Symbolic-Numeric Methods for Reliable and Trustworthy Problem Solving in Cyber-Physical Domains

Edited by
Sergiy Bogomolov[1], Martin Fränzle[2], Kyoko Makino[3], and Nacim Ramdani[4]

1 **Australian National University – Canberra, AU,** sergiy.bogomolov@anu.edu.au
2 **Universität Oldenburg, DE,** martin.fraenzle@informatik.uni-oldenburg.de
3 **Michigan State University – East Lansing, US,** makino@msu.edu
4 **University of Orléans, FR,** nacim.ramdani@univ-orleans.fr

Abstract

Reflecting the fundamental role numeric and mixed symbolic-numeric arguments play in the analysis, decision making, and control of cyber-physical processes, this seminar promoted cross-fertilization between the following research areas relevant to problem solving in cyber-physical domains: verification of numerical reactive systems such as embedded floating-point programs and hybrid systems, including novel means of error-propagation analysis; numerical and/or symbolic methods such as verified integrations, interval methods and arithmetic constraint solving; reactive and in-advance planning and optimization methods in complexly constrained spaces, robotics, astrodynamics and more. This combination of up to now only loosely coupled areas shed light on how advanced numerical methods can help improve the state of the art in rigorously interpreting and controlling cyber-physical phenomena. It naturally included the broad set of domain-specific solutions to the pertinent issues of performance impact of error propagation and control in various schemes of numeric and blended symbolic-numeric computation.

Seminar December 4–9, 2016 – http://www.dagstuhl.de/16491
1998 ACM Subject Classification D.2.4 Software/Program Verification, F.4.1 Mathematical Logic, G.1.7 Ordinary Differential Equations
Keywords and phrases constraint solving, cyber-physical systems, formal methods, hybrid systems, optimization methods, planning, robotics, verified numerical methods
Digital Object Identifier 10.4230/DagRep.6.12.1

1 Executive Summary

Sergiy Bogomolov
Martin Fränzle
Kyoko Makino
Nacim Ramdani

With the advent of cyber-physical systems increasingly penetrating our life, we are facing an ever-growing and permanent dependency on their reliable availability, continued function, and situationally adequate behavior even in highly sensitive application domains. As cyber-physical systems comprise complex, heteromorphic software systems, their reliability engineering calls for combinations of theories and methods traditionally considered separate. While we have recently seen some of the necessary combinations blossom, e.g. the theory of

Symbolic-Numeric Methods for Reliable and Trustworthy Problem Solving in Cyber-Physical Domains,
Dagstuhl Reports, Vol. 6, Issue 12, pp. 1–28
Editors: Sergiy Bogomolov, Martin Fränzle, Kyoko Makino, and Nacim Ramdani
DAGSTUHL REPORTS Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

hybrid systems bridging continuous control with reactive systems, other areas remain less developed and explored. A prominent one is the role of numerics in cyber-physical systems: while it is obvious that cyber-physical systems increasingly rely on numerical software components, e.g., in signal processing or in state representation and extrapolation during situation assessment and planning, specific methods for addressing the issues associated, like consequences of numerical inaccuracy and methods for confining propagation of errors, are just in their infancy. This is in stark contrast to the use of numerics in more mature branches of computing, like signal processing or numerical analysis, where quantization effects as well as genesis and propagation of numerical error is well-understood and dedicated methods for controlling it in critical application, like various forms of interval-based numerical algorithms, are readily available. The aforementioned "traditional" methods are, however, not versatile enough to cope with the cyber-physical setting, where numerical results, like state extrapolations over significant temporal horizons, enter into complex and safety-critical decision making, rendering error propagation potentially highly discontinuous. It seems that future critical applications, like automated driving contributing to the EU's "Vision Zero" of eliminating fatalities in road-bound traffic, consequently call for novel means of analyzing and controlling the impact of numerics on system correctness, complemented by pertinent means of verification for establishing the safety case. The germs of such methods obviously have to be sought in the fields of design and verification of cyber-physical systems, i.e. in particular, (1) hybrid discrete-continuous systems, as well as (2) verified numerics, arithmetic constraint solving also involving symbolic reasoning, and (3) planning and rigorous optimization in arithmetic domains. The seminar gathered prominent researchers from all these fields in order to address the pressing problems induced by our societal dependence on cyber-physical systems.

As argued above, bringing together researchers dealing with hybrid discrete-continuous systems, with verified numerics in arithmetic constraint solving, and with planning and optimization in arithmetic domains can help improve the state of the art in rigorously interpreting and controlling cyber-physical phenomena. In the sequel, we review existing and potential contributions of the three fields to problem solving in cyber-physical domains and sketch potentials for cross-fertilization, which was the aim of the proposed seminar.

2 Table of Contents

Executive Summary

Introduction

Overview of Talks

3 Introduction

Design and verification of hybrid and cyber-physical systems

The verification of software systems interacting with a continuous environment and manipulating state information in order to draw discrete decisions about control actions, like in supervisory control, or about task selection, like in layered architectures for autonomous technical systems, poses special challenges. Such systems are traditionally called hybrid systems and their correctness problem, which calls for reconciling the views of discrete and continuous mathematics, has gained considerable scientific interests over the past three decades, as witnessed by a series of dedicated international conferences, e.g. Hybrid Systems Computation Control (HSCC) and Analysis and Design of Hybrid Systems (ADHS) as well as continuous high impact on top conferences in the field of automatic verification, e.g. Computer Aided Verification (CAV) and Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), and control, e.g. Conference on Decision and Control (CDC) and European Control Conference (ECC). Hybrid systems are typically characterized by large discrete and continuous state spaces. This fact often makes their analysis computationally intractable. Verification therefore strongly relies on combinations of symbolic representation methods with numerical and optimization algorithms. For example, flowpipe-based reachability algorithms for hybrid systems use verified numerical integration routines in order to compute the image of a given polytope at a particular time moment. At the same time, polytopes can be efficiently represented and manipulated using support functions, which in turn strongly rely on linear optimization techniques. Other methods taken from the treasures of numerical methods are interval analysis, including Taylor model methods, various set-based computation techniques representing a variety of geometric shapes, automatic linearization of non-linear operations, to name just a few. The control of numerical error, however, remains inconsistent: while many approaches widely ignore the possibility and pursue best-effort numerics, some try to at least rigorously control its effect within the analysis algorithms (i.e., they try monitor error development and propagation e.g. in the calculations underlying reach-set computation), but none currently seems to rigorously address the dichotomy between real-world states and their real-time entities as well as the consequences these may induce for system correctness.

Constraint solving and verified numerics

A large class of decision problems can be encoded as constraints over some theory. In the last decade, the scientific community has paid a lot of attention to handling of various arithmetic theories ranging from boolean- to real-valued ones. For example, reachability problem for dynamic systems exhibiting large state space presents a very promising application domain for constraint solving. In this setting, a reachability problem is cast as a satisfiability problem so that satisfiable valuations returned by a constraint solving engine correspond to the initial states which lead to the safety property violation. Clearly, the efficiency of the resulting analysis schema strongly relies on the performance of the underlying constraint solver, which makes the development of scalable high-performance constraint solving engines imperative. The analysis of hybrid systems with dynamics in form of differential equations poses a special challenge for constraint solving techniques due to the interleaving of discrete and continuous artifacts and presence of dense time as part of the reachability problem. Usually, this interdependency is resolved by relying on the verified integration engine which computes an over-approximation of the system states reachable along the trajectory using error bounds on numerical errors during the integration. In the next step, this constraint is embedded into the constraint solving engine workflow which operates on it in a black-box fashion. This exemplifies a tight interconnection of constraint solving and verified integration.

