

Robustness in Cyber-Physical Systems

Edited by

Martin Fränzle¹, James Kapinski², and Pavithra Prabhakar³

1 Universität Oldenburg, DE, martin.fraenzle@informatik.uni-oldenburg.de

2 Toyota Technical Center – Gardena, US, jim.kapinski@toyota.com

3 Kansas State University – Manhattan, US, pprabhakar@ksu.edu

Abstract

Electronically controlled systems have become pervasive in modern society and are increasingly being used to control safety-critical applications, such as medical devices and transportation systems. At the same time, these systems are increasing in complexity at an alarming rate, making it difficult to produce system designs with guaranteed robust performance. Cyber-physical systems (CPS) is a new multi-disciplinary field aimed at providing a rigorous framework for designing and analyzing these systems, and recent developments in CPS-related fields provide techniques to increase robustness in the design and analysis of complex systems. This seminar brought together researchers from both academia and industry working in hybrid control systems, mechatronics, formal methods, and real-time embedded systems. Participants identified and discussed newly available techniques related to robust design and analysis that could be applied to open issues in the area of CPS and identified open issues and research questions that require collaboration between the communities. This report documents the program and the outcomes of Dagstuhl Seminar 16362 “Robustness in Cyber-Physical Systems”.

Seminar September 4–9, 2016 – <http://www.dagstuhl.de/16362>

1998 ACM Subject Classification C.4 Performance of Systems, C.1.m [Miscellaneous] Hybrid Systems, C.3 Special-Purpose and Application-Based Systems, D.2.4 Software/Program Verification, G.4 Mathematical Software, J.7 Computers in Other Systems

Keywords and phrases aerospace, automotive, cyber-physical systems, fault tolerance, formal verification, real-time and embedded systems, robustness

Digital Object Identifier 10.4230/DagRep.6.9.29

1 Executive Summary

Martin Fränzle

James Kapinski

Pavithra Prabhakar

License © Creative Commons BY 3.0 Unported license
© Martin Fränzle, James Kapinski, and Pavithra Prabhakar

Overview and Goals of the Seminar

Engineering robustness into systems under development has always been at the heart of good engineering practice, be it robustness against manufacturing tolerances and against variations in purity of construction materials in mechanical engineering, robustness against concentrations of educts in chemical engineering, against parameter variations in the plant model within control engineering, against quantization and measurement noise in signal processing, against faults in computer architecture, against attacks in security engineering, or against unexpected inputs or results in programming. In cyber-physical systems (CPS),



Except where otherwise noted, content of this report is licensed under a Creative Commons BY 3.0 Unported license

Robustness in Cyber-Physical Systems, *Dagstuhl Reports*, Vol. 6, Issue 9, pp. 29–45

Editors: Martin Fränzle, James Kapinski, and Pavithra Prabhakar



Dagstuhl Reports

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

all the aforementioned engineering disciplines meet, as the digital networking and embedded control involved in CPS brings many kinds of physical processes into the sphere of human and computer control. This convergence of disciplines has proven extremely fruitful in the past, inspiring profound research on hybrid and distributed control, transferring notions and methods for safety verification from computer science to control theory, transferring proof methods for stability from control theory to computer science, and shedding light on the complex interplay of control objectives and security threats, to name just a few of the many interdisciplinary breakthroughs achieved over the past two decades. Unfortunately, a joint, interdisciplinary approach to robustness remains evasive. While most researchers in the field of CPS concede that unifying notions across the disciplinary borders to reflect the close functional dependencies between heterogeneous components would be of utmost importance, the current state of affairs is a fragmentary coverage by the aforementioned disciplinary notions.

Synergies and research questions

The seminar set out to close the gap in the robustness investigations across the overlapping disciplines under the umbrella of CPS by gathering scientists from the entire spectrum of fields involved in the development of cyber-physical systems and their pertinent design theories. The seminar fostered interdisciplinary research answering the following central questions:

1. What is the rationale behind the plethora of existing notions of robustness and how are they related?
2. What measures have to be taken in a particular design domain (e.g., embedded software design) to be faithful to notions of robustness central to another domain it has functional impact on (e.g., feedback control)?
3. What forms of correctness guarantees are provided by the different notions of robustness and would there be potential for unification or synergy?
4. What design measures have been established by different disciplines for achieving robustness by construction, and how can they be lifted to other disciplines?
5. Where do current notions of robustness or current techniques of system design fall short and can this be alleviated by adopting ideas from related disciplines?

