

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, Lancaster, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Zurich, Switzerland*

John C. Mitchell

*Stanford University, Stanford, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Dortmund, Germany*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbrücken, Germany*


More information about this series at <http://www.springer.com/series/7407>

Alessandro Abate · Sylvie Boldo (Eds.)

# Numerical Software Verification

10th International Workshop, NSV 2017  
Heidelberg, Germany, July 22–23, 2017  
Proceedings

*Editors*

Alessandro Abate   
University of Oxford  
Oxford  
UK

Sylvie Boldo  
Université Paris-Sud, Inria  
Orsay  
France

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-63500-2              ISBN 978-3-319-63501-9 (eBook)  
DOI 10.1007/978-3-319-63501-9

Library of Congress Control Number: 2017932122

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© Springer International Publishing AG 2017

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

# Preface

The 10th International Workshop on Numerical Software Verification (NSV 2017) was held during July 22–23, 2017, in Heidelberg, Germany.

This year NSV 2017 took place alongside the International Workshop on Formal Methods for Rigorous Systems Engineering of Cyber-Physical Systems (RISE4CPS, a one-time, invite-only event, chaired by Ezio Bartocci of TU Vienna). NSV 2017 was co-located within CAV 2017, the 29th International Conference on Computer-Aided Verification.

The scope of NSV 2017 has broadened since the earlier editions, but its core retains known fundamental aspects. Numerical computations are ubiquitous in digital systems: Monitoring, supervision, prediction, simulation, and signal processing rely heavily on numerical calculus to achieve desired goals. Design and verification of numerical algorithms has a unique set of challenges, which set it apart from the rest of software verification. To achieve the verification and validation of global system properties, numerical techniques need to precisely represent the local behaviors of each component. The implementation of numerical techniques on modern hardware adds another layer of approximation because of the use of finite representations of infinite precision numbers that usually lack basic arithmetic properties, such as associativity. Finally, the development and analysis of cyber-physical systems (CPS), which involve interacting continuous and discrete components, pose a further challenge. It is hence imperative to develop logical and mathematical techniques for reasoning about programmability and reliability. The NSV workshop is dedicated to the development of such techniques.

NSV 2017 was a two-day event, featuring two invited talks, single-track regular podium sessions, and additionally four invited speakers providing tutorials within RISE4CPS.

In all, 18 Program Committee members helped to provide at least four reviews of the submitted contributions, which were presented during the single-track sessions and appear as full papers in these proceedings.

A highlight of NSV 2017 was the presence of two high-profile invited speakers: Kyoko Makino, Professor in the Department of Physics and Astronomy at Michigan State University (USA), gave a seminar titled “Verified Computations using Taylor Models and the Applications.” Nathalie Revol, researcher at Inria (Lyon, France), gave a talk titled “Introduction to the IEEE 1788-2015 Standard for Interval Arithmetic.”

Further details on NSV 2017 are featured on the website: <http://www.cs.ox.ac.uk/conferences/NSV17/>

Finally, a few words of acknowledgment are due. Thanks to Springer for publishing the NSV proceedings in its *Lecture Notes in Computer Science* series. Thanks to Sergiy Bogomolov and Pavithra Prabhakar from the Steering Committee for support, to Yassamine Seladji for the help with publicity, to Viraj Wijesuriya for the organization

of the workshop website, to all the Program Committee members and additional reviewers for their work in ensuring the quality of the contributions to NSV 2017, and to all the participants for contributing to this event.