In the following, we discuss in more details ideas behind verified numerical methods. One way to increase the confidence in numerical calculations is to use high precision numbers, and another is to use set-arithmetic methods with mathematical rigor instead of point evaluations, often called verified computational methods. The interval arithmetic method is widely known, where all operations are carried out on floating-point intervals instead of floating-point numbers, accounting floating-point inaccuracies by outward rounding. By evaluating a function in a set-arithmetic method, rigorous bounds of the sets are evaluated through the operations to obtain rigorous bounds in the end. Like many other problems, a task of verified ODE integration can be viewed as an evaluation of a series of operations in set-arithmetic methods. However, a mere usage of the interval method suffers from overestimation, and particularly severely in ODE integrations due to the wrapping effect, which has led to numerous inventive methods to overcome. For example, the Taylor model method retains both Taylor polynomials and the remainder error bounds in the arithmetic, describing a highly nonlinear system with tightly bounded errors. The method also includes differentiation and integration as the arithmetic operations, which is advantageous to solving differential equations.

Planning and optimization methods

Planners look for sequence of actions that steers a system from the initial state into the target one, given the description of the initial state, the target state, and the set of possible actions. A number of efficient algorithms to solve convex optimization problems exist. To the contrary, when planning involves cyber-physical systems with mixed discrete-continuous dynamics, and search over mixed continuous-discrete domains featuring tightly interdependent constraints, both the objective function and search domain typically do not exhibit any convexity properties which leads to a much harder computational problem. In this setting, planning methods can greatly benefit from powerful techniques developed in the verification community, such as symbolic reachability, for instance, and conversely, verification tools can also benefit from advanced planning approaches. There have been some initial efforts to bridge the two problems and work on the exchanges between the two areas. Indeed, a verification problem can be cast as a planning problem (as in the directed model checking setting, for instance), where the target set is a state violating a property to be verified in the original verification problem. Then, if the planner finds a plan, the latter is the error trace the verification method would have returned. Verification tools can also be endowed with a planning scheme that guides the search towards finding a state violating a property, by optimizing a suitable cost function. In this setting, guided search can improve the performance of the verification tools built upon counterexample search for property falsification. Conversely, the connection between verification and planning can be exploited the other way around. A planning problem can be cast as a verification problem, where the latter is stopped when the target state is found. Naturally, planners may benefit from verification methods, as the latter can speed up the search by pruning large subsets of the search domains where it can prove the absence of solution. By the way, this interplay between planning and verification is currently investigated in the robotics planning community, which aims to endow today sophisticated robots with reactive capabilities. For instance, provably correct high-level reactive behaviors can be designed by combining symbolic abstraction based computation of reachable sets, sampling-based strategy and libraries of verified local motion controllers.

Breakout sessions

The participants selected three breakout sessions and met twice to discuss the following issues.

Symbolic vs. Numeric

The panel worked on a clarification of the often controversial terms "symbolic method" and "numeric method", based on the observation that such methods often blend together in practical verification tools, leading to situations where the very same algorithm is called "symbolic" by one scientific community and "numeric" by the other. It was found that the ambiguity stems from adopting partial perspectives reflecting either just the choice between points vs. set representations or the nature of the operations thereupon, respectively. As all combinations seem to exist, it would make sense to distinguish between representations in operations when classifying algorithms as symbolic or numeric. The group consequently focused on achieving a classification of frequently used modelling representations, the computations involved, and their exact or approximate expected outcomes, for large classes of operations related to the analysis of cyber-physical systems.

Requirements and Industrial challenges

The panel discussed the problem of the meager availability of meaningful and sizable case studies and benchmarks and along with it the perceived industrial relevance of research on automatic analysis techniques for CPS. As the scientific process would require comprehensible and scalable case studies rather than hardly documented off-the-shelf industrial systems and code bases, a major issue was the identification of the key complexities in industrial system validation and verification challenges, compared to the actual capabilities of current analysis tools. The latter issue includes a plethora of quality and performance indicators, among others to which extent the tools are user-friendly, their particular trade-off between precision and computational speed, and the balance between influence given to users vs. skills and technological insight expected from them. It was found that safety issues of robots engaging into physical contact with humans might provide a source for extremely meaningful, societally relevant and thus potentially visible, and computationally hard benchmarks.

Differential equations and Inequalities

The panel discussed ways to handle differential equations with partial functions, and the issue of differential equations over manifolds in general. One way to address the issue of partial functions is to restrict evaluations to the definition domain of the functions, by using backward constraint propagation and constraint solving techniques to prune-off inconsistent domains. To address the issue of differential equations over manifolds, one may revert to solution projection. They also discussed the issue of tight evaluation of the solution sets for differential equations, and for which class of systems one should use comparison theorems for differential inequalities instead of interval methods for reachability computation. Tighter evaluation may be achieved by an optimal choice of the computation step size that should preserve the contractance property of the system. Finally, the panel concluded that precise evaluation of event detection is still challenging. There are good solutions with non-linear hybrid systems, but there is room for improvements with the main issue being the interplay between event detection and reset function. The use of affine arithmetics as set representation seems a step in the good direction.

4 Overview of Talks

4.1 HyPro: A C++ Library for State Set Representations for Hybrid Systems Reachability Analysis

Erika Ábrahám (RWTH Aachen, DE)

Joint work of Erika Ábrahám, Ibtissem Ben Makhlouf, Stefan Kowalewski, Stefan Schupp
Main reference S. Schupp, E. Abraham, I. Ben Makhlouf and S. Kowalewski, "HyPro: A C++ library for state set representations for hybrid systems reachability analysis", to appear in the Proc. of the 9th NASA Formal Methods Symposium (NFM 2017).

During the last two decades, the rising interest in hybrid systems satefy verification resulted in powerful tools implementing different approaches. Flowpipe-construction-based reachability analysis is one prominent approach, which over-approximates the set of reachable states of a hybrid system by a union of state sets, each of them being represented by a geometric object of a certain shape (like boxes, polyhedra, or zonotopes) or symbolically (like support functions or Taylor models). There is a variety of representations in use, each of them having its individual strengths and weaknesses.

The implementation of novel reachability analysis algorithms that use such state set representations is still effortful, as datatypes for all needed representations need to be implemented first. To support the fast implementation of new approaches, in this paper we introduce HyPro, our C++ library offering implementations for the most prominent state set representations. Our library provides a unified interface for different representations, which supports all operations required in reachability analysis as well as conversion methods between the different representations. Thus HyPro assists the rapid implementation of new algorithms by encapsulating all representation-related issues and allowing the developers to focus on other algorithmical aspects.

4.2 DynIbex: A Tool for the Formal Verification of Robotic Behaviors in Presence of Bounded Uncertainties

Julien Alexandre dit Sandretto (ENSTA – Palaiseau, FR) and Alexandre Chapoutot (ENSTA – Palaiseau, FR)

Robotic behaviors are mainly described by differential equations. Those mathematical models are usually not precise enough because of inaccurately known parameters or model simplifications. Nevertheless, robots are often used in critical contexts as medical or military fields. So, uncertainties in mathematical models have to be taken into account in order to produce reliable and safe analysis results. A framework based on interval analysis is proposed to safely verify and analyze robotic behaviors with bounded uncertainties. It follows an interval constraint programming approach, combined with validated numerical integration methods to deal with differential equations and temporal constraints. Some applications for robust control are presented and solved with DynIbex, a tool which implements the presented framework.