The overarching objective of such research would be to establish trusted engineering approaches incorporating methods for producing cyber-physical system designs

1. that sustain their correctness and performance guarantees even when used in a well-defined vicinity of their nominal operational regimes, and
2. that can be trusted to degrade gracefully even when some of the underlying modeling and analysis assumptions turn out to be false.

To satisfy these design objectives, we require notions of robustness that go well beyond the classical impurities of embedded systems, like sampling, measurement noise, jitter, and machine tolerances, and must draw on concepts of robustness from disparate fields. This seminar identified parallels between related notions of robustness from the many varied domains related to CPS design and bridged the divide between disciplines, with the goal of achieving the above objectives.

Topics of the Seminar

This seminar aimed to identify fundamental similarities and distinctions between various notions of robustness and accompanying design and analysis methods, with the goal of bringing together disparate notions of robustness from multiple academic disciplines and application domains. The following is a brief compendium of the robustness notions and application domains that were addressed in this seminar.

Robustness Notions and Design/Analysis Methods

One goal of this seminar was to identify crosscutting frameworks and design methodologies among the different approaches used to study robustness in the domains of control theory, computer science, and mechanical engineering. We considered the following broad classifications of robustness with the ultimate goal of synergizing the notions and techniques from the various disciplines.

- Input/Output Robustness
- Robustness with respect to system parameters
- Robustness in real-time system implementation
- Robustness due to unpredictable environments
- Robustness to Faults

Application Domains

The applications for the topics addressed in this seminar include cyber-physical systems for which robustness is a vital concern. The following is a partial list of these application domains.

- Automotive
- Aeronautics
- Medical devices
- Robotics
- Smart buildings
- Smart infrastructure

Outcome

We summarize the outcomes of the discussions in the break-out sessions that were conducted by forming subgroups among the participants. The topics referred to different approaches and/or applications in the framework of robustness. One of the topics was about robustness for discrete systems. In this session, the need for defining robustness for these systems was extensively discussed, and one of the most relevant challenges identified was to define appropriate metrics on the state-space relevant to the application. Also some specific robustness issues in the domain of medical devices and automotive systems were identified.

Another discussion was about guaranteeing robust performance from systems based on machine learning. This issue is a difficult task and it is growing in importance as many new safety critical applications, such as self-driving cars, are being designed using machine learning techniques. A challenge is to develop reliable methodologies for certifying or designing for robust performance for systems based on machine learning.

Discussions in a third break-out group were centered around the issue of established engineering means for obtaining robustness by design and how to accommodate these in

rigorous safety cases or formal proofs of correctness. A finding was that most formal models would currently require rather low-level coding of the dynamic behavior of such mechanisms, thereby requiring them to be re-evaluated on each new design rather than exploiting their guaranteed properties to simplify system analysis, which would be in line with their actual impact on engineering processes.

2 Table of Contents

Executive Summary

Martin Fränzle, James Kapinski, and Pavithra Prabhakar 29

Overview of Talks

Conformance-based robust semantics, and application to anytime control
Houssam Abbas 35

On Discrete Robustness in Controller Synthesis
Rüdiger Ehlers 35

Automatic Test Generation for Autonomous Vehicular Systems
Georgios Fainekos 36

When Robustness Comes for Free – Towards Laws of Large Numbers for Ultra-High Integrity Systems
Martin Fränzle 36

Automatically Robustifying Verified Hybrid Systems in KeYmaera X
Nathan Fulton 37

An algorithmic approach to global asymptotic stability verification of hybrid systems
Miriam García Soto 37

Automated Checking and Generation of Invariant Sets
Khalil Ghorbal 38

Connecting Robust Design with Testing
James Kapinski 38

Useful Robustness Notions For Some Industrial Examples
Jens Oehlerking 39

Automata-based approach to measuring robustness
Jan Otop 39

Robustness for compositional control design
Necmiye Ozay 40

Pre-orders for Reasoning about Stability Properties of Hybrid Systems
Pavithra Prabhakar 40

Uncertainty handling and robustness analysis of finite precision implementations
Sylvie Putot 41

