Report from Dagstuhl Seminar 14122

Verification of Cyber-Physical Systems

Edited by

Rupak Majumdar[1], Richard M. Murray[2], and Pavithra Prabhakar[3]

1 **Max Planck Institute for Software Systems, Germany** rupak@mpi-sws.org
2 **California Institute of Technology, USA** murray@cds.caltech.edu
3 **IMDEA Software Institute, Spain** pavithra.prabhakar@imdea.org

Abstract

Cyber-physical systems refer to a new genre of engineered systems consisting of a tight coupling between computation, communication and physical entities. The main focus of the seminar was to discuss issues related to the reliable development of cyber-physical systems by using formal verification. This is a multi-disciplinary area requiring collaboration between areas focusing discrete systems analysis and continuous systems analysis. To this end, the seminar brought together researchers working in the fields of formal methods, control theory and hybrid systems to identify and discuss potential issues and research questions which require collaboration between the communities. This report documents the program and the outcomes of Dagstuhl Seminar 14122 "Verification of Cyber-Physical Systems".

Seminar March 17–21, 2014 – http://www.dagstuhl.de/14122
1998 ACM Subject Classification D.2.4 Software/Program Verification, B.1.2 Control Structure Performance Analysis and Design Aids
Keywords and phrases Formal Verification, Cyber-Physical Systems, Hybrid Systems
Digital Object Identifier 10.4230/DagRep.4.3.85

1 Executive Summary

Rupak Majumdar
Richard M. Murray
Pavithra Prabhakar

Introduction

Cyber-physical systems are systems in which there exists a tight coupling between computation, communication and control. The drastic reduction in the cost of sensing, actuating, computing and communicating technology has enabled the proliferation of this new genre of engineered systems in which a network of embedded processors interact tightly with the physical world to achieve complex functionalities. They have applications in a wide-range of systems spanning communication, infrastructure, energy, health-care, manufacturing, military, robotics and transportation.

Cyber-physical systems are believed to be the systems of the future with an impact on the engineering systems technology comparable to the impact the internet had on the information systems. Governments around the world have taken several initiatives to exploit this potential. The report of the US President's Council of Advisors on Science and Technology (PCAST) has placed Cyber-Physical Systems on the top of the priority list for federal research investment.

Verification of Cyber-Physical Systems, *Dagstuhl Reports*, Vol. 4, Issue 3, pp. 85–102
Editors: Rupak Majumdar, Richard M. Murray, and Pavithra Prabhakar
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

The European Union has recognized the strategic importance of Embedded Computing Systems and has launched the ARTEMIS Joint Technology Initiative (JTI) as part of the FP7 program. Also, the latest European Commission Work Programme 2013 for Information and Communication technologies identifies this with the Objective ICT-2013.3.4 dedicated to Advanced Computing, Embedded and Control systems.

Cyber-Physical Systems have immense potential for a long-term impact on the society. At the same time, the unprecedented complexity arising due to the interleaving of the cyber and the physical components is overwhelming. On one hand, digital systems operate is a discrete manner, where computation and communication proceed in synchronization with the processor cycles. On the other hand, physical systems execute continuously in dense real-time. Hence, cyber-physical systems are complex systems exhibiting both discrete and continuous behaviors, and are networked and/or distributed with possibly humans in the loop. The grand challenge of the near future is the development of design methodologies and tools to cater to the development of reliable cyber-physical systems.

Model-based development has emerged as the de facto product development process in several domains including automotive and aeronautics. Here, the product development cycle begins with an abstract mathematical model of the system which is subject to rigorous analysis. The code is then generated from the model either automatically or manually. This enables early detection and correction of bugs which in turn results in the reduction of development costs and time, thereby providing companies with a competitive edge. However, the techniques used for analysis based on simulation of the mathematical models is still ad hoc, and does not provide the high level of reliability guarantees expected out of safety-critical CPS. Formal verification is an alternative approach which aims to provide a proof of correctness of the system. It is a promising technique for achieving the goal of developing high confidence cyber-physical systems.

Outcomes of the seminar

The seminar focused on the challenges in the application of formal methods towards verification of CPS. The seminar had a total of 28 participants with a mix of computer scientists and control theorists.

Tutorials

Given the cross disciplinary nature of the seminar, 6 tutorials were arranged on the following topics to provide a common ground to enable researchers with different backgrounds to communicate.