4.3 Modelling and Verifying Recursive Workflow Models using Attribute Grammars

Roman Barták (Charles University – Prague, CZ)

Main reference R. Barták, "Using Attribute Grammars to Model Nested Workflows with Extra Constraints", in Proc. of the Int'l Conf. on Current Trends in Theory and Practice of Informatics (SOFSEM 2016), LNCS, Vol. 9587, pp. 171–182, Springer, 2016.
URL http://dx.doi.org/10.1007/978-3-662-49192-8_14
Main reference R. Barták, T. Dvořák, "On Verification of Workflow and Planning Domain Models using Attribute Grammars", Presentation at the 15th Mexican Int'l Conf. on Artificial Intelligence (MICAI 2016).

Workflow is a formal description of a process. Nested workflows were proposed to model processes with a hierarchical structure and they support extra logical and temporal constraints to express relations beyond the hierarchical structure. This workflow model supports scheduling applications with a known number of activities in the process, but it cannot be used to model planning problems, where the number of activities is unknown beforehand.

We propose to model nested workflows using a modified version of attribute grammars. In particular, we show that nested workflows with extra constraints can be fully translated to attribute grammars. The major advantage of this novel modeling framework is a support for recursive tasks that can model planning problems in the style of hierarchical task networks. Hence attribute grammars may serve as a unifying framework to describe workflow and planning domains models.

One of the critical aspects of the domain model is its soundness, that is, the model should not contain any dead-ends and should describe at least one plan. We describe how the domain model can be verified by using the concept of reduction of attribute grammars. Two verification methods are suggested, one based on transformation to context-free grammars and one direct method exploiting constraint satisfaction.

4.4 Taylor Model based Verified Integrators for Large Domains

Martin Berz (Michigan State University – East Lansing, US)

The Taylor model approach allows to rigorously propagate ranges of initial conditions with an error that scales as a high power of the diameter of the initial conditions. Starting from the Picard operation based method of integrating ODEs via Taylor models for one time step, we discuss several advanced Taylor model techniques including the pre-conditioning method, the Lie derivative based method applied to the defect equations, and the error parametrization technique. This allows long-term propagations of large ranges of domains and parameter ranges, and further by virtue of automatic domain decomposition tools. Using these methods, it is often possible to propagate very large domains in an economical manner.

We show various applications of the method, including proofs of chaoticity of the Henon map, as well as applications for the commonly used method of discretizing the motion into a finite but large graph and studying global dynamics based on that representation for the Duffing equations and the well-known Lorenz equations.

4.5 Scalable Static Hybridization Methods for Analysis of Nonlinear Systems

Sergiy Bogomolov (Australian National University – Canberra, AU)

Joint work of Stanley Bak, Sergiy Bogomolov, Thomas A. Henzinger, Taylor T. Johnson, Pradyot Prakash
Main reference S. Bak, S. Bogomolov, T. A. Henzinger, T. T. Johnson, P. Prakash, "Scalable static hybridization methods for analysis of nonlinear systems", in Proc. of the 19th Int'l Conf. on Hybrid Systems: Computation and Control (HSCC 2016), pp. 155–164, ACM, 2016.
URL http://dx.doi.org/10.1145/2883817.2883837

Hybridization methods enable the analysis of hybrid automata with complex, nonlinear dynamics through a sound abstraction process. Complex dynamics are converted to simpler ones with added noise, and then analysis is done using a reachability method for the simpler dynamics. Several such recent approaches advocate that only "dynamic" hybridization techniques – i.e., those where the dynamics are abstracted on-the-fly during a reachability computation – are effective. In this talk, we demonstrate this is not the case, and create static hybridization methods that are more scalable than earlier approaches.

The main insight in our approach is that quick, numeric simulations can be used to guide the process, eliminating the need for an exponential number of hybridization domains. Transitions between domains are generally time-triggered, avoiding accumulated error from geometric intersections. We enhance our static technique by combining time-triggered transitions with occasional space-triggered transitions, and demonstrate the benefits of the combined approach in what we call mixed-triggered hybridization. Finally, error modes are inserted to confirm that the reachable states stay within the hybridized regions.

The developed techniques can scale to higher dimensions than previous static approaches, while enabling the parallelization of the main performance bottleneck for many dynamic hybridization approaches: the nonlinear optimization required for sound dynamics abstraction. We implement our method as a model transformation pass in the HYST tool, and perform reachability analysis and evaluation using an unmodified version of SpaceEx on nonlinear models with up to six dimensions.

4.6 Bit-Exact Automated Reasoning About Floating-Point Arithmetic

Martin Brain (University of Oxford, GB)

The majority of new instrumentation and control systems, even those that are safety critical, make use of floating-point numbers. Thus the value of computer-generated assurance evidence (including verification, test coverage, etc.) depends on the correctness, completeness and efficiency of automated reasoning about floating-point expressions. In this talk we will review the SMT-LIB Theory of Floating-Point, its semantics and the rationale behind key design decisions as well as surveying the current state-of-the-art in solver technology and future research directions. We aim to provide system integrators with sufficient information to integrate floating-point support into SMT interfaces and solver developer enough ideas to work on the next generation of floating-point reasoning.

4.7 Industrial Cyber-Physical System Examples and Challenges

Mauricio Castillo-Effen (General Electric – Niskayuna, US)

Examples of cyber-physical systems from the General Electric company are introduced. The first example is the "Digital Twin" – a set of multi-domain/multi-aspect hierarchical models of individual physical assets used to predict and make decisions. According to this vision, all industrial assets such as aircraft engines, power generation plants, locomotives, etc. possess a "Digital Twin", fed permanently with data collected via diverse types of sensors. Important decisions are made at multiple time scales with the support of tools and analytics that update and make use of the "Digital Twin". Hence, algorithms and code implementing them need to exhibit appropriate levels of assurance and validity.

The second example is presented as a "grand challenge" that exposes research needs in the context of high assurance autonomous systems. Specifically, a team of aerial robots is used to perform inspection, maintenance, and repair tasks in safety-rated industrial environments such as oil refineries and off-shore platforms. A high level approach to tackling the problem of achieving trustworthiness is presented, which consists of decomposing the work it into four areas: formal synthesis, verification and validation, test and evaluation, and run-time assurance. Synthesis techniques need to operate in a compositional fashion generating not only individual robot behaviors, but also provably correct dynamic role allocation and coordinated action from specifications that may still require formalization. Because of the distributed nature of the system, the need for compositionality also applies to offline and online verification. Finally, test and evaluation (T&E) is presented as an important area of opportunity for the CPS community to provide significant value to industry in the short term. T&E strategy and system-level test-case generation tools are needed to accelerate the fielding of trustworthy autonomous systems and machines in the real world.

In summary, advances in validated symbolic-numeric methods help accelerate the deployment of industrial cyber physical systems unleashing all their benefits. Challenges and research needs are known at a high level. Collaboration between industrial and academic research communities could now focus on developing relevant and specific benchmark problems that present levels of fidelity and granularity commensurate to real-life applications while avoiding exposure of proprietary information.

