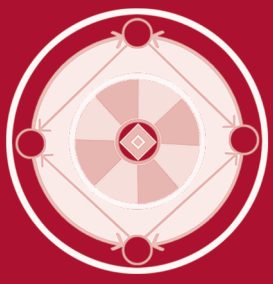
Maurice H. ter Beek
Leopoldo Teixeira (Eds.)

Formal Methods: Foundations and Applications

LNCS 16363

28th Brazilian Symposium, SBMF 2025
Recife, Brazil, December 3–5, 2025
Proceedings



SBMF 2025
28th Brazilian Symposium on
Formal Methods

Springer

Lecture Notes in Computer Science **16363**

The series Lecture Notes in Computer Science (LNCS), including its subseries Lecture Notes in Artificial Intelligence (LNAI) and Lecture Notes in Bioinformatics (LNBI), has established itself as a medium for the publication of new developments in computer science and information technology research, teaching, and education.

LNCS enjoys close cooperation with the computer science R & D community, the series counts many renowned academics among its volume editors and paper authors, and collaborates with prestigious societies. Its mission is to serve this international community by providing an invaluable service, mainly focused on the publication of conference and workshop proceedings and postproceedings. LNCS commenced publication in 1973.

Maurice H. ter Beek · Leopoldo Teixeira
Editors

Formal Methods: Foundations and Applications

28th Brazilian Symposium, SBMF 2025
Recife, Brazil, December 3–5, 2025
Proceedings

Springer

Editors
Maurice H. ter Beek
CNR-ISTI
Pisa, Italy

Leopoldo Teixeira
Federal University of Pernambuco
Recife, Pernambuco, Brazil

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-032-12085-4 ISBN 978-3-032-12086-1 (eBook)
https://doi.org/10.1007/978-3-032-12086-1

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

Preface

This volume contains the papers presented at the 28th Brazilian Symposium on Formal Methods (SBMF 2025), held in Recife, Brazil, from December 3–5, 2025. The SBMF conference series is devoted to the development, dissemination, and use of formal methods for the construction of high-quality computational systems.

The main topics discussed at SBMF include the following. Formal aspects of specification languages and theoretical foundations, such as the development of new domain-specific languages, the formalization of existing languages, and the study of the foundations of software engineering. Formal aspects of systems development, such as the application of formal methods to the development of cyber-physical systems, embedded systems, and software-intensive systems. Verification and validation, such as the formal verification of the correctness of software systems, the model checking of the requirements of software systems, and the fuzz testing of software systems. Formal verification of neural networks, such as the application of formal methods to the verification of the correctness of deep learning models. Self-formalization and formal aspects in practice, such as the automation of formal methods, the use of formal methods in industrial settings, and the teaching of formal methods.

SBMF 2025 solicited high-quality papers with a strong emphasis on formal methods, whether practical or theoretical, in the form of regular or short papers. The Program Committee (PC), with members from 14 different countries spread over 5 continents, originally received a total of 25 submissions from 8 different countries spread over 4 continents: 24 regular papers and 1 short paper. Of these, 24 papers went through a rigorous single-blind review process according to which all papers were reviewed by three PC members, with the help of a few external reviewers. The decision to accept or reject a submission was based not only on the review reports and scores, but also and in particular on the in-depth and sometimes intense discussions. In the end, the PC of SBMF 2025 decided to accept 1 short and 12 regular papers, resulting in an acceptance rate of 54%.

The conference also featured three inspiring keynotes by our invited speakers:

- *Formal Reasoning for Assuring Product Lines of Complex Systems* by Marsha Chechik (University of Toronto, Canada)
- *Safe Evolution of Smart Contracts Supported by LLMs and Bounded Model Checking* by Augusto Sampaio (Federal University of Pernambuco, Brazil)
- *Exploring Modelling Language Engineering* by Hans Vangheluwe (University of Antwerp, Belgium)

We are very grateful for the contributions of our invited speakers.

Thanks are due to all involved in SBMF 2025. Specifically, all PC members and external reviewers for their accurate and timely reviewing, all authors for their submissions, and all attendees for their participation. We also thank in particular the conference General Chair, Lucas Lima from the Federal Rural University of Pernambuco (UFRPE,

Brazil), as well as the Web and Social Media Chair and of course the Steering Committee, all itemised on the following pages.

