeinab Nehaï and François Bobot

Verifying Smart Contracts with Cubicle ............................................................ 312
Sylvain Conchon, Alexandrina Korneva, and Fattha Zaïdi

Call Me Back, I Have a Type Invariant ............................................................. 325
M. Anthony Aiello, Johannes Kanig, and Taro Kurita

Statistical Model Checking of RANDAO’s Resilience to Pre-computed Reveal Strategies .......................................................... 337
Musab A. Alturki and Grigore Roșu

A Distributed Blockchain Model of Selfish Mining ............................................. 350
Dennis Eijkel and Ansgar Fehnker

Towards a Verified Model of the Algorand Consensus Protocol in Coq .......... 362
Musab A. Alturki, Jing Chen, Victor Luchangco, Brandon Moore, Karl Palmskog, Lucas Peña, and Grigore Roșu

Mi-Cho-Coq, a Framework for Certifying Tezos Smart Contracts .................... 368
Bruno Bernardo, Raphaël Cauderlier, Zhenlei Hu, Basile Pesin, and Julien Tesson

Smart Contract Interactions in Coq ................................................................. 380
Jakob Botsch Nielsen and Bas Spitters

Mikhail Mandrykin, Jake O’Shannessy, Jacob Payne, and Ilya Shchepetkov

FMIS 2019 - 8th Formal Methods for Interactive Systems Workshop

Examples of the Application of Formal Methods to Interactive Systems ........... 409
Michael D. Harrison

Modelling Human Reasoning in Practical Behavioural Contexts Using Real-Time Maude .......................................................... 424
Antonio Cerone and Peter Csaba Ölveczky

A Survey of Papers from Formal Methods for Interactive Systems (FMIS) Workshops ........................................................ 443
Pascal Béger, Sebastien Leriche, and Daniel Prun

Sapna Jaidka, Steve Reeves, and Judy Bowen
Model-Based Testing of Post-WIMP Interactions Using Object Oriented Petri-Nets .......................................................... 486
  Alexandre Canny, David Navarre, José Creissac Campos,
  and Philippe Palanque

Fortune Nets for Fortunettes: Formal, Petri Nets-Based, Engineering of Feedforward for GUI Widgets ................................. 503
  David Navarre, Philippe Palanque, Sven Coppers, Kris Luyten,
  and Davy Vanacken

Author Index .................................................................................. 521
## Contents – Part II

### HFM 2019 - History of Formal Methods Workshop

Flow Diagrams, Assertions, and Formal Methods ........................................ 15
*Mark Priestley*

The School of Squiggol: A History of the Bird–Meertens Formalism .......... 35
*Jeremy Gibbons*

Reasoning About Shared-Variable Concurrency: Interactions Between
Research Threads ......................................................................................... 54
*Cliff B. Jones*

Specification with Class: A Brief History of Object-Z .............................. 73
*Graeme Smith and David J. Duke*

Formal Specifications and Software Testing, a Fruitful Convergence ........... 87
*Marie-Claude Gaudel*

From Manuscripts to Programming Languages: An Archivist Perspective .... 95
*Alexandra Vidal, Ana Sandra Meneses, and António Sousa*

What Have Formal Methods Ever Done for Us? An Audience Discussion .... 103
*Troy Kaighin Astarte*

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

Combination of Boxes and Polyhedra Abstractions for Constraint Solving ...... 119
*Ghiles Ziat, Alexandre Maréchal, Marie Pelleau, Antoine Miné, and Charlotte Truchet*

An Abstract Domain for Objects in Dynamic Programming Languages ....... 136
*Vincenzo Arceri, Michele Pasqua, and Isabella Mastroeni*

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

A Survey of Learning Methods in Open Source Software ......................... 157
*Aidarbek Suleimenov, Assiya Khuzyakhmetova, and Antonio Cerone*
A Calculus of Chaos in Stochastic Compilation: Engineering in the Cause of Mathematics ............................................................ 167