4.8 Making Runge-Kutta Methods Validated

Alexandre Chapoutot (ENSTA – Palaiseau, FR)

Joint work of Alexandre Chapoutot, Julien Alexandre dit Sandretto, Olivier Mullier

Validated numerical integration is an appealing approach to produce rigorous results on Initial Value Problem of Ordinary Differential Equations (ODE). An IVP-ODE is defined by

$$\begin{cases}\dot{\mathbf{y}} = f(t, \mathbf{y}) \\ \mathbf{y}(0) \in \mathcal{Y}_0 \subseteq \mathcal{R}^n,\ t \in [0, t_{\text{end}}]\end{cases} . \tag{1}$$

The set $\mathcal{Y}_0$ of initial conditions is used to model some (bounded) uncertainties. For a given initial condition $\mathbf{y}_0$, the solution when it exists is denoted $\mathbf{y}(t;\mathbf{y}_0)$. The goal of validated (or rigorous) numerical integration methods is to compute the set of solution, or an over-approximation, of the solutions of (1), *i.e.*, $\{\mathbf{y}(t;\mathbf{y}_0) : \forall \mathbf{y}_0 \in \mathcal{Y}_0, \forall t \in [0, t_{\text{end}}]\}$.

Most of the rigorous techniques defined so far, since Ramon Moore's seminal work [2], are based on Taylor series approach, see for example [3, 7, 10, 13] and the references therein. Nervertheless, it is unlikely that only one kind of methods is adapted to all various classes of ODE. So, more recent work [4, 6, 5, 9, 11] deals with the adaptation of Runge-Kutta methods to be validated methods in order to try to benefit the good properties such as A-stability. A generic s-step Runge Kutta method for IVP-ODE is defined by

$$\mathbf{y}_{n+1} = \mathbf{y}_n + h \sum_{i=1}^{s} b_i \mathbf{k}_i \tag{2}$$

with

$$\mathbf{k}_i = f(t_n + c_i h, \mathbf{y}_n + \sum_{j=1}^{s} a_{ij} \mathbf{k}_j), \quad i = 1, \dots, s \ . \tag{3}$$

The real coefficients c_i, $a_{i,j}$ and b_i fully characterize a Runge-Kutta methods, see [8].

The challenge to make a Runge-Kutta validated is to bound the *local truncation error* (LTE), *i.e.*, the distance between the true solution $\mathbf{y}(t_n;\mathbf{y}_{n-1})$ at time t_n with $\mathbf{y}_{n-1}$ as intial conditions and the numerical solution $\mathbf{y}_n$ starting from the same initial condition so to bound $\mathbf{y}(t_n;\mathbf{y}_{n-1}) - \mathbf{y}_n$.

Following the *order condition*, see [1], a Runge-Kutta method is of order p if the p first terms of the Taylor form associated to the numerical solution $\mathbf{y}_n$ are equal to the terms of the exact solution of (1) that is $\mathbf{y}(t;\mathbf{y}_{n-1})$ assuming the same initial condition. In this case the LTE corresponds to the difference of the two Taylor remainders. Now, the challenge is to compute these Taylor remainders.

In this talk, we present a novel approach to bound the LTE based on the order condition which is usable for explicit and implicit Runge-Kutta methods. More precisely, our approach is an instance of the algorithm defined in [12] and applied in the context of validated numerical integration methods based on Runge-Kutta methods.

References

1 J. C. Butcher. Coefficients for the study of Runge-Kutta integration processes. *Journal of the Australian Mathematical Society*, 3:185–201, 1963.

2 R. E. Moore. *Interval Analysis.* Series in Automatic Computation. Prentice Hall, 1966.

3 N. S. Nedialkov, K. R. Jackson, and G. F. Corliss. Validated solutions of initial value problems for ordinary differential equations. *Applied Mathematics and Computation*, 105(1):21–68, 1999.

4 K. Gajda, A. Marciniak, and B. Szyszka. Three- and four-stage implicit interval methods of Runge-Kutta type. *Computational Methods in Science and Technology*, 6(1):41–59, 2000.

5 A. Marciniak. Implicit interval methods for solving the initial value problem. *Numerical Algorithms*, 37(1-4):241–251, 2004.

6 A. Marciniak and B. Szyszka. On representations of coefficients in implicit interval methods of runge-kutta type. *Computational Methods in Science and Technology*, 10(1):57–71, 2004.

7 K. Makino and M. Berz. COSY INFINITY version 9. *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, 558(1):346–350, 2006.

8 E. Hairer, C. Lubich, and G. Wanner. *Geometric numerical integration: structure-preserving algorithms for ordinary differential equations.* Computational Mathematics. Springer, 2006.

9 O. Bouissou and M. Martel. GRKLib: a Guaranteed Runge-Kutta Library. In *International Symposium on Scientific Computing, Computer Arithmetic and Validated Numerics*. IEEE, 2006.

10 Y. Lin and M. A. Stadtherr. Validated solutions of initial value problems for parametric ODEs. *Applied Numerical Mathematics*, 57(10):1145–1162, 2007.

11 O. Bouissou, A. Chapoutot, and A. Djoudi. Enclosing temporal evolution of dynamical systems using numerical methods. In *NASA Formal Methods*, number 7871 in LNCS, pages 108–123. Springer, 2013.

12 F. A. Bartha and H. Z. Munthe-Kaas. Computing of b-series by automatic differentiation. *Discrete and Continuous Dynamical Systems*, 34(3):903–914, 2014.

13 T. Dzetkulič. Rigorous integration of non-linear ordinary differential equations in chebyshev basis. *Numerical Algorithms*, 69(1):183–205, 2015.

4.9 Decomposed Reachability Analysis for Nonlinear Systems

Xin Chen (University of Colorado – Boulder, US)

Joint work of Xin Chen, Sriram Sankaranarayanan
Main reference X. Chen, S. Sankaranarayanan, "Decomposed Reachability Analysis for Nonlinear Systems", in Proc. of the Real-Time Systems Symposium (RTSS 2016), pp. 13–24, IEEE, 2016.
URL http://dx.doi.org/10.1109/RTSS.2016.011

The reachability analysis on the systems whose dynamics are defined by large-scale nonlinear Ordinary Differential Equations (ODEs) is notoriously difficult in general. In this talk, we introduce a method that conservatively abstracts a nonlinear continuous system by a hybrid automaton whose continuous dynamics are given by a decomposition of the original dynamics, such that the reachability analysis on the abstracted model is much easier than that on the original one.

The main idea is to decompose the original high-dimensional ODE into a set of lower-dimensional ODEs with time-varying uncertainties whose ranges are updated in a hybridization framework. More precisely, the uncertainties are the decomposed variables in the ODE, their evolutions are only updated in each time step by the hybridization domain. Also, the computed reachable set overapproximation and hybridization domain in each step can be mutually refined. In order to reduce the heavy overestimation accumulation, we also present a technique to partially keep a Taylor model remainder symbolically.

We implemented a prototype tool based on the computational library in Flow*, and evaluate the performance on a set of challenging benchmarks whose dimensions range from 7 to 30. It can be seen that our approach has an apparent advantage over the existing tools in handling large-scale systems.