1. Simulation-Based Techniques for the Falsification of Cyber-Physical Systems
2. Verification of Automotive Engine Control
3. Formal Methods for Control Design
4. On Optimal and Reasonable Control in the Presencve of Adversaries
5. Compositionality Results for Cardiac Cell Dynamics
6. Logic of Hybrid Games

Sessions

The following topics were identified as important issues in the application of formal verification to CPS. A separate session was dedicated to discuss the topics in the context of CPS.

1. **Simulation based methods**: Application of simulation techniques for performing verification of CPS was discussed.
2. **Using verification for control design**: This session focused on the application of formal verification techniques such as those based on abstractions for control design.
3. **Foundation of CPS**: This session discussed the complexity and decidability of problems in verification and control of CPS.
4. **Applications**: This session discussed the methods and challenges in the verification of aircraft control, biological systems and multi-robot path planning.
5. **Abstractions**: This session discussed the issues regarding simplification techniques for scalable analysis of CPS.
6. **Lyapunov based methods**: This session discussed notions of stability and techniques for their analysis.
7. **Constraint solving**: Several verification problems can be formulated as constraint solving problems. This session discussed the challenges in constraint solving problems arising in CPS.
8. **Symbolic Verification**: This session discussed problems related to building efficient algorithms and tools for symbolic state-space exploration.

Research Directions

The seminar successfully fostered communication between computer scientist and control theorist. Some challenges and research directions were identified such as the need for the development of compositional reasoning of CPS with multiple components and lightweight analysis methods to boost scalability (such as using simulation for verification).

2 Table of Contents

Executive Summary
Rupak Majumdar, Richard M. Murray, and Pavithra Prabhakar 85

Overview of Talks

Formal Methods for Dynamical Systems
Calin Belta 90

Guided Search for Hybrid Systems
Sergiy Bogomolov 90

Verification of Automotive Engine Control
Ken Butts 91

Flow*: Reachability Analysis of Non-Linear Hybrid Systems
Xin Chen 91

Conflict-Tolerant Specifications
Deepak D'Souza 91

Parameter Synthesis for Biological Models
Thao Dang 92

Simulation-Guided Formal Analysis
Jyotirmoy V. Deshmukh 92

Descending MTL Robustness
Georgios Fainekos 93

Reachability in Space-Time for Piecewise Affine Dynamics
Goran Frehse 93

Compositionality Results for Cardiac Cell Dynamics
Radu Grosu 94

Two Approaches to Applying Verification to Control Design
Bruce Krogh 94

Finite-time Lyapunov functions
Mircea Lazar 94

On Optimal and Reasonable Control in the Presencve of Adversaries
Oded Maler 95

Scalable Techniques for Viability Kernels and Safe Control Synthesis in Linear Time Invariant Systems
Ian Mitchell 95

Verification of Nonlinear Models with Modular Annotations
Sayan Mitra 95

Challenges in Verification of Hybrid Systems for Aerospace Applications
Richard M. Murray 96

Logic of Hybrid Games
André Platzer 96

Algorithmic Verification of Stability of Hybrid Systems
Pavithra Prabhakar 97

Highlights on Recent Progresses in Quantitative Games
Jean-François Raskin 97

Analysis and Synthesis of CPS using EF-SMT
Harald Ruess 98

Compositional Synthesis of Multi-Robot Motion Plans via SMT Solving
Indranil Saha 99

Simulation-Based Techniques for the Falsification of Cyber-Physical Systems
Sriram Sankaranarayanan 99

Certified-by-design control of systems over finite alphabets
Danielle Tarraf 100

EF-SMT
Ashish Tiwari 100

Stability of Linear Autonomous Systems Under Regular Switching Sequences
Mahesh Viswanathan 100

Participants 102

3 Overview of Talks

3.1 Formal Methods for Dynamical Systems

Calin Belta (Boston University, Brookline, US, cbelta@bu.edu)

In control theory, "complex" models of physical processes, such as systems of differential equations, are usually checked against "simple" specifications, such as stability and set invariance. In formal methods, "rich" specifications, such as languages and formulae of temporal logics, are checked against "simple" models of software programs and digital circuits, such as finite transition graphs. With the development and integration of cyber physical and safety critical systems, there is an increasing need for computational tools for verification and control of complex systems from rich, temporal logic specifications.

The formal verification and synthesis problems have been shown to be undecidable even for very simple classes of infinite-space continuous and hybrid systems. However, provably correct but conservative approaches, in which the satisfaction of a property by a dynamical system is implied by the satisfaction of the property by a finite over-approximation (abstraction) of the system, have received a lot of attention in recent years. The focus of this talk is on discrete-time linear systems, for which it is shown that finite abstractions can be constructed through polyhedral operations only. By using techniques from model checking and automata games, this allows for verification and control from specifications given as Linear Temporal Logic (LTL) formulae over linear predicates in the state variables. The usefulness of these computational tools is illustrated with various examples.