Peter T. Breuer and Simon J. Pickin

Runtime Verification of Linux Kernel Security Module .................... 185

Denis Efremov and Ilya Shchepetkov

Open and Interactive Learning Resources for Algorithmic Problem Solving ................................................................. 200

João F. Ferreira and Alexandra Mendes

Challenges Faced by Students in an Open Source Software Undergraduate Course ............................................................. 209

Dias Issa

Open Source Software as a Learning Tool for Computer Science Students ................................................................. 224

Assiya Khuzyakhmetova and Aidarbek Suleimenov

Overture 2019 - 17th Overture Workshop

Exploring Human Behaviour in Cyber-Physical Systems with Multi-modelling and Co-simulation ............................................ 237

Ken Pierce, Carl Gamble, David Golightly, and Roberto Palacin

Migrating the INTO-CPS Application to the Cloud .......................... 254

Hugo Daniel Macedo, Mikkel Bayard Rasmussen, Casper Thule, and Peter Gorm Larsen

Towards a Static Check of FMUs in VDM-SL ................................ 272

Nick Battle, Casper Thule, Cláudio Gomes, Hugo Daniel Macedo, and Peter Gorm Larsen

ViennaDoc: An Animatable and Testable Specification Documentation Tool ................................................................. 289

Tomohiro Oda, Keijiro Araki, Yasuhiro Yamamoto, Kumiyo Nakakoji, Hiroshi Sako, Han-Myung Chang, and Peter Gorm Larsen

Refine 2019 - 19th Refinement Workshop

A Map of Asynchronous Communication Models .......................... 307

Florent Chevrou, Aurélie Hurault, Shin Nakajima, and Philippe Quéinnec

An Abstract Semantics of Speculative Execution for Reasoning About Security Vulnerabilities .............................................. 323

Robert J. Colvin and Kirsten Winter
Weakening Correctness and Linearizability for Concurrent Objects on Multicore Processors

Graeme Smith and Lindsay Groves

Towards a Method for the Decomposition by Refinement in Event-B

Kenza Kraibi, Rahma Ben Ayed, Joris Rehm, Simon Collart-Dutilleul, Philippe Bon, and Dorian Petit

Transformations for Generating Type Refinements

Douglas R. Smith and Stephen J. Westfold

Comparing Correctness-by-Construction with Post-Hoc Verification—A Qualitative User Study

Tobias Runge, Thomas Thüm, Loek Cleophas, Ina Schaefer, and Bruce W. Watson

RPLA 2019 - Workshop on Reversibility in Programming, Languages, and Automata

Reversible Programs Have Reversible Semantics

Robert Glück, Robin Kaarsgaard, and Tetsuo Yokoyama

Two-Way Quantum and Classical Automata with Advice for Online Minimization Problems

Kamil Khadiev and Aliya Khadieva

Quotients and Atoms of Reversible Languages

Hellis Tamm

SASB 2019 - 10th International Workshop on Static Analysis and Systems Biology

Bayesian Verification of Chemical Reaction Networks

Gareth W. Molyneux, Viraj B. Wijesuriya, and Alessandro Abate

Nested Event Representation for Automated Assembly of Cell Signaling Network Models

Evan W. Becker, Kara N. Bocan, and Natasa Miskov-Zivanov

TAPAS 2019 - 10th Workshop on Tools for Automatic Program Analysis

PrideMM: Second Order Model Checking for Memory Consistency Models

Simon Cooksey, Sarah Harris, Mark Batty, Radu Grigore, and Mikoláš Janota
Fkcc: The Farkas Calculator .................................................. 526
Christophe Alias

Handling Heap Data Structures in Backward Symbolic Execution ........ 537
Robert Husák, Jan Kofroň, and Filip Zavoral

AUTHCHECK: Program-State Analysis for Access-Control Vulnerabilities .... 557
Goran Piskachev, Tobias Petrasch, Johannes Spáth, and Eric Bodden

Author Index ................................................................. 573