Deciding the Undecidable
Stefan Ratschan 41

Towards Robustness for Cyber-Physical Systems
Matthias Rungger, Sina Caliskan, Rupak Majumdar, and Paulo Tabuada 41

Robust Cyber-Physical Systems: An utopia within reach
Paulo Tabuada 42

Temporal-logic-constrained synthesis and verification without discretization
Ufuk Topcu 42

Robustness in Self-Driving Cars
Eric M. Wolff 43


34 16362 – Robustness in Cyber-Physical Systems

Probabilistic Reachability for Hybrid Systems with Uncertain Parameters <i>Paolo Zuliani and Fedor Shmarov</i>	43
Participants	45

3 Overview of Talks

3.1 Conformance-based robust semantics, and application to anytime control

Houssam Abbas (University of Pennsylvania – Philadelphia, US)


License  Creative Commons BY 3.0 Unported license
© Houssam Abbas

We first describe a Skorokhod-like distance between signals, and generalize the robust semantics of MTL to base them on this new distance. We show that even though the new distance is not a metric, the resulting semantics still satisfy the fundamental properties of (metric-based) robust semantics. In particular, they can be used in a falsification framework. This opens the way to a principled application of robustness-guided falsification to application domains in hybrid systems where the difference between signals might not be adequately captured by the sup norm or other metrics. This new distance was motivated by work in the verification of cardiac devices, where it was found to provide better discrimination between fatal and non-fatal arrhythmias.

We next explore how to use the robust semantics for Anytime control: consider a controller that is being fed noisy state estimates. Can the controller make requests to the estimator, telling it to supply an estimate within a certain time delay, and with a certain error bound? This capability can be used by the controller to save computation power or perform “last-millisecond” aggressive maneuvers. When the control objective is low-level, we present a Model Predictive Control-based solution. We explore how a similar paradigm can be applied to higher-level specifications.

3.2 On Discrete Robustness in Controller Synthesis

Rüdiger Ehlers (Universität Bremen, DE)

License  Creative Commons BY 3.0 Unported license
© Rüdiger Ehlers
Joint work of Rüdiger Ehlers, Ufuk Topcu

A classical approach to CPS control is to first compute a faithful discrete abstraction of the physical environment and to then synthesize a discrete controller that ensures that the specification is satisfied on the discrete abstraction. The approach splits the question of how to obtain robust controllers, i.e., those that can tolerate deviations from the modeled environment conditions whenever possible, into two parts: (1) ensuring robustness of the discrete controller against glitches in the (discrete) abstraction of the environment and (2) making the execution of the continuous actions as robust as possible. We will reconsider the former problem in this talk and study the question if we can infer how the system should behave in case of environment assumption failures from the specification for the nominal operation case. A simple example shows that this is frequently not the case. The example is followed by an outlook on an approach to integrate the system engineer’s application knowledge of what constitutes robust behavior into the synthesis process of robust CPS controllers in the future.

3.3 Automatic Test Generation for Autonomous Vehicular Systems

Georgios Fainekos (Arizona State University – Tempe, US)

License © Creative Commons BY 3.0 Unported license
© Georgios Fainekos

Joint work of Cumhuri Erkan Tuncali, Theodore P. Pavlic

Main reference C. E. Tuncali, T. P. Pavlic, G. Fainekos, “Utilizing S-TaLiRo as an Automatic Test Generation Framework for Autonomous Vehicles,” in Proc. of the 19th IEEE Int’l Conf. on Intelligent Transportation Systems (ITCS’16), pp. 1470–1475, IEEE, 2016.

URL <http://dx.doi.org/10.1109/ITSC.2016.7795751>

Dynamic safety for autonomous vehicular systems is easy to define: avoid collisions at all costs. This definition leads to a natural notion of robustness: keep the distance from all objects of interest as large as possible. Similarly, for passive safety, a system is more robust when the damage to the vehicle is minimized. Even though such notions of robustness may be useful for system design, they are not necessarily useful for the automatic test generation and falsification problems for dynamic safety. Falsification seeks to detect system behaviors that exhibit minimum robustness. Under these metrics, it is easy to produce scenarios where the system under test fails unavoidably and catastrophically. In this work, we define a robustness metric (or, more accurately, a cost function) that combines notions of dynamic and passive safety in order to detect boundary conditions between safe and unsafe behaviors. We demonstrate our results on a simple scenario of autonomous vehicles driving on a multi-lane road.