3.2 Guided Search for Hybrid Systems

Sergiy Bogomolov (Universität Freiburg, DE, bogom@informatik.uni-freiburg.de)

Hybrid systems represent an important and powerful formalism for modeling real-world applications such as embedded systems. A verification tool like SpaceEx is based on the exploration of a symbolic search space (the region space). As a verification tool, it is typically optimized towards proving the absence of errors. In some settings, e.g., when the verification tool is employed in a feedback-directed design cycle, one would like to have the option to call a version that is optimized towards finding an error path in the region space. A recent approach in this direction is based on guided search. Guided search relies on a cost function that indicates which states are promising to be explored, and preferably explores more promising states first. In this talk, we present two approaches to define and compute efficient cost functions. We develop our approaches on the top of the symbolic hybrid model checker SpaceEx which uses regions as its basic data structures.

In the first part of the talk, we introduce a box-based distance measure which is based on the distance between regions in the concrete state space. In the second part of the talk, we discuss an abstraction-based cost function based on pattern databases for guiding the reachability analysis. For this purpose, a suitable abstraction technique that exploits the flexible granularity of modern reachability analysis algorithms is introduced. We illustrate the practical potential of our approaches in several case studies.

3.3 Verification of Automotive Engine Control

Ken Butts (Toyota Technical Center, Ann Arbor, US, ken.butts@tema.toyota.com)

In-vehicle control systems provide improved fuel consumption, emissions, vehicle dynamics and active safety features for the automotive customer. Attendant with these improvements is increased system and software complexity and thus, effective system verification and validation (V&V) is critical to assure dependability and reliability. Our group strives to apply advanced V&V to automotive engine control in a Model-Based Development (MBD) context.

In our work, we observe the following automotive control system characteristics:

1. The systems under control (i.e. the plant) are nonlinear and often hybrid in nature.
2. The systems are developed iteratively and thus, legacy designs play a prominent role.
3. Due to 1) and 2) above, the design synthesis process has been largely incremental and ad-hoc, though ISO26262 is yielding traceable-requirements-driven processes.
4. The de-facto standard control design development environment is Matlab/Simulink while the use of acausal methods (e.g. Modelica, Simscape, VHDL-AMS) for plant modeling is emerging.

In this talk, we outline how these observed characteristics motivate our research and present an overview of our current activities. We hope to learn new and effective ways to synthesize and verify in-vehicle control systems this workshop.

3.4 Flow*: Reachability Analysis of Non-Linear Hybrid Systems

Xin Chen (RWTH Aachen University, DE, xin.chen@cs.rwth-aachen.de)

In this talk, we give a brief introduction of Flow* which is a reachability analysis tool for non-linear continuous and hybrid systems. Since the reachability problem on hybrid systems is not decidable, the tool computes an over-approximation which is represented by a finite set of Taylor models for the reachable set in bounded time horizon and number of jumps. The flowpipe/guard intersections are handled by the techniques of domain contraction and range over-approximation. They are extensions of the Taylor model method developed by Berz and Makino. To improve the performance of the tool, various techniques and heuristics are applied, and the effectiveness of them is demonstrated by several applications.

3.5 Conflict-Tolerant Specifications

Deepak D'Souza (Indian Institute of Science, Bangalore, IN, deepakd@csa.iisc.ernet.in)

We consider the setting of a plant under the control of multiple independent controllers. Such systems are common in telecom, automobile, and other embedded domains. We propose

a mechanism for specifying the behaviour of such controllers, called a conflict-tolerant specification, which is modular and gives us a compositional way of reasoning about the behaviour of the overall system. The theory is developed for discrete, timed, and hybrid system models.

This is joint work with Madhu Gopinathan, Prahlad Sampath, S. Ramesh, and others.

3.6 Parameter Synthesis for Biological Models

Thao Dang (VERIMAG, Gieres, FR, thao.dang@imag.fr)

Parameter determination is an important task in the development of biological models. In this paper we consider parametric polynomial dynamical systems and address the following parameter synthesis problem: find a set of parameter values so that the resulting system satisfies a desired property. Our synthesis technique exploits the Bernstein polynomial representation to solve the synthesis problem using linear programming. We apply our framework to two case studies involving epidemic models.