We are very grateful for the support of the Brazilian Computer Society (SBC), promoting this event, with local support from UFRPE, Centre for Strategic Technologies of the Northeast (CETENE), and the Informatics Center at Federal University of Pernambuco (CIn-UFPE). We also acknowledge our sponsors: AWS, Cadence, CAPES, CNPq, FACEPE, and Formal Methods Europe (FME).

Finally, we would like to thank Springer for publishing these proceedings and we gratefully acknowledge the support from EasyChair in assisting us in managing the entire process from submissions through these proceedings to the programme.

We hope you enjoyed the conference!

December 2025

Leopoldo Teixeira
Maurice H. ter Beek

Organization

General Chair

Lucas Lima	Federal Rural University of Pernambuco, Brazil

PC Chairs

Leopoldo Teixeira	Federal University of Pernambuco, Brazil
Maurice H. ter Beek	CNR–ISTI, Pisa, Italy

Web and Social Media Chair

Diego Ferreira	Federal Rural University of Pernambuco, Brazil

Steering Committee

Vince Molnár	Budapest University of Technology and Economics, Hungary
Lucas Lima	Federal Rural University of Pernambuco, Brazil
Yoni Zohar	Bar-Ilan University, Israel
Haniel Barbosa	Federal University of Minas Gerais, Brazil
Ciprian Teodorov	ENSTA Bretagne, France
Sidney C. Nogueira	Federal Rural University of Pernambuco, Brazil

Program Committee

Jefferson O. Andrade	Federal Institute of Espírito Santo, Brazil
Luís Soares Barbosa	University of Minho and INESC TEC, Portugal, and UNU-EGOV, Brazil
Haniel Barbosa	Federal University of Minas Gerais, Brazil
Davide Basile	CNR–ISTI, Pisa, Italy
Armin Biere	University of Freiburg, Germany
Laura Bussi	University of Amsterdam, The Netherlands
Sérgio Campos	Federal University of Minas Gerais, Brazil

Gustavo Carvalho	Federal University of Pernambuco, Brazil
Valentina Castiglioni	Eindhoven University of Technology, The Netherlands
Márcio Cornélio	Federal University of Pernambuco, Brazil
Katalin Fazekas	TU Wien, Austria
Mathias Fleury	University of Freiburg, Germany
Rohit Gheyi	Federal University of Campina Grande, Brazil
Ahmed Irfan	SRI International, USA
Juliano Iyoda	Federal Rural University of Pernambuco, Brazil
Thierry Lecomte	CLEARSY, France
Michael Leuschel	University of Düsseldorf, Germany
Lucas Lima	Federal Rural University of Pernambuco, Brazil
Alberto Lluch Lafuente	Technical University of Denmark, Denmark
Alvaro Miyazawa	University of York, UK
Vince Molnár	Budapest University of Technology and Economics, Hungary
Alexandre Mota	Federal University of Pernambuco, Brazil
Sidney Nogueira	Federal Rural University of Pernambuco, Brazil
Marcel Oliveira	Federal University of Rio Grande do Norte, Brazil
José Proença	CISTER and University of Porto, Portugal
Pedro Ribeiro	University of York, UK
Philipp Rümmer	University of Regensburg, Germany, and Uppsala University, Sweden
Augusto Sampaio	Federal University of Pernambuco, Brazil
Hans-Jörg Schurr	University of Iowa, USA
Volker Stolz	Western Norway University of Applied Sciences, Norway
Ciprian Teodorov	ENSTA Bretagne, France
Nils Timm	University of Pretoria, South Africa
Jim Woodcock	University of York, UK
Yoni Zohar	Bar-Ilan University, Israel

Additional Reviewers

Bertalan Zoltán Péter	Budapest University of Technology and Economics, Hungary
Caio Ribeiro	Federal University of Minas Gerais, Brazil
Kangfeng Ye	University of York, UK

Invited Talks

Formal Reasoning for Assuring Product Lines of Complex Systems

Marsha Chechik

University of Toronto, Canada
chechik@cs.toronto.edu

Abstract. Assuring the reliability of complex systems is a difficult and expensive undertaking. These costs are further exacerbated when a family of similar products with varying features need to be assured, or when products evolve due to changing requirements or to introduce new functionalities. In this talk I will discuss methods for assuring reliability of such systems, from their representation as product lines to their efficient analysis to methods for building and maintaining assurance cases for such systems using templates. The focus would be on formal techniques underlying these methods.