3.4 When Robustness Comes for Free – Towards Laws of Large Numbers for Ultra-High Integrity Systems

Martin Fränzle (Universität Oldenburg, DE)

License © Creative Commons BY 3.0 Unported license
© Martin Fränzle

Joint work of Martin Fränzle, Sebastian Gerwinn, Ingo Stierand

Statistical physics successfully derives almost sure – i.e., very robust- properties of large ensembles from unpredictable component behavior. Given that cyber-physical systems (CPS) are in fact large ensembles of components, we address the question whether we may expect similar emergent properties of ensembles within CPS and whether these implicitly robustify our systems, giving “robustness for free”. We exemplify that effect and demonstrate the underlying mathematics on a single example we very recently have successfully analyzed. It deals with the hard real-time analysis of task systems and is meant to serve as a demonstrator shedding light on the more general applicability of the concept.

Historically in research on real-time systems, hard real-time (in the sense that missing a deadline may have catastrophic effect on the system or its environment) has always been identified with worst-case timing (in the sense of worst-case execution times of tasks, worst-case end-to-end latencies in circuits or reactive systems, etc.). The question, however, is whether this identification is scientifically valid? Given that, e.g., the likelihood of actually encountering the worst-case execution time (WCET) of a single task in a task system already is low (which is why empirical WCET determination is so hard), the probability of simultaneously encountering close to worst-case behavior on most tasks in a set of hundreds of tasks seems to be bound to be astronomically low – probably too low to even worry about. Do we thus really need to care for the sum of the individual tasks’ WCETs when computing

the utilization, response time, etc., in the various established schedulability checks? Or would a weaker criterion suffice to establish likelihoods of deadline hits high enough to be acceptable even for extreme integrity systems in highly safety-critical domains?

To address these questions, we set up a formal model facilitating to compute rigorous answers to this question. We therefore reconsider the notion of hard real-time, giving it a stochastic tweak of extremely high confidence rather than sure dead-line hit, and devise a pertinent formal model and analysis method. The reader should note that the question at hand is very different from average-case analysis, which can be pursued with scrutiny by various techniques, among them statistical model-checking (SMC) as a general-purpose tool not requiring any particular theory development. The assurance levels we want to achieve are, however, far beyond its scope, which proves both a burden, as the straightforward techniques like SMC fail, and a virtue, permitting us to set up a powerful approximation theory for those rare events. This theory rigorously proves that the likelihood of a full task system to exceed a certain percentile – say 90%.

3.5 Automatically Robustifying Verified Hybrid Systems in KeYmaera X

Nathan Fulton (Carnegie Mellon University – Pittsburgh, US)

License © Creative Commons BY 3.0 Unported license
© Nathan Fulton

Formal verification of realistic hybrid systems models is an iterative endeavor. Verification efforts typically begin with a simple system model that elides most sources of uncertainty and disturbance. After this relatively simple verification task is completed, the model is robustified against sensing error, actuation uncertainty, plant disturbances, adversarial environments, and other sources of uncertainty or disturbance that arise during testing and simulation. Each new source of uncertainty or disturbance further complicates the model and therefore requires a systematic but none-the-less time-intensive re-verification.

This talk presents early work toward a systematic approach for automatically hardening previously verified hybrid systems against sources of uncertainty and disturbance without requiring re-verification of the robustified system, and discusses an ongoing implementation of this technique in the KeYmaera X theorem prover.

3.6 An algorithmic approach to global asymptotic stability verification of hybrid systems

Miriam García Soto (IMDEA Software – Madrid, ES)

License © Creative Commons BY 3.0 Unported license
© Miriam García Soto

Joint work of Pavithra Prabhakar, Miriam García Soto

Main reference P. Prabhakar, M. García Soto, “An algorithmic approach to global asymptotic stability verification of hybrid systems”, in Proc. of the 2016 Int’l Conf. on Embedded Software (EMSOFT’16), pp. 9:1–9:10, ACM, 2016.