4.10 Daisy – A Framework for Accuracy Analysis of Numerical Programs

Eva Darulova (MPI-SWS – Saarbrücken, DE)

The analysis of roundoff errors of finite-precision computations has produced several tools in previous years, but we found it difficult to extend them beyond their original purpose, either because they were commercial or simply not very extension-friendly. For the past year, my group has been developing a new framework – called Daisy – for the analysis of numerical programs whose aim is to be modular, and easily extensible. In my talk, I will report on the current and up-coming features of Daisy, and at the same time review our past work on finite-precision static analysis as well as some of our new projects.

4.11 Frugal Dynamic Analysis of Linear Dynamical Systems

Parasara Sridhar Duggirala (University of Connecticut – Storrs, US)

In this talk, I will focus on simulation based verification technique for CPS where the continuous behavior is specified by a linear differential equations, a class well studied in the domain of control theory. Specifically, I will present a technique that will require very few simulations, namely, our technique will require a mere n+1 simulations to verify the correctness of an n-dimensional linear system.

4.12 Formal Specification Debugging for Monitoring and Testing of Cyber-Physical Systems

Georgios Fainekos (Arizona State University – Tempe, US)

Joint work of Adel Dokhanchi, Georgios Fainekos, Bardh Hoxha
Main reference A. Dokhanchi, B. Hoxha, G. Fainekos, "Formal Requirement Debugging for Testing and Verification of Cyber-Physical Systems", arXiv:1607.02549v2 [cs.SY], 2016.
URL https://arxiv.org/abs/1607.02549v2

A framework for the debugging of formal specifications for Cyber-Physical Systems is presented. Two debugging algorithms are presented for specifications expressed in Signal Temporal Logic. The first checks for erroneous or incomplete temporal logic specifications without considering the system. The problem reduces to a number of satisfiability checks of bounded Metric Temporal Logic requirements. The second can be utilized for the analysis of reactive requirements with respect to system test traces. In this case, the solution depends on syntactic analysis of the temporal logic formulas and optimization based falsification methods. The specification debugging framework is applied to a number of formal specifications collected through a user study. The user study establishes that requirement errors are common and that the debugging framework can resolve many insidious specification errors and improve the falsification process.

4.13 Counterexample-guided Refinement of Template Polyhedra

Mirco Giacobbe (IST Austria – Klosterneuburg, AT)

Joint work of Sergiy Bogomolov, Goran Frehse, Mirco Giacobbe, Thomas A. Henzinger
Main reference S. Bogomolov, G. Frehse, M. Giacobbe, T. A. Henzinger, "Counterexample-guided Refinement of Template Polyhedra", to appear in the Proc. of the 23rd Int'l Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2017).

Template polyhedra generalize intervals and octagons to polyhedra whose facets are orthogonal to a given set of arbitrary directions. They offer a very powerful framework for the reachability analysis of hybrid automata, as an appropriate choice of directions allows an effective tuning between accuracy and precision. In this talk, I will present a method for the automatic discovery of directions that generalize and eliminate spurious counterexamples, task which was previously left to the user or a heuristic. I will show that for the class of convex hybrid automata, i.e. hybrid automata with (possibly non-linear) convex constraints on derivatives, such directions can be found using convex optimization. Finally, I will show our experimental results on several bechmarks, demonstrating an effective time-unbounded reachability analysis for a richer class of hybrid automata than was previously possible, and superior performance for the special case of linear hybrid automata.

4.14 Dependable Control of Modular Robots

Michael W. Hofbaur (Joanneum Research – Klagenfurt/Wörthersee, AT), Arthur Angerer, and Mathias Brandstötter

Modular robots are versatile mechanisms that allow one to design a serial manipulator according to a given task or application. Their structure, however, differs from the standard ortho-parallel robot structure and it is therefore non-trivial to control such a mechanism. The core functionality of a robot controller deals with computing the inverse kinematics that translates a given pose of the robot in its appropriate joint-angle configuration. To obtain a dependable operation of the robot, it is therefore essential to have a computational procedure that provides the IK result reliably within the robots workspace at hand. The non-standard topology of a modular robot requires numeric or semi-algebraic solutions for the IK. The latter approach utilizes symbolic methods that take advantage of the problem's geometric structure and employs numeric methods to solve a remaining nonlinear problem. We utilize the algorithm of Husty and Pfurner [1] for this purpose. In its core, the algorithm solves a polynomial of order 56 in order to obtain up to 16 real valued solutions for the IK problem. The talk analyses the characteristic properties of this algorithm by presenting a detailed state-space analysis for the IK problem of modular robots [2, 3, 4]. In this way, it highlights the value of using combined symbolic-numeric methods for solving a demanding engineering problem.

References

1 M. Husty, M. Pfurner, H.-P. Schroecker. *A new and efficient algorithm for the inverse kinematics of a general serial 6R manipulator*. Mechanism and Machine Theory, 42(1):66–81, Jan. 2007

2 M. Brandstoetter. *Adaptable Serial Manipulators in Modular Design*. PhD thesis, UMIT, Nov. 2016

3 A. Angerer, M. Hofbaur. *Industrial Versatility of Inverse Kinematics Algorithms for General 6R Manipulators*. IEEE International Conference on Advanced Robotics (ICAR 2013), Uruguay, November 25-28, 2013

4 M. Brandstoetter. *Collection of General Serial 6R Manipulators with 16 Real Solutions for the Inverse Kinematics Problem*. Data Collection DOI: `10.13140/RG.2.2.13496.75524`, http://www.researchgate.net, November 2016

4.15 The Method of Taylor Models and the Applications

Kyoko Makino (Michigan State University – East Lansing, US)

The method of Taylor models provides rigorous enclosures of functions over given domains, where the bulk of the dependency is represented by a high order multivariate Taylor polynomial, and the remaining error is enclosed by a remainder bound. In this talk, we will discuss how to construct Taylor model arithmetic on computers, which naturally includes integrations as a part of arithmetic. Computations using Taylor models provide rigorous results, and advantageous features of the method have shown to be able to solve various practical problems that were unsolvable earlier. The applications start from mere range bounding of functions, leading to sophisticated rigorous global optimization, and especially fruitful is the use for rigorous solvers of differential equations.

4.16 Combining Symbolic Analysis and Simulation in Uppaal Stratego

Marius Mikucionis (Aalborg University, DK)

Joint work of Alexandre David, Peter G. Jensen, Kim G. Larsen, Marius Mikucionis, Jacob H. Taankvist
Main reference A. David, P. G. Jensen, K. G. Larsen, M. Mikučionis, J. H. Taankvist, "Uppaal stratego", in Proc. of the 21st Int'l Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2015), LNCS, Vol. 9035, pp. 206–211, Springer, 2015.
URL http://dx.doi.org/10.1007/978-3-662-46681-0_16

Uppaal Stratego[1] is an integrated toolset combining model checking and controller synthesis of timed game automata, statistical model checking and machine learning for stochastic hybrid systems [1]. In this talk I would like to outline the basic building blocks and techniques behind the toolset, how they cohere with each while supporting various workflows, and then discuss parts which could be improved. I hope that this platform could serve as basis for "requirements" and/or application framework to test various techniques on real-world examples. In particular:

- ODE integration. Uppaal allows arbitrary ODEs in the context of simulations, however the race protocol undermines precise and efficient integration. The race protocol requires that processes make their delay decisions locally, but the dynamical bounds (unlike clock

[1] http://people.cs.aau.dk/~marius/stratego

bounds) are too complex to predict at once thus we resolve to fixed time steps. These time steps are usually set to small values to provide more stable integration, but small time steps force unnecessary re-evaluation of many other expressions (guards and invariants) even though little-to-nothing has changed. Alternatively, we could pre-compute longer trajectories and compute precise delay bounds, but then we would throw most of the trajectory away if preempted by another process (which is the case most of the time because the winner is always just one among many).