3.7 Simulation-Guided Formal Analysis

Jyotirmoy V. Deshmukh (Toyota Technical Center, US, jyotirmoy.deshmukh@tema.toyota.com)

Industrial-scale control systems are often developed in the model-based development (MBD) paradigm. This typically involves capturing a 'plant model' that describes the dynamical characteristics of physical processes within the system, and a 'controller model,' which is a block-diagram-based representation of the software used to regulate the plant behavior. In practice, plant models and controller models are highly complex; typical features include highly nonlinear and hybrid dynamics, dynamics involving delay differential equations, look-up tables storing pre-computed values, several levels of design-hierarchy, and design-blocks that operate at different frequencies. Design validation in the industry often takes the form of extensive testing on various platforms such in-vehicle testing, hardware-in-the-loop simulations, and software/model-in-the-loop simulations. The Simulink modeling framework (from the MathWorks) has become the de facto standard across industry for describing closed-loop plant + controller MBD designs. The key feature of this framework is a high-fidelity simulation tool, routinely used by control designers to experimentally validate their controller designs. In effect, we have a situation where designers have access to a wide range of methods that can perform extensive (but not exhaustive) simulations of a system. On the other end of the spectrum, the hybrid systems community has been developing a number of formal verification techniques that provide sound (but conservative and hence inaccurate) results. We consider the question: 'What can we "formally" accomplish if all we have is the ability to simulate a system?' As a tentative answer to this question, we suggest a paradigm called "Simulation-guided Formal Analysis". Such a framework could include key components such as procedures to perform inductive learning from simulations, procedures to check whether the information learned from simulations is consistent with all

behaviors of the model being simulated, and techniques that focus on best-effort verification with probabilistic completeness guarantees. As an instance of this paradigm, we present a technique to discover Lyapunov functions for nonlinear and hybrid systems from simulation data using linear programming techniques, global optimization tools and nonlinear SMT solvers.

3.8 Descending MTL Robustness

Georgios Fainekos (Arizona State University, Tempe, US, fainekos@asu.edu)

Metric Temporal Logic (MTL) specifications can capture complex state and timing requirements. Given a nonlinear dynamical system and an MTL specification for that system, our goal is to find a trajectory that violates or satisfies the specification. This trajectory can be used as a concrete feedback to the system designer in the case of violation or as a trajectory to be tracked in the case of satisfaction. The search for such a trajectory is conducted over the space of initial conditions, system parameters and input signals. We convert the trajectory search problem into an optimization problem through MTL robust semantics. Robustness quantifies how close the trajectory is to violating or satisfying a specification. Starting from some arbitrary initial condition and parameter and given an input signal, we compute a descent direction in the search space, which leads to a trajectory that optimizes the MTL robustness. This process can be iterated to reach local optima (min or max). We demonstrate the method on examples from the literature.

3.9 Reachability in Space-Time for Piecewise Affine Dynamics

Goran Frehse (Université Joseph Fourier – Verimag, FR, goran.frehse@imag.fr)

Symbolic simulation, also referred to as reachability analysis, can complement trajectory-based analysis techniques to ensure a dynamic system satisfies a safety property. Instead of computing a sequence of points on a single trajectory, we compute a sequence of sets that covers all possible trajectories of the system. Computing with sets allows us to use conservative over-approximations and take into account various kinds of nondeterminism in the plant and the controller. While computing with sets is inherently costly and has long been restricted to toy problems, recent advances based on implicit ("lazy") set representations have made symbolic simulation applicable to linear ODEs with hundreds of variables. In this talk, we present a semi-template data structure, consisting of a set of piecewise linear scalar functions, that is used to approximate the nonconvex reachable set over time. It represents a (usually large) set of convex polyhedra in space-time in a compact manner. A number of operations, such as affine transformations, convex hull, and simplification, can be carried out very efficiently in this representation, and the resulting approximation error can be measured accurately. This has lead to gains in both accuracy and performance, and opens up new domains of application for symbolic simulation. The approach has been implemented on the verification platform SpaceEx developed at Verimag.