Keywords: Assurance cases · reliability · product lines · theorem-proving · consistency

Acknowledgments. The author would like to thank her group members and collaborators: Logan Murphy, Torin Viger, Aren Babikian, Alessio Di Sandro, Claudio Menghi, Jeff Joyce, Simon Diemert, Ramesh S., Sahar Kokaly. This research was funded by NSERC, General Motors and Critical Systems Lab.

Safe Evolution of Smart Contracts Supported by LLMs and Bounded Model Checking

Augusto Sampaio

Universidade Federal de Pernambuco, Brazil
acas@cin.ufpe.br

Abstract. The talk presents a trusted deployer framework for safely deploying and upgrading smart contracts within the design-by-contract (DbC) paradigm. The inputs are (i) a reference interface specification, which defines invariants and pre- and postconditions for each function, and (ii) an implementation to be verified. The framework ensures that any deployed implementation must conform to the given specification. Both specification and implementation evolution are supported. Specifications might evolve by changing data representations or extending the interface with new functions, provided that the evolved specification is a (data) refinement of the current reference one. A new implementation must conform to the current reference specification. A distinguishing feature of the overall approach is the automation of the verification process in a hidden formal methods style. Since developers tend to be reluctant to provide formal specifications for software components, we are investigating state-of-the-art natural language processing technologies—particularly Large Language Models (LLMs) from the GPT family—to automatically infer formal (DbC) interface specifications from textual requirements. Furthermore, when a specification upgrade involves a change in data representation, we use a strategy built with the Alloy Analyzer to automatically infer the relation between the two data representations. The applicability of the framework is evaluated in the context of Solidity smart contracts implementing Ethereum standards.

Keywords: Solidity smart contracts · Ethereum standards · Formal verification · GPTAlloy

Acknowledgments. This project is being developed by a consortium including the Universidade Federal de Pernambuco (Brazil), the University College Oxford Blockchain Research Centre (UK), and the Blockhouse Technology Limited (UK). This is a collaboration with Pedro Antonino, Filipe Arruda, Juliandson Ferreira, Gabriel Leite and Bill Roscoe.

Exploring Modelling Language Engineering

Hans Vangheluwe

University of Antwerp, Belgium
hans.vangheluwe@uantwerpen.be

Abstract. Models described in a plethora of modelling languages are ubiquitous. They allow us to encode knowledge for various purposes at an appropriate level of abstraction, using appropriate notations. A floor-plan model for example allows an architect to specify the structure of a building so that a contractor can use it as a specification for building. A differential equation model, based on laws of physics allows an engineer to describe the behaviour of a physical system, either to explain observed system behaviour, or as a means to find, through simulation-based experimentation, an optimal design of the system. Programming languages are also modelling languages, which allow programmers to specify, at a computing-platform independent level, what a computer should do. Such programs are commonly either interpreted or compiled (or just-in-time compiled, as a hybrid). In addition to general-purposes modelling languages, so-called domain-specific languages (DSLs) have limited expressiveness, restricting their use to a specific application domain. This often makes them easier to learn by non-programmers and more amenable to the application of advanced analysis techniques such as model checking. Recently, Low Code, closely related to DSLs, have gained in popularity. Designing these modelling languages, with their associated modelling editors, simulators, debuggers, code-generators, … is hard. That is why modelling language engineering requires rigorous techniques. After some definitions of modelling language engineering concepts, the question arises what the most appropriate modelling formalisms are to precisely model/specify all aspects a modelling language. Models of modelling languages should encompass all aspects: concrete syntax, abstract syntax, semantics, the interaction behaviour of a model editor, of a simulator, and a debugger. Furthermore, from the onset, evolution of all these aspects should be taken into consideration.

An overview will be given of some techniques to model modelling languages, with a focus on graph-based approaches. This leads to some interesting insights into the co-design of requirements-, design-, trace- and property-languages. Furthermore, if the semantics of a modelling language is expressed in the form of graph transformation rules, this specification is not only easy to understand, even to non-computer scientists, but it is also amenable to certain kinds of analysis.

Contents