- Arithmetics on "reals" (including user code, integration and stochastic behavior generation). Currently only floating point "double" precision is supported, and no error propagation is done. The operations are compiled into byte-code and executed in a virtual machine, but no optimizations are done. Virtual machine is faster than any other AST evaluation, but it is still about 100x slower than native code, thus expensive. Dependency analysis could allow caching values to avoid re-evaluation as much as possible. Some applications may require fixed point arithmetic to ensure the same density of numbers at various scales in order to guarantee better uniform distributions. Other applications may require astronomical precision (like Avogadro number).
- Stochastic differential equations (e.g. Brownian motion, economy models). Simple Euler integration algorithm requires only one lookup thus in principle it is possible to combine stochastic delays with stochastic dynamics. The better integration algorithms (like Runge-Kutta) require multiple lookups at different points in time, therefore a specialized algorithm is needed.
- Different algorithms with various settings yield slightly different behavior.
- Statistical engine allows new possibilities for machine learning techniques to resolve controllable choices for controller synthesis.

A number of case studies (SBML models in particular) yield many floating point and integer expressions to be evaluated and integrated on-the-fly, which could be used as a test bed for various methods.

References

1 A. David, P. G. Jensen, K. Guldstrand Larsen, M. Mikučionis, and J. H. Taankvist. Uppaal stratego. In Christel Baier and Cesare Tinelli, editors, *Tools and Algorithms for the Construction and Analysis of Systems*, volume 9035 of *Lecture Notes in Computer Science*, pages 206–211. Springer Berlin Heidelberg, 2015.

4.17 Structural Analysis and Numerical Solution of High-Index Differential-Algebraic Equations

Ned Nedialkov (McMaster University – Hamilton, CA) and John D. Pryce (Cardiff University, GB)

Joint work of Ned Nedialkov, John Pryce, Gary Tan

Systems of differential-algebraic equations (DAEs) arise in many engineering and scientific disciplines. The index of a DAE is a measure of how difficult it is to solve it, compared to an ordinary differential equation (ODE). Problems of index 3 and higher are considered high index, and are very difficult to solve numerically.

We overview Pryce's structural analysis (SA) theory and its realization in the DAETS solver (Nedialkov and Pryce), a C++ package for solving high-index DAEs. This solver can deal with fully implicit, any index, and aribrary-order DAEs.

We also present DAESA (Nedialkov, Pryce, and Tan), a standalone Matlab tool for SA of DAEs. It provides convenient facilities for rapid investigation of DAE structures. In particular it reveals subsystems of a DAE to a finer resolution than many other methods.

4.18 Introduction to Interval and Taylor Model Methods

Markus Neher (KIT – Karlsruher Institut für Technologie, DE)

Verified methods are techniques that compute rigorous bounds for some specific solution of a given problem. When these methods are implemented in computer programs, mathematical validity is maintained by including the effects of all roundoff errors in the computation.

Interval arithmetic has been developed by Ramon Moore in the late 1950s. In his pioneering book on interval analysis in 1966, Moore employed interval arithmetic for the verified solution of diverse problems, including ranges of functions, linear systems, the determination of zeros and the solution of initial value problems.

Unfortunately, interval methods sometimes suffer from overestimation. This is caused by the dependency problem, that is the lack of interval arithmetic to identify different occurrences of the same variable, and by the wrapping effect, which occurs when intermediate results of a calculation are enclosed into intervals.

To reduce overestimation, Taylor models have been developed as a combination of symbolic and interval computations by Martin Berz and his group since the 1990s. A Taylor model consists of a multivariate polynomial and some remainder interval. In computations, the polynomial part is propagated by symbolic calculations, which are neither affected by the dependency problem nor the wrapping effect. Only the interval remainder term and polynomial terms of high order, which are usually small, are bounded using interval arithmetic.

In our talk, we first present fundamentals of interval arithmetic and Taylor model arithmetic. Then we compare interval methods and Taylor model methods for initial value problems.

4.19 Automatic Verification of Linear Controller Software

Junkil Park (University of Pennsylvania – Philadelphia, US)

Joint work of Insup Lee, Miroslav Pajic, Junkil Park, Oleg Sokolsky
Main reference J. Park, M. Pajic, I. Lee, O. Sokolsky, "Scalable verification of linear controller software", in Proc. of the 22nd Int'l Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2016), LNCS, Vol. 9636, pp. 662–679, Springer, 2016.
URL http://dx.doi.org/10.1007/978-3-662-49674-9_43

We consider the problem of verifying software implementations of linear time-invariant controllers against mathematical specifications. Given a controller specification, multiple correct implementations may exist, each of which uses a different representation of controller state (e.g., due to optimizations in a third-party code generator). To accommodate this variation, we first extract a controller's mathematical model from the implementation via symbolic execution, and then check input-output equivalence between the extracted model and the specification by similarity checking. We show how to automatically verify the correctness of C code controller implementation using the combination of techniques such as symbolic execution, satisfiability solving and convex optimization. Through evaluation using randomly generated controller specifications of realistic size, we demonstrate that the scalability of this approach has significantly improved compared to our own earlier work based on the invariant checking method.

4.20 Bounded Error Approximation based Verification of Parameterized Linear Systems

Pavithra Prabhakar (Kansas State University – Manhattan, US)

Joint work of Ratan Lal, Pavithra Prabhakar
Main reference R. Lal, P. Prabhakar, "Bounded Error Flowpipe Computation of Parameterized Linear Systems", in Proc. of the 12th Int'l Conf. on Embedded Software (EMSOFT'15), pp. 237–246, IEEE, 2015.
URL http://dx.doi.org/10.1109/EMSOFT.2015.7318279

We consider the problem of bounded safety verification of a class of hybrid systems in which the dynamics is specified as parameterized linear systems. We present a method to construct piecewise linear approximations of the solutions of the dynamics that have a guaranteed bound on the deviation from the exact solution of the system. We encode the executions of the system that evolve for a bounded amount of time and bounded number of switches as an SMT formula with linear arithmetic using these approximations. Thus, we reduce the bounded safety analysis to satisfiability checking of SMT formulae. Our experimental results and case studies involving air-traffic collision avoidance protocols demonstrate the scalability of our approach.

4.21 Differential-Algebraic Equations, Structural Analysis Examples, and Dummy Derivatives

John D. Pryce (Cardiff University, GB) and Ned Nedialkov (McMaster University – Hamilton, CA)

Joint work of Ross McKenzie, Ned Nedialkov, John D. Pryce, Guangning (Gary) Tan

Typically, a cyber-physical system – during the time-interval between two events – is described by a differential algebraic equation system (DAE). Following on Ned Nedialkov's introduction to *structural analysis*- (SA-)based numerical methods for numerically solving DAEs, I give tutorial examples of the use of SA on simple problems. As an example of the serious use of SA, I outline the *dummy derivatives* method, widely used to prepare a DAE for numerical solution by converting it to an equivalent ODE.