June 2017

Alessandro Abate  
Sylvie Boldo

# Organization

## Program Committee Chairs

Alessandro Abate	University of Oxford, UK
Sylvie Boldo	Inria, France

## Program Committee

Stanley Bak	Air Force Research Lab - Information Directorate, USA
Sergiy Bogomolov	IST Austria
Olivier Bouissou	The Mathworks, USA
Martin Brain	University of Oxford, UK
Alexandre Chapoutot	ENSTA ParisTech, France
Pieter Collins	Maastricht University, The Netherlands
Lucas Cordeiro	University of Oxford, UK
Eva Darulova	Max Planck Institute for Software Systems, Germany
Georgios Fainekos	Arizona State University, USA
François Févotte	EDF, France
Susmit Jha	SRI International, USA
James Kapinski	Toyota, USA
Guillaume Melquiond	Inria, France
Ian Mitchell	University of British Columbia, Canada
Sylvie Putot	LIX, Ecole Polytechnique, France
Sriram Sankaranarayanan	University of Colorado, USA
Walid Taha	Halmstad University, Sweden/Rice University, USA
Alexander Wittig	ESA ESTEC, Netherlands

## Steering Committee

Sergiy Bogomolov	Australian National University, Australia
Radu Grosu	TU Vienna, Austria
Matthieu Martel	Université de Perpignan, France
Pavithra Prabhakar	Kansas State University, USA
Sriram Sankaranarayanan	University of Colorado, USA

## Additional Reviewer

Franck Vedrine

## **Keynote Abstracts**



# Verified Computations Using Taylor Models and Their Applications

Kyoko Makino and Martin Berz

Michigan State University, East Lansing, MI 48824, USA  
{Makino,berz}@msu.edu  
<http://bt.pa.msu.edu>

**Abstract.** Numerical methods assuring confidence involve the treatment of entire sets instead of mere point evaluations. We briefly review the method of interval arithmetic that is long known for rigorous, verified computations, and all operations are conducted on intervals instead of numbers. However, interval computations suffer from overestimation, the dependency problem, the dimensionality curse, and the wrapping effect, to name a few, and those difficulties often make conventional interval based verified computational methods useless for practical challenging problems.

The method of Taylor models combines Taylor polynomials and remainder error enclosures, and operations are now conducted on Taylor models, where the bulk amount of the functional dependency is carried in the polynomial part, and the error enclosures provides a safety net to rigorously guarantee the result. Using simple and yet challenging benchmark problems, we demonstrate how the method works to bring those conventional difficulties under control. In the process, we also illustrate some ideas that lead to several Taylor model based algorithms and applications.

# Introduction to the IEEE 1788–2015 Standard for Interval Arithmetic

Nathalie Revol 

Inria – LIP, ENS de Lyon, University of Lyon  
46 allée d'Italie, 69364 Lyon Cedex 07, France

`Nathalie.Revol@inria.fr`

**Abstract.** Interval arithmetic is a tool of choice for numerical software verification, as every result computed using this arithmetic is self-verified: every result is an interval that is guaranteed to contain the exact numerical values, regardless of uncertainty or roundoff errors.

From 2008 to 2015, interval arithmetic underwent a standardization effort, resulting in the IEEE 1788–2015 standard. The main features of this standard are developed: the structure into levels, from the mathematic model to the implementation on computers; the possibility to accommodate different mathematical models, called flavors; the decoration system that keeps track of relevant events during the course of a calculation; the exact dot product for point (as opposed to interval) vectors.

## **Keynote Abstracts for RISE4CPS**

# CounterExample Guided Synthesis of Sound Controllers for Cyber-Physical Systems with SAT Solvers

Alessandro Abate

Department of Computer Science, University of Oxford, Oxford, UK  
aabate@cs.ox.ac.uk

We consider a classical model setup for Cyber-Physical Systems, comprising a physical plant represented as a linear, time-invariant model, which is closed loop with a digitally-implemented controller. As a key CPS feature, the plant model is given as a dynamical equation with inputs, evolving over a continuous state space, whereas the control signals are discrete in time and value.

The goal is to design a controller with a linear architecture ensuring that the closed-loop plant is safe, and at the same time accounting for errors due to the signals digitalisation, the manipulation of quantities represented with finite word length, and finally possible imprecisions in the description of the plant model.

