Lucas Lima
Vince Molnár (Eds.)

LNCS 13768

Formal Methods: Foundations and Applications

25th Brazilian Symposium, SBMF 2022
Virtual Event, December 6–9, 2022
Proceedings

Springer

Lecture Notes in Computer Science 13768

More information about this series at https://link.springer.com/bookseries/558

Lucas Lima · Vince Molnár (Eds.)

Formal Methods: Foundations and Applications

25th Brazilian Symposium, SBMF 2022
Virtual Event, December 6–9, 2022
Proceedings

Springer

Editors

Lucas Lima
Federal Rural University of Pernambuco
Recife, Brazil

Vince Molnár
Budapest University of Technology
and Economics
Budapest, Hungary

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-22475-1 ISBN 978-3-031-22476-8 (eBook)
https://doi.org/10.1007/978-3-031-22476-8

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 SBMF 2022: the 25th Brazilian Symposium on Formal Methods. Similarly to the previous two editions, the Steering Committee had to make the hard decision to organize a virtual-only event, as the COVID-19 situation in Brazil was still concerning at the beginning of the year. Therefore, the conference was held online, from December 6 to December 9, 2022.

The Brazilian Symposium on Formal Methods (SBMF) is an event devoted to the development, dissemination, and use of formal methods for the construction of high-quality computational systems, aiming to promote opportunities for researchers and practitioners with an interest in formal methods to discuss the recent advances in this area. SBMF is a consolidated scientific-technical event in the software area. Its first edition took place in 1998, reaching the jubilee 25th edition in 2022. The proceedings of the previous editions have been published mostly in Springer's Lecture Notes in Computer Science series as volumes 5902 (2009), 6527 (2010), 7021 (2011), 7498 (2012), 8195 (2013), 8941 (2014), 9526 (2015), 10090 (2016), 10623 (2017), 11254 (2018), 12475 (2020), and 13130 (2021).

This year's conference included four invited talks, given by Dirk Beyer (Ludwig-Maximilians-Universität München, Germany), Robert Karban (NASA's Jet Propulsion Laboratory, USA), Kristin Yvonne Rozier (Iowa State University, USA), and Valdivino Santiago (Instituto Nacional de Pesquisas Espaciais, Brazil). A total of eight papers were presented at the conference and are included in this volume. They were selected from 14 submissions that came from authors in seven different countries: Brazil, Canada, Estonia, Germany, Ireland, the UK, and the USA. The Program Committee comprised 40 members from the national and international community of formal methods. Each submission was reviewed by three Program Committee members (single blind review). Submissions, reviews, deliberations, and decisions were handled via EasyChair, which provided good support throughout this process.

We are grateful to the Program Committee for their hard work in evaluating submissions and suggesting improvements. We are very thankful to the general chair of SBMF 2022, Giovanny Fernando Lucero Palma (Universidade Federal de Sergipe, Brazil), who made everything possible for the conference to run smoothly. SBMF 2022 was organized by the Universidade Federal de Sergipe (UFS), and promoted by the Brazilian Computer Society (SBC). We would further like to thank SBC for their sponsorship, and Springer for agreeing to publish the proceedings as a volume of Lecture Notes in Computer Science.

December 2022

Lucas Lima
Vince Molnár

Organization

General Chair

Giovanny Lucero	Universidade Federal de Sergipe, Brazil

Program Committee Chairs

Lucas Lima	Universidade Federal Rural de Pernambuco, Brazil
Vince Molnár	Budapest University of Technology and Economics, Hungary

Steering Committee

Adolfo Duran	Universidade Federal da Bahia, Brazil
Phillip Wadler	University of Edinburgh, UK
Gustavo Carvalho	Universidade Federal de Pernambuco, Brazil
Volker Stolz	Western Norway University of Applied Sciences, Norway
Sérgio Campos	Universidade Federal de Minas Gerais, Brazil
Marius Minea	University of Massachusetts Amherst, USA

Program Committee

Aline Andrade	Universidade Federal da Bahia, Brazil
Haniel Barbosa	Universidade Federal de Minas Gerais, Brazil
Luis Barbosa	Universidade do Minho, Portugal
Armin Biere	Albert-Ludwigs-Universität Freiburg, Germany
Manfred Broy	Technische Universität München, Germany
Sérgio Campos	Universidade Federal de Minas Gerais, Brazil
Gustavo Carvalho	Universidade Federal de Pernambuco, Brazil
Márcio Cornélio	Universidade Federal de Pernambuco, Brazil
David Déharbe	CLEARSY Systems Engineering, France
Clare Dixon	University of Liverpool, UK
Jose Fiadeiro	University of Dundee, UK
Rohit Gheyi	Universidade Federal de Campina Grande, Brazil
Juliano Iyoda	Universidade Federal de Pernambuco, Brazil
Alfons Laarman	Leiden University, The Netherlands
Thierry Lecomte	CLEARSY Systems Engineering, France