URL <http://dx.doi.org/10.1145/2968478.2968483>

I will present an algorithmic approach to global asymptotic stability (GAS) verification of hybrid systems. Global asymptotic stability is a fundamental property in control system

design which states that small perturbations in the equilibrium point result in only small perturbations in the behaviour of the system, and every execution of the system converges to the equilibrium point. The broad approach is to reduce GAS verification to local asymptotic stability (AS) and region stability (RS) verification. The AS problem is solved by using a quantitative predicate abstraction technique which is also used to compute a stability zone. The RS problem is stated with respect to the stability zone and it is solved by applying an abstraction technique and by performing a termination analysis over it. Positive results of both verification problems result in GAS of the hybrid system. The GAS analysis theory is developed for the case of polyhedral switched systems. The technique is applied to an automatic gearbox model, and provides a GAS proof for this model. Most of the analysis is automated except for certain tasks such as the predicate selection defining the stability zone.

3.7 Automated Checking and Generation of Invariant Sets

Khalil Ghorbal (INRIA – Rennes, FR)

License  Creative Commons BY 3.0 Unported license
© Khalil Ghorbal

We focus on dynamical systems described by ordinary differential equations with polynomial right-hand side. We investigate two questions of interest for those systems: (i) decision procedures for the invariance of semi-algebraic sets for a given dynamical system, and (ii) the automated generation of invariant algebraic and semi-algebraic sets. We enumerate and theoretically compare previously reported methods as well as the most recent ones. We also empirically assess the practical running performance of such methods on a generic set of benchmarks. The advantages and limitations of such methods will be clearly established throughout the talk.

3.8 Connecting Robust Design with Testing


James Kapinski (Toyota Technical Center – Gardena, US)

License  Creative Commons BY 3.0 Unported license
© James Kapinski

Robust design paradigms provide the capability of designing systems that meet performance standards in the presence of parameter variations and disturbances, but they do not guarantee that the deployed system exhibits robust performance. Testing is required to ensure that the system that is ultimately realized displays robust performance. The goal of robust design techniques can therefore be viewed as a means to reduce the amount of testing required to achieve the necessary level of robust performance. This talk argues that artifacts obtained through robust design practices should be used to reduce the effort involved in the test and calibration phases of development. Also, knowledge gained through tests should be used to update the abstractions used in the robust design phase.

3.9 Useful Robustness Notions For Some Industrial Examples

Jens Oehlerking (Robert Bosch GmbH – Stuttgart, DE)

License  Creative Commons BY 3.0 Unported license
© Jens Oehlerking

A plethora of robustness notions have been defined in recent years for many model classes and engineering domains. In this talk, three example system from the automotive industry were presented, focusing on useful robustness notions that can be interpreted by engineers. In general, robustness notions tend to be more useful in this context, if they can be traced back to quantities over which the engineer has some form of control. This includes (both physical and non-physical) system parameters, as well as control inputs. In contrast to this, many robustness notions provided by academia focus on quantifying the distance of output signals to desirable or undesirable behavior, leading to robustness metrics that cannot easily be interpreted by an engineer. While such metrics are still very useful (e.g., in the context of optimization based test case generation), it seems that they are not ideal with an engineer in the loop. Therefore, in this talk, a parallel was drawn to approaches for the inversion of dynamical systems, e.g, flatness-based feedforward control. There, the goal is to derive an optimal control input signal given a desired control output signal based on an inverse model. Since it seems that some kind of inverse model is also needed to map robustness notions on system output back onto robustness notions of system inputs or parameters, the question was raised whether this would be a useful research direction.

3.10 Automata-based approach to measuring robustness

Jan Otop (University of Wroclaw, PL)

License  Creative Commons BY 3.0 Unported license
© Jan Otop

Joint work of Thomas A. Henzinger, Jan Otop, Roopsha Samanta

Main reference T. A. Henzinger, J. Otop, “Model measuring for discrete and hybrid systems”, *Nonlinear Analysis: Hybrid Systems*, Vol. 23, pp. 166–190, 2017.

URL <http://dx.doi.org/10.1016/j.nahs.2016.09.001>

Robust systems are the one that continue to work correctly despite of perturbations. The perturbation model is crucial here; we therefore refer to robustness of a system with respect to specific perturbations. Also, it is unlikely that a system is completely immune to all perturbations. This motivates quantitative approach to robustness, where systems are characterized by the level of (specific) perturbations, which they tolerate.

In this talk, I present an automata-based approach to robustness, where perturbations are modeled by weighted automata. The resulting frameworks subsume (some) previously studied notions of robustness, and allow for modelling of a wide range of perturbations, which are additionally graded. Grading perturbations enables us to measure robustness (i.e., establish the level of perturbations safe for the system).