We present a sound and automated approach based on counterexample guided inductive synthesis (CEGIS). The CEGIS architecture encompasses two phases: a synthesis step and a verification phase. We first synthesise a feedback controller that stabilises the plant but that may not be safe; safety is thereafter verified either via BMC or abstract acceleration. If the verification step fails, a counterexample is provided to the synthesis engine and the process iterates.

We demonstrate the practical value of this new CEGIS-based approach by automatically synthesising digital controllers for numerous models of physical plants extracted from the control literature. The details of this work appear in [2], which generalises work in [1]: the latter characterises models by transfer functions and exclusively considers stabilisation objectives.

## References

1. Abate, A., Bessa, I., Cattaruzza, D., Cordeiro, L., David, C., Kesseli, P., Kroening, D.: Sound and automated synthesis of digital stabilizing controllers for continuous plants. In: HSCC 2017, pp. 197–206 (2017)
2. Abate, A., Bessa, I., Cattaruzza, D., Cordeiro, L., David, C., Kesseli, P., Polgreen, E., Kroening, D.: Automated formal synthesis of digital controllers for state-space physical plants. In: CAV 2017 (2017, to Appear)

# Techniques and Tools for Hybrid Systems

## Reachability Analysis

Erika Ábrahám

RWTH Aachen University, Aachen, Germany

*Hybrid systems* are systems with combined discrete and continuous behaviour, typical examples being physical systems controlled by discrete controllers. Such systems can be found in various fields such as aviation, control engineering, medicine, or the wide field of cyber-physical systems.

The increasing relevance of hybrid systems, especially systems which interact with humans, requires careful design and proper *safety verification* techniques. Whereas the verification of purely continuous or purely discrete systems are already well-established research areas, the combination of discrete and continuous behaviours brings additional challenges for formal methods.

Logical formalisations are used in theorem-proving-based tools like KEYMAERA [12], ARIADNE [4], or the ISABELLE/HOL-based tool described in [10]. Other tools like dREACH [11], iSAT-ODE [6] and HSOLVER [13] also use logical characterisations but in combination with interval arithmetic and SMT solving. The tool C2E2 [5] uses validated numerical simulation; Bernstein expansion is implemented in [15]. This variety is complemented by approximation methods like hybridization, linearisation and abstraction techniques to increase the applicability of hybrid systems verification.

In this tutorial we focus on *flowpipe-construction-based* techniques and their implementation. As the reachability problem for hybrid systems is in general undecidable, flowpipe-construction-based reachability analysis techniques usually compute *over-approximations* of the set of reachable states of hybrid systems: starting from some initial sets, their time trajectories (*flowpipes*) and successors along discrete transitions (*jump successors*) are over-approximated in an iterative manner. Some tools in this area are CORA [1], FLOW\* [3], HYCREATE [9], HYSON [2], SOAPBOX [8], and SPACEEX [7].

The development of such tools is effortful, as datatypes for the underlying state set representations need to be implemented first. Our free and open-source C++ library HYPRO [14] provides implementations for the most prominent state set representations, with the aim to offer assistance for the rapid implementation of new algorithms by encapsulating all representation-related issues and allowing the developers to focus on higher-level algorithmic aspects.

In this tutorial we give an introduction to hybrid systems, and to flowpipe-construction-based algorithms for computing their reachable state sets. After discussing theoretical aspects, we shortly describe available tools and introduce in more

detail our HyPro library, explain its functionalities, and give some examples to demonstrate its usage.