3.10 Compositionality Results for Cardiac Cell Dynamics

Radu Grosu (Vienna University of Technology, Wien, AT, radu.grosu@tuwien.ac.at)

Joint work of Islam, Ariful; Murthy, Abhishek; Girard, Antoine; Smolka, Scott A.; Grosu, Radu
Main reference A. Islam, A. Murthy, A. Girard, S. A. Smolka, R. Grosu, "Compositionality results for cardiac cell dynamics," in Proc. of the 17th Int'l Conf. on Hybrid Systems: Computation and Control, pp. 243–252, ACM, 2014.
URL http://dx.doi.org/10.1145/2562059.2562138

By appealing to the small-gain theorem of one of the authors (Girard), we show that the 13-variable sodium-channel component of the IMW cardiac-cell model (Iyer-Mazhari-Winslow) can be replaced by an approximately bisimilar, 2-variable HH-type (Hodgkin-Huxley) abstraction. We show that this substitution of (approximately) equals for equals is safe in the sense that the approximation error between sodium-channel models does not get amplified by the feedback-loop context in which it is placed. To prove this feedback-compositionality result, we exhibit quadratic-polynomial, exponentially decaying bisimulation functions between the IMW and HH-type sodium channels, and also for the IMW-based context in which these sodium-channel models are placed. These functions allow us to quantify the overall error introduced by the sodium-channel abstraction and subsequent substitution in the IMW model. To automate the computation of the bisimulation functions, we employ the SoS-Tools optimization toolbox. Our experimental results validate our analytical findings. To the best of our knowledge, this is the first application of approximately bisimilar, feedback-assisting, compositional reasoning in biological systems.

3.11 Two Approaches to Applying Verification to Control Design

Bruce Krogh (Carnegie Mellon University, Pittsburgh, US, krogh@ece.cmu.edu)

The standard application of verification tools to control design is to design the controller and then verify properties of the closed-loop system. We are investigating an alternative approach in which verification is used first to establish the safety of a nondeterministic controller. This becomes an envelope which can then be used either as a constraint in a control design process, or it can be used to verify a designed controller. One advantage of this second approach is that the envelope is a condition on only the input- output behavior of the controller rather than a condition on the closed-loop behavior.

3.12 Finite-time Lyapunov functions

Mircea Lazar (Eindhoven University of Technology, Eindhoven, NL, m.lazar@tue.nl)

Lyapunov functions are essential tools for verifying stability of real-life systems, such as modern cars or power systems. However, choosing a Lyapunov function candidate and then verifying if such a function exists is a very complex process. In this work we study a

relaxation of the Lyapunov function concept, termed finite-time Lyapunov function and we demonstrate that it can lead to scalable stability analysis tests for linear and switched linear systems (with state dependent switching). The analysis is carried out in the discrete-time setting. Examples from power systems will be used to demonstrate the applicability of the developed stability tests. A preliminary approach to the verification of stability for general nonlinear discrete-time systems based on finite-time Lyapunov functions is also presented.

3.13 On Optimal and Reasonable Control in the Presencve of Adversaries

Oded Maler (VERIMAG, Gieres FR, oded.maler.imag.fr)

This work constitutes a sketch of a unified framework for posing and solving problems of optimal control in the presence of uncontrolled disturbances. After laying down the general framework we look closely at a concrete instance where the controller is a scheduler and the disturbances are related to uncertainties in task durations.

3.14 Scalable Techniques for Viability Kernels and Safe Control Synthesis in Linear Time Invariant Systems

Ian Mitchell (University of British Columbia, Vancouver, CA, mitchell@cs.ubc.ca)

We present a connection between the viability kernel and maximal reachable sets. Current numerical schemes that compute the viability kernel suffer from a complexity that is exponential in the dimension of the state space. In contrast, extremely efficient and scalable techniques are available that compute maximal reachable sets. We show that under certain conditions these techniques can be used to conservatively approximate the viability kernel for possibly high-dimensional systems. We demonstrate three implementations using different set representations, and several examples. One of these set representations can be used to generate a nondeterministic hybrid control automaton which synthesizes a permissive but safe feedback control signal.

3.15 Verification of Nonlinear Models with Modular Annotations

Sayan Mitra (University of Illinois at Urbana-Champaign, US, mitras@illinois.edu)

In this talk I will give a overview of techniques for obtaining bounded time invariant proofs from simulations and model annotations. We use annotations called discrepancy functions that quantify the continuity of trajectories starting from neighboring states. Then, I will present a modular technique for simulation-based bounded verification for nonlinear dynamical systems.

We introduce the notion of input-to-state discrepancy of each subsystem A_i in a larger nonlinear dynamical system A which bounds the distance between two (possibly diverging) trajectories of A_i in terms of their initial states and inputs. Using the IS discrepancy functions, we construct a low dimensional deterministic dynamical system $M(\delta)$. For any two trajectories of A starting δ distance apart, we show that one of them bloated by a factor determined by the trajectory of M contains the other. Further, by choosing appropriately small δ's the over-approximations computed by the above method can be made arbitrarily precise. Using the above results we develop a sound and relatively complete algorithm for bounded safety verification of nonlinear ODEs with modular annotations. Our preliminary experiments with a prototype implementation of the algorithm show that the approach can be effective for verification of large nonlinear models.