3.11 Robustness for compositional control design

Necmiye Ozay (University of Michigan – Ann Arbor, US)

License  Creative Commons BY 3.0 Unported license
© Necmiye Ozay

Joint work of Stanley Smith, Petter Nilsson, Necmiye Ozay


Composing controllers designed individually for interacting subsystems, while preserving the guarantees that each controller provides on each subsystem is a challenging task. In this talk, I will present some of our recent work on using robust control design techniques for compositional design of complex decentralized safety controllers for cyber-physical systems. I will start by introducing some classical qualitative and quantitative notions of robustness in control and estimation. Then, I will present a method for synthesis of controlled invariant sets and associated controllers, that is robust against affine parametric uncertainties in the system matrices. Given a complex system composed of linear parameter varying subsystems, where the system matrices of each subsystem depend (possibly nonlinearly) on the states of the other subsystems, this method can be used for separately designing controllers for subsystems if the uncertainty imposed by a subsystem onto others can be quantified. I will present asymptotically tight techniques for quantification of the uncertainty. Finally, an application of the overall design methodology to vehicle safety systems will be presented. In particular, I will demonstrate how controllers for lane-keeping and adaptive cruise control can be synthesized in a compositional way using the proposed techniques. Our simulations illustrate how these controllers keep their individual safety guarantees when implemented simultaneously, as the theory suggests.

References

- 1 S. W. Smith, P. Nilsson, and N. Ozay, “Interdependence quantification for compositional control synthesis with an application in vehicle safety systems”, Proc. 55th IEEE Conference on Decision and Control (CDC), Las Vegas, NV, December 2016.
- 2 P. Nilsson and N. Ozay, “Synthesis of separable controlled invariant sets for modular local control design”, Proc. American Control Conference (ACC), Boston, MA, July 2016.

3.12 Pre-orders for Reasoning about Stability Properties of Hybrid Systems

Pavithra Prabhakar (Kansas State University – Manhattan, US)

License  Creative Commons BY 3.0 Unported license
© Pavithra Prabhakar

An important class of robustness specifications in control system design is stability. Stability captures the property that small perturbations in the initial state or input lead to only small deviations in the system behavior. We discuss the generalization of stability notions to hybrid systems, and investigate preorders on hybrid systems that preserve stability. The preorders strengthen the classical notions of simulations/bisimulations with uniform continuity conditions that forces preservation of the stability notions.

3.13 Uncertainty handling and robustness analysis of finite precision implementations

Sylvie Putot (Ecole Polytechnique – Palaiseau, FR)

License © Creative Commons BY 3.0 Unported license
© Sylvie Putot

Joint work of Eric Goubault, Sylvie Putot

Main reference E. Goubault, S. Putot, “Robustness analysis of finite precision implementations”, in Proc. of the 11th Asian Symp. on Programming Languages and Systems (APLAS’13), LNCS, Vol. 8301, pp. 50–57, Springer, 2013.

URL http://dx.doi.org/10.1007/978-3-319-03542-0_4

A desirable property of control systems is robustness to inputs, when small perturbations of the inputs of a system will cause only small perturbations on outputs. This property should be maintained at the implementation level, where close inputs can lead to different execution paths. The problem becomes crucial for finite precision implementations, where any elementary computation is affected by an error. In this context, almost every test is potentially unstable, that is, for a given input, the finite precision and real numbers paths may differ. Still, state-of-the-art error analyses often rely on the stable test hypothesis, yielding unsound error bounds when the conditional block is not robust to uncertainties. We propose an abstract-interpretation based error analysis of finite precision implementations, which is sound in presence of unstable tests, by bounding the discontinuity error for path divergences. This gives a tractable analysis implemented in the FLUCTUAT analyzer.

3.14 Deciding the Undecidable

Stefan Ratschan (The Czech Academy of Sciences – Prague, CZ)

License © Creative Commons BY 3.0 Unported license
© Stefan Ratschan

Main reference P. Franek, S. Ratschan, P. Zgliczynski, “Quasi-decidability of a Fragment of the First-Order Theory of Real Numbers”, *Journal of Autom. Reasoning*, 57(2):157–185, 2016.