Finally I briefly describe the MANDAE project that Ned and I are part of, which is bidding to run an EU Innovative Training Network (ITN). The research aim is to create a new software infrastructure for modelling languages such as Modelica that represent a model mathematically as a DAE system. Hybrid systems, such as cyber-physical systems, feature prominently in our proposed work plan.

References

1 S. E. Mattsson and G. Söderlind, 1993. Index reduction in differential-algebraic equations using dummy derivatives. *SIAM J. Sci. Comput. 14,* 3, 677–692.

2 N. S. Nedialkov and J. D. Pryce, 2008. Solving differential-algebraic equations by Taylor series (III): The DAETS code. *JNAIAM 3,* 1–2, 61–80. ISSN 1790–8140.

3 C. C. Pantelides, 1988. The consistent initialization of differential-algebraic systems. *SIAM. J. Sci. Stat. Comput. 9*, 213–231.

4 J. D. Pryce, 2001. A simple structural analysis method for DAEs. *BIT 41,* 2, 364–394.

4.22 Validated Hybrid Reachability Computation

Nacim Ramdani (University of Orléans, FR)

Joint work of Christophe Combastel, Moussa Maïga, Nacim Ramdani, Louise Travé-Massuyès
Main reference M. Maïga, N. Ramdani, L. Travé-Massuyès, C. Combastel, "A Comprehensive Method for Reachability Analysis of Uncertain Nonlinear Hybrid Systems", in IEEE Transactions on Automatic Control, 61(9):2341–2356, IEEE, 2016.
URL http://dx.doi.org/10.1109/TAC.2015.2491740

Reachability computation with cyber-physical systems modelled as nonlinear uncertain hybrid automata, i.e., continuous-discrete dynamical systems whose continuous dynamics, guard sets and reset functions are defined by nonlinear functions, may rely on three algorithmic steps: (1) computing the reachable set when the system is in a given continuous operation mode, (2) computing the discrete transitions, i.e., detecting and localizing when (and where) the trajectory tube intersects the guard sets, and (3) aggregating the multiple trajectories that result from an uncertain transition once the whole tube has transitioned so that the algorithm can resume.

In the first part of the talk, I review validated approaches for the continuous reachability problem, the ones based on comparison theorems for differential inequalities [1] or the theory of order preserving monotone dynamical systems [2]. In the second part of the talk, I describe a comprehensive method that provides a nicely integrated solution to the hybrid reachability problem. It combines approaches used to control the over-approximation in Taylor's method for IVP ODE, and solution techniques for solving constraint satisfaction problems underlying discrete transitions ; both approaches using the same set representation [3].

References

1 Nacim Ramdani, Nacim Meslem, Yves Candau. *A Hybrid Bounding Method for Computing an Over-Approximation for the Reachable Set of Uncertain Nonlinear Systems.* IEEE Trans. Automat. Contr. 54(10): 2352–2364 (2009).

2 Nacim Ramdani, Nacim Meslem, Yves Candau. *Computing reachable sets for uncertain nonlinear monotone systems.* Nonlinear Analysis : Hybrid Systems. 4(2): 263–278 (2010).

3 Moussa Maïga, Nacim Ramdani, Louise Travé-Massuyès, Christophe Combastel. *A Comprehensive Method for Reachability Analysis of Uncertain Nonlinear Hybrid Systems.* IEEE Trans. Automat. Contr. 61(9): 2341–2356 (2016).

4.23 Problem Solving in Cyber-Physical Domains: A Unifying Perspective

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

The term "cyber-physical" combines traditions of science and engineering that have, to a large extent, developed separately. This has resulted in a cultural gap that is not always easy to overcome. In the talk, I will a provide short and non-comprehensive attempt at providing a unifying perspective on some problems that have traditionally been studied independently for the computational and the physical world.

4.24 Parallel Reachability Analysis of Hybrid Systems in XSpeed.

Rajarshi Ray (NIT – Meghalaya, IN)

Joint work of Ezio Bartocci, Sergiy Bogomolov, Arup Deka, Radu Grosu, Amit Gurung, Rajarshi Ray
Main reference A. Gurung, A. Deka, E. Bartocci, S. Bogomolov, R. Grosu, R. Ray, "Parallel reachability analysis for hybrid systems", in Proc. of the 2016 ACM/IEEE Int'l Conf. on Formal Methods and Models for System Design (MEMOCODE 2016), pp. 12–22, IEEE, 2016.
URL http://dx.doi.org/10.1109/MEMCOD.2016.7797741

We discuss two parallel state-space exploration algorithms for hybrid systems with the goal of enhancing performance on multi-core shared memory systems. The first is an adaption of the parallel breadth first search in the SPIN model checker. We see that the adapted algorithm does not provide the desired load balancing for many hybrid systems benchmarks. The second is a task parallel algorithm based on cheaply pre-computing cost of post (continuous and discrete) operations for an effective load balancing. We illustrate the task parallel algorithm and the cost pre-computation of post operators on a support-function-based algorithm for state-space exploration. The performance comparison of the two algorithms displays a better CPU utilization/load-balancing of the second over the first, except for certain cases. The algorithms are implemented in the model checker XSpeed and our experiments show a significant speed-up on benchmarks with respect to SpaceEx LGG scenario.

4.25 Hybrid Petri Nets: Evaluation Algorithms and Applications

Anne Remke (Universität Münster, DE)

Critical infrastructures are (remotely) controlled by ICT networks and subject to cyber and physical failures that pose a serious threat to their dependability and survivability. It is important to be able to quantify the impact of failures on the physical process and to be able to analyse how quickly such systems recover to acceptable levels of service after the occurrence of failures, e.g., leakages or component breakdowns.

The so-called survivability expresses how quickly systems recover to acceptable levels of service, using so called Given the Occurrence Of Disaster (GOOD) models. We use Stochastic timed logic (STL) to rigorously define the notion of survivability and evaluate STL formulas using model checking techniques e.g. on Hybrid Petri nets.

This modeling formalism of Hybrid Petri nets incorporates continuous and discrete elements as well as stochastic variables to describe the occurrence of random events, and their fluid dynamics. New efficient techniques are needed to evaluate the evolution of the system over time. Both, symbolic and numeric techniques are currently investigated in order to tackle systems with a large number of stochastic events.

4.26 Over and Under Approximations of Reachable Sets Within Hamilton-Jacobi Framework

Zhikun She (Beijing University of Aeronautics & Astronautics, CN)

Joint work of Meilun L., Zhikun She

For dynamical systems, reachable sets can be described by the solutions of Hamilton-Jacobi equations. In this paper, we discuss a methodology to compute approximations, defined by zero sub-level sets of polynomials, of time-bounded reachable sets (i.e., flowpipes) with arbitrary bounded errors for polynomial dynamical systems via solving derived Hamilton-Jacobi equations with inequality constraints. We start with evolution functions for describing the flowpipes of systems, and then prove the existence of polynomial approximations to the evolution functions with arbitrary bounded errors by investigating these approximations as the solutions of the corresponding partial differential equations with derived inequality constraints, which shows the applicability of this methodology to obtain both over and under approximations of reachable sets. Afterwards, we propose two methods to compute template polynomial evolution functions with constraints, based on sum-of-squares decomposition and quantifier elimination respectively. We test these two methods on some examples. The computation results show that the QE based method to certain extent has a better performance than the SOS based method. Especially, the QE based method has a clear advantage since it works for certain non-polynomial dynamical systems.