3.16 Challenges in Verification of Hybrid Systems for Aerospace Applications

Richard M. Murray (California Institute of Technology, US, murray@cds.caltech.edu)

Flight critical subsystems in aerospace vehicles must achieve probability of failure rates of less than 1 failure in 10^9 flight hours (i.e. less than 1 failure per 100,000 years of operation). Systems that achieve this level of reliability are hard to design, hard to verify, and hard to validate, especially if software is involved. In this talk I describe some of the challenges in design of vehicle management systems for aerospace applications and some of the opportunities for the use of formal methods for verification and synthesis.

3.17 Logic of Hybrid Games

André Platzer (Carnegie Mellon University, Pittsburgh, US, aplatzer@cs.cmu.edu)

Hybrid systems model cyber-physical systems as dynamical systems with interacting discrete transitions and continuous evolutions along differential equations. They arise frequently in many application domains, including aviation, automotive, railway, and robotics. This talk studies hybrid games, i.e. games on hybrid systems combining discrete and continuous dynamics. Unlike hybrid systems, hybrid games allow choices in the system dynamics to be resolved adversarially by different players with different objectives.

This talk describes how logic and formal verification can be lifted to hybrid games. The talk describes a logic for hybrid systems called differential game logic dGL. The logic dGL can be used to study the existence of winning strategies for hybrid games, i.e. ways of resolving the player's choices in some way so that he wins by achieving his objective for all choices of the opponent. Hybrid games are determined, i.e. one player has a winning strategy from each state, yet their winning regions may require transfinite closure ordinals. The logic dGL, nevertheless, has a sound and complete axiomatization relative to any expressive logic. Separating axioms are identified that distinguish hybrid games from hybrid systems. Finally, dGL is proved to be strictly more expressive than the corresponding logic of hybrid systems.

3.18 Algorithmic Verification of Stability of Hybrid Systems

Pavithra Prabhakar (IMDEA Software Institute, ES, pavithra.prabhakar@imdea.org)

We focus on the verification of stability of hybrid systems. Stability is a fundamental property in control system design and captures the notion that small perturbations to the initial state or input to the system result in only small variations in the eventual behavior of the system. We present foundations and concrete techniques for abstraction based stability analysis. In contrast to the well-known methods for automated verification of stability based on Lyapunov functions, which are deductive, we present algorithmic techniques for stability analysis.

3.19 Highlights on Recent Progresses in Quantitative Games

Jean-François Raskin (Université Libre de Bruxelles, BE, jraskin@ulb.ac.be)

In this talk, I have summarized the results obtained in the three following papers:

- **The Complexity of Multi-Mean-Payoff and Multi-Energy Games.** In mean-payoff games, the objective of the protagonist is to ensure that the limit average of an infinite sequence of numeric weights is nonnegative. In energy games, the objective is to ensure that the running sum of weights is always nonnegative. Multi-mean-payoff and multi-energy games replace individual weights by tuples, and the limit average (resp. running sum) of each coordinate must be (resp. remain) nonnegative. These games have applications in the synthesis of resource-bounded processes with multiple resources. We prove the finite-memory determinacy of multi-energy games and show the inter-reducibility of multimean-payoff and multi-energy games for finite-memory strategies. We also improve the computational complexity for solving both classes of games with finite-memory strategies: while the previously best known upper bound was EXPSPACE, and no lower bound was known, we give an optimal coNP-complete bound. For memoryless strategies, we show that the problem of deciding the existence of a winning strategy for the protagonist is NP-complete. Finally we present the first solution of multi-meanpayoff games with infinite- memory strategies. We show that multi-mean-payoff games with mean-payoff- sup objectives can be decided in NP and coNP, whereas multi-mean-payoff games with mean-payoff-inf objectives are coNP-complete.
- **Meet Your Expectations With Guarantees: Beyond Worst-Case Synthesis in Quantitative Games.** We extend the quantitative synthesis framework by going beyond the worst-case. On the one hand, classical analysis of two-player games involves an adversary (modeling the environment of the system) which is purely antagonistic and asks for strict guarantees. On the other hand, stochastic models like Markov decision processes represent situations where the system is faced to a purely randomized environment: the aim is then to optimize the expected payoff, with no guarantee on individual outcomes. We introduce the beyond worst-case synthesis problem, which is to construct strategies that guarantee some quantitative requirement in the worst-case while providing an higher expected value against a particular stochastic model of the environment given as input. This problem is relevant to produce system controllers that provide nice expected performance in the

everyday situation while ensuring a strict (but relaxed) performance threshold even in the event of very bad (while unlikely) circumstances. We study the beyond worst-case synthesis problem for two important quantitative settings: the mean-payoff and the shortest path. In both cases, we show how to decide the existence of finite-memory strategies satisfying the problem and how to synthesize one if one exists. We establish algorithms and we study complexity bounds and memory requirements.