Michael Leuschel	Universität Düsseldorf, Germany
Lucas Lima	Universidade Federal Rural de Pernambuco, Brazil
Patrícia Machado	Universidade Federal de Campina Grande, Brazil
Tiago Massoni	Universidade Federal de Campina Grande, Brazil
Ana Melo	Universidade de São Paulo, Brazil
Marius Minea	University of Massachusetts Amherst, USA
Alvaro Miyazawa	University of York, UK
Vince Molnár	Budapest University of Technology and Economics, Hungary
Sidney Nogueira	Universidade Federal Rural de Pernambuco, Brazil
Marcel Oliveira	Universidade Federal do Rio Grande do Norte, Brazil
Peter Csaba Ölveczky	University of Oslo, Norway
Leila Ribeiro	Universidade Federal do Rio Grande do Sul, Brazil
Elvinia Riccobene	University of Milan, Italy
Kristin Yvonne Rozier	Iowa State University, USA
Augusto Sampaio	Universidade Federal de Pernambuco, Brazil
Adenilso Simão	Universidade de São Paulo, Brazil
Volker Stolz	Western Norway University of Applied Sciences, Norway
Sofiène Tahar	Concordia University, Canada
Leopoldo Teixeira	Universidade Federal de Pernambuco, Brazil
Máté Tejfel	Eötvös Loránd University, Hungary
Maurice ter Beek	Istituto di Scienza e Tecnologie dell'Informazione, Italy
Nils Timm	University of Pretoria, South Africa
András Vörös	Budapest University of Technology and Economics, Hungary
Tim Willemse	Eindhoven University of Technology, The Netherlands
Jim Woodcock	University of York, UK

Invited Talks

Cooperative Verification

Dirk Beyer

Ludwig-Maximilians-Universität München, Germany

Abstract. Cooperative verification is an approach where several verifiers help each other solving the verification problem by sharing artifacts about the verification task. There are many verification tools available, but the power of combining them is not yet fully leveraged. The problem is that in order to use verifiers ‘off-the-shelf’, we need clear interfaces to invoke the tools and to pass information. Part of the interfacing problem is to define standard artifacts to be passed between verifiers. We explain a few recent approaches for cooperative combinations and also give a brief overview of CoVeriTeam, a tool for composing verification systems from existing off-the-shelf components.

Taming Monsters with Dragons: A Fractal Approach to Digital Twin Pipelines

Robert Karban

Jet Propulsion Laboratory - NASA, USA

Abstract. This presentation will discuss how development pipelines evolve over the systems lifecycle to integrate systems and its embedded software, resulting in a digital twin to enable system qualification and auditable artifacts. We will also touch on how the Europa Clipper project leverages such pipelines.

Developing an Open-Source, State-of-the-Art Symbolic Model-Checking Framework for the Model-Checking Research Community

Kristin Yvonne Rozier

Iowa State University, USA

Abstract. Safety-critical and security-critical systems are entering our lives at an increasingly rapid pace. These are the systems that help fly our planes, drive our cars, deliver our packages, ensure our electricity, or even automate our homes. Especially when humans cannot perform a task in person, e.g., due to a dangerous working environment, we depend on such systems. Before any safety-critical system launches into the human environment, we need to be sure it is really safe. Model checking is a popular and appealing way to rigorously check for safety: given a system, or an accurate model of the system, and a safety requirement, model checking is a "push button" technique to produce either a proof that the system always operates safely, or a counterexample detailing a system execution that violates the safety requirement. Many aspects of model checking are active research areas, including more efficient ways of reasoning about the system's behavior space, and faster search algorithms for the proofs and counterexamples.

As model checking becomes more integrated into the standard design and verification process for safety-critical systems, the platforms for model checking research have become more limited. Previous options have become closed-source or industry tools; current research platforms don't have support for expressive specification languages needed for verifying real systems. Our goal is to fill the current gap in model checking research platforms: building a freely-available, open-source, scalable model checking infrastructure that accepts expressive models and efficiently interfaces with the currently-maintained state-of-the-art back-end algorithms to provide an extensible research and verification tool. We are creating a community resource with a well-documented intermediate representation to enable extensibility, and a web portal, facilitating new modeling languages and back-end algorithmic advances. To add new modeling languages or algorithms, researchers need only to develop a translator to/from the new intermediate language, and will then be able to integrate each advance with the full state-of-the-art in model checking.

This community infrastructure will be ideal for catapulting formal verification efforts in many cutting-edge application areas, including security, networking, and operating system verification. We particularly target outreach to the embedded systems (CPS) community as our new framework will make hardware verification problems from this community more accessible.

Some Applications of Formal Methods

Valdivino Santiago

Instituto Nacional de Pesquisas Espaciais - INPE, Brazil

Abstract. This talk will present some applications of formal methods for aerospace and geoinformatics systems. Firstly, it will be discussed the feasibility, in the context of space systems such as satellites, of probabilistic model checking to the mitigation problem of single event upsets (SEUs) in field-programmable gate arrays (FPGAs). Secondly, it will be presented a method for automated unit test case/data generation based on functional model checking and focusing on C++ source code. The method was applied to two geoinformatics software products. Finally, the topic will be the assessment of the safety of navigation systems for a civil commercial transport category aircraft via probabilistic model checking. Considering these applications, strengths and weaknesses of such formal methods will also be addressed during the talk.

Contents

Model Checking and Semantics

Generation and Synthesis

Verification and Solvers