URL <http://dx.doi.org/10.1007/s10817-015-9351-3>

Every engineer strives for robustness, simply because models of physical systems have to be robust to be able to work in practice. But robustness has another advantage: it is beneficial for computation. Especially, undecidable problems can become solvable under the assumption of robustness. In the talk, I discussed some results in this direction.

3.15 Towards Robustness for Cyber-Physical Systems

Matthias Rungger (TU München, DE), Sina Caliskan, Rupak Majumdar (MPI-SWS – Kaiserslautern, DE), and Paulo Tabuada (University of California at Los Angeles, US)

License © Creative Commons BY 3.0 Unported license
© Matthias Rungger, Sina Caliskan, Rupak Majumdar, and Paulo Tabuada

Main reference P. Tabuada, S. Y. Caliskan, M. Rungger, R. Majumdar, “Towards Robustness for Cyber-Physical Systems”, *IEEE Trans. Automat. Contr.*, 59(12):3151–3163, 2014.

URL <http://dx.doi.org/10.1109/TAC.2014.2351632>

Robustness as a system property describes the degree to which a system is able to function correctly in the presence of disturbances, i.e., unforeseen or erroneous inputs. In this talk, we present a notion of robustness termed input-output dynamical stability for cyber-physical

systems (CPS) which merges existing notions of robustness for continuous systems and discrete systems. The notion captures two intuitive aims of robustness: bounded disturbances have bounded effects and the consequences of a sporadic disturbance disappear over time. For cyber systems modeled as finite-state transducers, the proposed notion of robustness can be verified in pseudo-polynomial time. The synthesis problem, consisting of designing a controller enforcing robustness, can also be solved in pseudo-polynomial time.

3.16 Robust Cyber-Physical Systems: An utopia within reach

Paulo Tabuada (University of California at Los Angeles, US)

License  Creative Commons BY 3.0 Unported license
© Paulo Tabuada

Joint work of Daniel Neider, Paulo Tabuada

Main reference P. Tabuada, D. Neider, “Robust Linear Temporal Logic”, in Proc. of the 25th EACSL Annual Conference on Computer Science Logic (CSL’16), LIPIcs, Vol. 62, pp. 10:1–10:21, Schloss Dagstuhl, 2016.

URL <http://dx.doi.org/10.4230/LIPIcs.CSL.2016.10>

Robustness plays a major role in the analysis and design of engineering systems. Although robust control is a well established area within control theory and fault-tolerant computation is a well established area within computer science, it is surprising that robustness remains a distant mirage for Cyber-Physical Systems. The intricate crochet made of control, computation, and communication yarns is known to be brittle in the sense that “small” software errors or “small” sensing, communication, or actuation noise can lead to unexpected, and often unintended, consequences. In this talk I will build on classical notions of robustness from control theory and computer science to make progress towards the utopia of robust Cyber-Physical Systems.

3.17 Temporal-logic-constrained synthesis and verification without discretization

Ufuk Topcu (University of Texas – Austin, US)

License  Creative Commons BY 3.0 Unported license
© Ufuk Topcu

Joint work of Ivan Papusha, Jie Fu, Ufuk Topcu, Richard Murray, Tichakorn Wongpiromsarn, Andrew Lamperski

Can we algorithmically synthesize temporal-logic-constrained controllers for dynamical systems with 50 continuous states? Using conventional methods based on discretization, the answer is ‘no’. Even the coarsest discretization would result in intractably large discrete state spaces.

We present a novel approach that avoids explicit discretization in synthesis. We investigate the synthesis of optimal controllers for continuous-time and continuous-state systems under temporal logic specifications. We consider a setting in which the specification can be expressed as a deterministic, finite automaton (the specification automaton) with transition costs, and the optimal system behavior is captured by a cost function that is integrated over time. Specifically, we construct a dynamic programming problem over the product of the underlying continuous-time, continuous-state system and the discrete specification automaton. This dynamic programming formulation relies on the optimal substructure of the additive transition costs over the product of the system and specification automaton. Furthermore,

we propose synthesis algorithms based on approximate dynamic programming for both linear and nonlinear systems under temporal logic constraints. We show that, for linear systems under co-safe temporal logic constraints, this approximate dynamic programming solution reduces to a semidefinite program.