- **Looking at Mean-Payoff and Total-Payoff through Windows.** We consider two-player games played on weighted directed graphs with mean- payoff and total-payoff objectives, two classical quantitative objectives. While for single-dimensional games the complexity and memory bounds for both objectives coincide, we show that in contrast to multi-dimensional mean-payoff games that are known to be coNP-complete, multi-dimensional total-payoff games are undecidable. We introduce conservative approximations of these objectives, where the payoff is considered over a local finite window sliding along a play, instead of the whole play. For single dimension, we show that (i) if the window size is polynomial, deciding the winner takes polynomial time, and (ii) the existence of a bounded window can be decided in NP ∩ coNP, and is at least as hard as solving mean-payoff games. For multiple dimensions, we show that (i) the problem with fixed window size is EXPTIME-complete, and (ii) there is no primitive-recursive algorithm to decide the existence of a bounded window.

3.20 Analysis and Synthesis of CPS using EF-SMT

Harald Ruess (fortiss GmbH – München, DE, harald.ruess@gmail.com)

The design of cyber-physical systems is challenging in that it includes the analysis and synthesis of distributed and embedded real-time systems for controlling, often in a nonlinear way, the environment. We address this challenge with EFSMT, the exists-forall quantified first-order fragment of propositional combinations over constraints (including nonlinear arithmetic), as the logical framework and foundation for analyzing and synthesizing cyber-physical systems. We demonstrate the expressiveness of EFSMT by reducing a number of pivotal verification and synthesis problems to EFSMT. Exemplary problems include synthesis for robust control via BIBO stability, Lyapunov coefficient finding for nonlinear control systems, distributed priority synthesis for orchestrating system components, and synthesis for hybrid control systems. We are also proposing an algorithm for solving EFSMT problems based on the interplay between two SMT solvers for respectively solving universally and existentially quantified problems. This algorithms builds on commonly used techniques in modern SMT solvers, and generalizes them to quantifier reasoning by counterexample-guided constraint strengthening. The EFSMT solver uses Bernstein polynomials for solving nonlinear arithmetic constraints.

3.21 Compositional Synthesis of Multi-Robot Motion Plans via SMT Solving

Indranil Saha (University of California – Berkeley, US, saha.indra@gmail.com)

We present a constraint based compositional motion planning framework for multi-robot systems. In this framework, the runtime behavior of a group of robots is specified using a set of safe LTL properties. Our method relies on a library of motion primitives that provides a set of controllers to be used to control the behavior of the robots in different configurations. Using the closed loop behavior of the robots under the action of different controllers, we formulate the motion planning problem as a constraint solving problem and use an off-the-shelf satisfiability modulo theories (SMT) solver to solve the constraints and generate trajectories for the individual robot. Our approach can also be extended to synthesize optimal cost trajectories where optimality is defined with respect to the available motion primitives. Experimental results show that our framework has potential to solve complex motion planning problems in the context of multi-robot systems.

3.22 Simulation-Based Techniques for the Falsification of Cyber-Physical Systems

Sriram Sankaranarayanan (University of Colorado Boulder, US, srirams@colorado.edu)

The tutorial will describe some of the major ideas on the use of simulations to automate the discovery of property violations in CPS designs. As model-based design is increasingly prevalent, frameworks such as Simulink(tm)/Stateflow(tm), SCADE(tm) and Modelica(tm) are becoming de-facto standards for designing and verifying CPS. Simulation, therefore, is an attractive approach for finding defects in designs including violations of reachability and stability specifications. Our review will highlight some of the major simulation approaches including ideas from robotic motion planning (e.g. Rapid Exploration of Random Trees, Probabilistic Roadmaps), optimization/optimal control (e.g., robustness-guided falsification, trajectory optimization, multiple shooting methods), and the relation with well-known symbolic approaches used in formal verification (e.g., bounded-model checking, abstraction-refinement). We will briefly describe some of the successes of these techniques and open problems including "simulation explosion" and the need for formal underpinnings for these techniques. We will conclude by describing some attempts at solving these open problems.