## References

1. Althoff, M., Dolan, J.M.: Online verification of automated road vehicles using reachability analysis. *IEEE Trans. Robot.* **30**(4), 903–918 (2014)
2. Bouissou, O., Chapoutot, A., Mimram, S.: Computing flowpipe of nonlinear hybrid systems with numerical methods. CoRR abs/1306.2305 (2013). <http://arxiv.org/abs/1306.2305>
3. Chen, X., Ábrahám, E., Sankaranarayanan, S.: Flow\*: An analyzer for non-linear hybrid systems. In: Sharygina, N., Veith, H. (eds.) CAV 2013. LNCS, vol. 8044, pp. 258–263. Springer, Berlin (2013)
4. Collins, P., Bresolin, D., Geretti, L., Villa, T.: Computing the evolution of hybrid systems using rigorous function calculus. In: ADHS 2012, pp. 284–290. IFAC-PapersOnLine (2012)
5. Duggirala, P., Mitra, S., Viswanathan, M., Potok, M.: C2E2: A verification tool for Stateflow models. In: Baier, C., Tinelli, C. (eds.) TACAS 2015. LNCS, vol. 9035, pp. 68–82. Springer, Berlin (2015)
6. Eggers, A.: Direct handling of ordinary differential equations in constraint-solving-based analysis of hybrid systems. Ph.D. thesis, Universität Oldenburg, Germany (2014)
7. Frehse, G., et al.: SpaceEx: scalable verification of hybrid systems. In: Gopalakrishnan, G., Qadeer, S. (eds.) CAV 2011. LNCS, vol. 6806, pp. 379–395. Springer, Berlin (2011)
8. Hagemann, W., Möhlmann, E., Rakow, A.: Verifying a PI controller using SoapBox and Stabhyli: Experiences on establishing properties for a steering controller. In: ARCH 2014. EPIc Series in Computer Science, vol. 34. EasyChair (2014)
9. HyCreate: A tool for overapproximating reachability of hybrid automata. <http://stanleybak.com/projects/hycreate/hycreate.html>
10. Immmler, F.: Tool presentation: Isabelle/hol for reachability analysis of continuous systems. In: ARCH14-15. EPIc Series in Computer Science, vol. 34, pp. 180–187. EasyChair (2015)
11. Kong, S., Gao, S., Chen, W., Clarke, E.M.: dReach:  $\delta$ -reachability analysis for hybrid systems. In: Baier, C., Tinelli, C. (eds.) TACAS 2015. LNCS, vol. 9035, pp. 200–205. Springer, Berlin (2015)
12. Platzer, A., Quesel, J.: KeYmaera: A hybrid theorem prover for hybrid systems (system description). In: Armando, A., Baumgartner, P., Dowek, G. (eds.) IJCAR 2008. LNCS, vol. 5195, pp. 171–178. Springer, Berlin (2008)
13. Ratschan, S., She, Z.: Safety verification of hybrid systems by constraint propagation based abstraction refinement. In: Morari, M., Thiele, L. (eds.) HSCC 2005. LNCS, vol. 3414, pp. 573–589. Springer, Berlin (2005)
14. Schupp, S., Ábrahám, E., Ben Makhlof, I., Kowalewski, S.: HyPro: A C++ library for state set representations for hybrid systems reachability analysis. In: Barrett, C., Davies, M., Kahsai, T. (eds.) NFM 2017. LNCS, vol. 10227, pp. 288–294. Springer, Cham (2017)
15. Testylier, R., Dang, T.: NLTOOLBOX: a library for reachability computation of nonlinear dynamical systems. In: Van Hung, D., Ogawa, M. (eds.) ATVA 2013. LNCS, vol. 8172, pp. 469–473. Springer, Cham (2013)

# ProbReach: Probabilistic Bounded Reachability for Uncertain Hybrid Systems

Fedor Shmarov and Paolo Zuliani

School of Computing Science, Newcastle University, Newcastle upon Tyne, UK  
{f.shmarov,paolo.zuliani}@ncl.ac.uk

**Abstract.** We give an overview of our recent work on verified probabilistic reachability for hybrid systems with uncertain parameters [1–3]. Essentially, the problem reduces to computing validated enclosures for reachability probabilities. We present two approaches: one has high computational cost and provides absolute guarantees on the correctness of the answers, *i.e.*, the computed enclosures are formally guaranteed to contain the reachability probabilities. The other approach combines rigorous and statistical reasoning, thereby yielding better scalability by trading absolute guarantees with statistical guarantees. We exemplify both approaches with case studies from systems biology and cyber-physical systems.