As time allows, we overview a similar approach for the dual problem of verification of dynamical systems against temporal logic specifications. This approach combines automata-based verification and the use of so-called barrier certificates.

References

- 1 Ivan Papusha, Jie Fu, Ufuk Topcu and Richard Murray. *Automata Theory Meets Approximate Dynamic Programming: Optimal Control with Temporal Logic Constraints*. Conference on Decision and Control, 2016.
- 2 Tichakorn Wongpiromsarn, Ufuk Topcu and Andrew Lamperski. *Automata theory meets barrier certificates: Temporal logic verification of nonlinear systems*. IEEE Transactions on Automatic Control, <http://dx.doi.org/10.1109/TAC.2015.2511722>, 2015.

3.18 Robustness in Self-Driving Cars

Eric M. Wolff (nuTonomy – Cambridge, US)

License © Creative Commons BY 3.0 Unported license
© Eric M. Wolff

Joint work of nuTonomy team

Self-driving cars are poised to revolutionize transportation, potentially making travel safer, cheaper, and more efficient. Numerous teams have demonstrated autonomous driving on public roads with a safety driver, but there are key technical challenges that must be answered before the safety driver can be removed.

In this talk, I will overview the (public) state-of-the-art in self-driving cars, specifically related to verification and validation. I will introduce different notions of robustness as related to planning, control, perception, and localization, and discuss how careful composition of these subsystems can make the entire system more robust and easier to validate.

3.19 Probabilistic Reachability for Hybrid Systems with Uncertain Parameters

Paolo Zuliani (University of Newcastle, GB) and Fedor Shmarov

License © Creative Commons BY 3.0 Unported license
© Paolo Zuliani and Fedor Shmarov

Joint work of Fedor Shmarov, Paolo Zuliani

Main reference F. Shmarov, P. Zuliani, “Probabilistic Hybrid Systems Verification via SMT and Monte Carlo Techniques,” in Proc. of the 12th Haifa Verification Conf. (HVC’16), LNCS, Vol. 10028, pp. 152–168, Springer, 2016.

URL http://dx.doi.org/10.1007/978-3-319-49052-6_10

Hybrid systems are a framework much used for modelling cyber-physical systems, and are finding more application in other areas, such as systems biology and systems medicine. Reachability is a key verification analysis: in this talk I will focus on bounded reachability, i.e., in a finite number of steps (or jumps). If a hybrid system contains random parameters, then reachability amounts to computing a probability; if the system also features uncertain

(nondeterministic) parameters, then reachability generalises to finding enclosures for reachability probabilities. In this talk I will survey our two approaches to probabilistic bounded reachability. One is fully rigorous – and comes high computational complexity – and one is a mixture of a rigorous and a statistical approach, thereby yielding better scalability by trading absolute guarantees with statistical guarantees.

Participants

- Houssam Abbas
University of Pennsylvania – Philadelphia, US
- Paul Bogdan
USC – Los Angeles, US
- Alexandre Donzé
University of California – Berkeley, US
- Rüdiger Ehlers
Universität Bremen, DE
- Georgios Fainekos
Arizona State University – Tempe, US
- Martin Fränzle
Universität Oldenburg, DE
- Nathan Fulton
Carnegie Mellon University – Pittsburgh, US
- Miriam García Soto
IMDEA Software – Madrid, ES
- Khalil Ghorbal
INRIA – Rennes, FR
- James Kapinski
Toyota Technical Center – Gardena, US
- Scott C. Livingston
Washington D.C., US
- Sarah M. Loos
Google Research, US
- Rupak Majumdar
MPI-SWS – Kaiserslautern, DE
- Jens Oehlerking
Robert Bosch GmbH – Stuttgart, DE
- Jan Otop
University of Wroclaw, PL
- Necmiye Ozay
University of Michigan – Ann Arbor, US
- Pavithra Prabhakar
Kansas State University – Manhattan, US
- Sylvie Putot
Ecole Polytechnique – Palaiseau, FR
- Stefan Ratschan
The Czech Academy of Sciences – Prague, CZ
- Matthias Rungger
TU München, DE
- Paulo Tabuada
University of California at Los Angeles, US
- Ufuk Topcu
University of Texas – Austin, US
- Eric M. Wolff
nuTonomy – Cambridge, US
- Bai Xue
Universität Oldenburg, DE
- Paolo Zuliani
University of Newcastle, GB