3.23 Certified-by-design control of systems over finite alphabets

Danielle Tarraf (Johns Hopkins University, US, dtarraf@jhu.edu)

In this talk, I propose a theoretical and algorithmic framework for synthesizing certified-by-design control systems using simple components with limited information processing and memory capabilities. Specifically, I consider a setup in which plants interact with their controllers via fixed discrete alphabets, and in which controller memory is finite. I describe a set of analysis tools for systems over finite alphabets and a set of synthesis tools for finite state models. A common theme is the use of input-output constraints to describe system properties of interest. I then propose a control-oriented notion of finite state approximation compatible with these analysis and synthesis tools, I present constructive algorithms for generating these approximations, and I demonstrate their use in simple examples. Finally, I discuss some aspects of state estimation under finite alphabet and memory constraints.

3.24 EF-SMT

Ashish Tiwari (SRI International – Menlo Park, US, tiwari@csl.sri.com)

Many problems in verification and synthesis of cyber-physical systems can be reduced to deciding formulas of the form exists-forall-F, where F is a quantifier-free formula in some combination of theories. Satisfiability modulo theory (SMT) solvers decide satisfiability of formulas of the form exists-F, whereas Exists-Forall-SMT (EF-SMT) solvers decide formulas of the form exists-forall-F.

We show how a generic EF-SMT solver can be built over an SMT solver, much in the same way as an SMT solver is built over a Boolean SAT solver. We also briefly describe a new procedure for solving EF and E problems over a fragment of the theory of nonlinear real arithmetic. The new procedure can be viewed as a generalized SAT solver.

3.25 Stability of Linear Autonomous Systems Under Regular Switching Sequences

Mahesh Viswanathan (University of Illinois at Urbana-Champaign, US, vmahesh@illinois.edu)

A linear autonomous system under regular switching sequences is constructed by viewing the dynamic modes of a linear autonomous switched system as the alphabet of a Muller Automaton with accepting conditions on transitions instead of states and restricting the switching sequences of dynamic modes by the language generated by the automaton. The asymptotic stability of this system, defined as regular asymptotic stability, generalizes two well-known definitions of stability of linear autonomous switching system namely absolute asymptotic stability and shuffle asymptotic stability. We also extend the definitions of

stability to their robust versions. We prove that absolute asymptotic stability, robust absolute asymptotic stability robust shuffle asymptotic stability are equivalent to uniform exponential stability. In addition, by using Kronecker product, we convert a regular stability problem into the conjunction of shuffle asymptotic stability problems and prove that a robust regular stability problem is equivalent to the conjunction of several robust absolute asymptotic stability problems or uniformly exponential stability problems.

Participants

- Erika Ábrahám
RWTH Aachen, DE
- Calin A. Belta
Boston University, US
- Sergiy Bogomolov
Universität Freiburg, DE
- Ken Butts
Toyota Research Center – Ann Arbor, US
- Xin Chen
RWTH Aachen, DE
- Deepak D'Souza
Indian Institute of Science, IN
- Thao Dang
VERIMAG – Gières, FR
- Jyotirmoy Deshmukh
Toyota Technical Center – Gardena, US
- Georgios Fainekos
ASU – Tempe, US
- Goran Frehse
VERIMAG – Gières, FR
- Sebastian Gerwinn
Universität Oldenburg, DE
- Radu Grosu
TU Wien, AT
- Bruce H. Krogh
Carnegie Mellon University, US
- Mircea Lazar
TU Eindhoven, NL
- Rupak Majumdar
MPI-SWS – Kaiserslautern, DE
- Oded Maler
VERIMAG – Gières, FR
- Ian M. Mitchell
University of British Columbia – Vancouver, CA
- Sayan Mitra
University of Illinois – Urbana Champaign, US
- Richard M. Murray
CalTech, US
- André Platzer
Carnegie Mellon University, US
- Pavithra Prabhakar
IMDEA Software Institute – Madrid, ES
- Jean-François Raskin
Université Libre de Bruxelles, BE
- Harald Ruess
fortiss GmbH – München, DE
- Indranil Saha
University of California – Berkeley, US
- Sriram Sankaranarayanan
Univ. of Colorado – Boulder, US
- Konstantin Selyunin
TU Wien, AT
- Danielle Tarraf
The Johns Hopkins Univ., US
- Ashish Tiwari
SRI – Menlo Park, US
- Mahesh Viswanathan
Univ. of Illinois – Urbana, US