The tutorial is divided into three parts:

1. introduction to delta-satisfiability and delta-complete decision procedures;
2. probabilistic bounded delta-reachability;
3. ProbReach tool demo.

No previous knowledge of systems biology or cyber-physical systems is necessary.

## References

1. Shmarov, F., Zuliani P.: ProbReach: verified probabilistic  $\delta$ -reachability for stochastic hybrid systems. In: HSCC, pp. 134–139. ACM (2015)
2. Shmarov, F., Zuliani, P.: Probabilistic hybrid systems verification via SMT and Monte Carlo techniques. In: Bloem, R., Arbel, E. (eds.) HVC 2016. LNCS, vol. 10028, pp. 152–168. Springer, Cham (2016)
3. Shmarov, F., Zuliani, P.: SMT-based reasoning for uncertain hybrid domains. In: AAAI-16 Workshop on Planning for Hybrid Systems, 30th AAAI Conference on Artificial Intelligence, pp. 624–630 (2016)

# Data-Driven Verification of Cyber-Physical Systems with DryVR and C2E2

Sayan Mitra

Department of Electrical and Computer Engineering, Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA  
mitras@illinois.edu

**Abstract.** Data-driven verification algorithms combine static analysis of models of control systems with dynamic information generated from executions or simulations. For cyber-physical systems and complex control systems, promising new algorithms and tools have been developed over the past five years following this approach. These methods have been used in verifying challenging benchmark problems correctness of air-traffic control protocols, meta-stability of mixed signal circuits, temporal properties of engine control systems, and safety related problems arising in autonomous vehicles and advanced driving assist systems. In this tutorial, I will give an overview of two verification tools that embody recent developments in data-driven verification, namely C2E2 and DryVR. Both use simulation or execution data; while C2E2 relies on static analysis of detailed dynamic models and give deterministic guarantees, DryVR only uses black-box simulators and gives probabilistic guarantees. Thus, the latter can check systems with partially known models. We will discuss some of the recent case studies and open problems in the area.



# Contents

## Keynote Abstracts

Verified Computations Using Taylor Models and Their Applications . . . . .	3
<i>Kyoko Makino and Martin Berz</i>	
Introduction to the IEEE 1788-2015 Standard for Interval Arithmetic . . . . .	14
<i>Nathalie Revol</i>	

## Precise Numerics

Formal Correctness of Comparison Algorithms Between Binary64 and Decimal64 Floating-Point Numbers . . . . .	25
<i>Arthur Blot, Jean-Michel Muller, and Laurent Théry</i>	
Sound Numerical Computations in Abstract Acceleration . . . . .	38
<i>Dario Cattaruzza, Alessandro Abate, Peter Schrammel, and Daniel Kroening</i>	
Studying the Numerical Quality of an Industrial Computing Code: A Case Study on Code_aster . . . . .	61
<i>François Févotte and Bruno Lathuilière</i>	

## Analysis and Verification of Continuous and Hybrid Models

Challenges and Tool Implementation of Hybrid Rapidly-Exploring Random Trees . . . . .	83
<i>Stanley Bak, Sergiy Bogomolov, Thomas A. Henzinger, and Aviral Kumar</i>	
Rigorous Reachability Analysis and Domain Decomposition of Taylor Models . . . . .	90
<i>Martin Berz and Kyoko Makino</i>	
A Study of Model-Order Reduction Techniques for Verification . . . . .	98
<i>Yi Chou, Xin Chen, and Sriram Sankaranarayanan</i>	

Author Index . . . . .	115
------------------------	-----