4.27 Rigorous Simulation

Walid Taha (Halmstad University, SE)

Joint work of Aaron Ames, Pererik Andreasson, Kevin Atkinson, Ferenc Bartha, Paul Brauner, Robert Cartwright, Alexandre Chapoutot, Adam Duracz, Jan Duracz, Jun Inoue, Michal Konecný, Jawad Masood, Eugenio Moggi, Roland Philippsen, Anita Sant'Anna, Walid Taha, Fei Xu, Yingfu Zheng
Main reference W. Taha, A. Duracz, Y. Zeng, K. Atkinson, F. A. Bartha, P. Brauner, J. Duracz, F. Xu, R. Cartwright, M. Konečný, E. Moggi, J. Masood, P. Andreasson, J. Inoue, A. Sant'Anna, R. Philippsen, A. Chapoutot, M. O'Malley, A. Ames, V. Gaspes, L. Hvatum, S. Mehta, H. Eriksson, C. Grante, "Acumen: An Open-Source Testbed for Cyber-Physical Systems Research", in Proc. of the 2nd Int'l Summit on Internet of Things. IoT Infrastructures, LNICST, Vol. 169, pp. 118–130, Springer, 2015.
URL http://dx.doi.org/10.1007/978-3-319-47063-4_11

The falling price of computational and communication components means that they will increasingly be embedded into physical products. Verifying the designs of the resulting "cyber-physical" products is challenging for several reasons. First, closed-form solutions for the behavior of physical systems rarely exist. Second, the most natural mathematical tool for modeling cyber-physical combinations, namely, hybrid (discrete/continuous) systems, exhibit pathologies that arise in neither purely continuous nor purely discrete systems. Third, the expressivity of existing continuous dynamics formalisms is generally lower than those used by domain experts.

To address these problems, we are developing a technology called "rigorous simulation". The back-end for rigorous simulation uses validated numerics algorithms, which compute guaranteed bounds for the precision of all solutions. We show that these algorithms can be extended to compute trajectories for some hybrid systems exhibiting Zeno behavior. Ongoing work suggests that chattering behavior can be similarly addressed. We make validated numerics more accessible to non-specialists through the use of a domain-specific language, based on hybrid ordinary differential equations, which we also extend to support partial derivatives and certain types of equational modeling. An implementation called "Acumen" has been built and used for several case studies. These include virtual testing of advanced driver assistance functions, bipedal robotics, and a range of model problems for teaching at both graduate and undergraduate levels.

4.28 Path Planning Using Intervals: Application to Autonomous Parking

Yuichi Tazaki (Kobe University, JP)

Joint work of Hiroyuki Okuda, Tatsuya Suzuki, Yuichi Tazaki
Main reference H. Fuji, J. Xiang, Y. Tazaki, B. Levedahl, T. Suzuki, "Trajectory planning for automated parking using multi-resolution state roadmap considering non-holonomic constraints", in Proc. of the 2014 IEEE Intelligent Vehicles Symposium 2014, pp. 407–413, IEEE, 2014.
URL http://dx.doi.org/10.1109/IVS.2014.6856433

This talk presents a trajectory planning method for automated parking that makes use of graph-based digital maps. The proposed digital map contains information of parking spot layout, obstacle configuration, and a set of geometric features called guidelines. In addition, it contains feasible transitions between guidelines that define safe trajectories satisfying the non-holonomic constraint of the vehicle, curvature limit, and collision-avoidance between the vehicle and the boundary of the parking environment. A digital map of a parking environment is constructed off-line by dividing the guidelines in multiple resolutions until enough coverage over the set of feasible transitions is achieved. Using this digital map, a complex parking trajectory composed of both forward and reverse motions can be computed with small online computation cost. The proposed method is evaluated in both numerical simulations and real experiments.

4.29 BTC EmbeddedPlatform – Tool Demo

Tino Teige (BTC-ES AG – Oldenburg, DE)

In this presentation I roughly demonstrate BTC EmbeddedPlatform, an automatic test and verification tool for embedded systems. The focus of the demonstration is on use cases where verification technologies are applied, e.g. automatic test case generation and verification of requirements. The presentation concludes with some challenges for ongoing and future work.

4.30 Set-membership Identifiability and its Application to Fault Detection and Identification

Louise Travé-Massuyès (LAAS – Toulouse, FR)

Joint work of Carine Jauberthie, Louise Travé-Massuyès, Nathalie Verdiére
Main reference C. Jauberthie, N. Verdière, L. Travé-Massuyès, "Fault detection and identification relying on set-membership identifiability", Annual Reviews in Control, 37(1):129–136, Elsevier, 2013.
URL http://dx.doi.org/10.1016/j.arcontrol.2013.04.002

Identifiability is the property that a mathematical model must satisfy to guarantee an unambiguous mapping between its parameters and the output trajectories. It is of prime importance when parameters are to be estimated from experimental data representing input-output behavior and clearly when parameter estimation is used for fault detection and identification. Definitions of identifiability and methods for checking this property for linear and nonlinear systems are now well established and, interestingly, some recent works [1,2] have provided identifiability definitions for set-membership models in a bounded-error context, established links with classical identifiability definitions, and proposed numerical test methods. These works have been summarized in the first part of the talk, reminding the two complementary definitions of set-membership identifiability and μ-set-membership identifiability [1]. The first one is conceptual whereas the second one can be put in correspondence with existing set-membership parameters estimation methods. In the second part, one method for checking set-membership identifiability and μ-set-membership identifiability have been presented. This method is based on differential algebra and makes use of relations linking the input and output variables as well as the unknown parameters of the system. Building on these results, a method for fault detection via parameter estimation has been presented in the third part of the talk. The relations mentioned above are used to estimate the parameters of the model in a set-membership framework, through an analytic solution. The estimated value sets are then checked against the parameter nominal ranges. Advantageously, the identification of the fault(s) is a byproduct of this detection test. The method has been illustrated with an example describing the capacity of a macrophage mannose receptor to endocytose a specific soluble macromolecule.

4.31 Compositionality in the Science of System Design

Stavros Tripakis (University of California – Berkeley, US)

Main reference S. Tripakis, "Compositionality in the Science of System Design," Proceedings of the IEEE, 104(5):960–972, IEEE, 2016.
URL http://dx.doi.org/10.1109/JPROC.2015.2510366

In this talk we discuss systems, system design, and compositionality. We begin by proposing a generic definition of system and debate classic and modern system theories. Motivated by cyber-physical systems, most of which are safety-critical, we ask what is the best way to design such systems, and answer "model-based design". We then discuss work by the author and colleagues on model-based design, focusing on compositionality, and in particular on the refinement calculus of reactive systems.

References

1 I. Dragomir and V. Preoteasa and S. Tripakis. Compositional Semantics and Analysis of Hierarchical Block Diagrams. 23rd International SPIN Symposium on Model Checking of Software (SPIN 2016). LNCS 9641, pages 38–56, Springer, April, 2016.

2 I. Dragomir, V. Preoteasa, and S. Tripakis. Translating Hierarchical Block Diagrams into Composite Predicate Transformers. *CoRR*, abs/1510.04873, October 2015.

3 R. Lublinerman, C. Szegedy, and S. Tripakis. Modular Code Generation from Synchronous Block Diagrams – Modularity vs. Code Size. In *36th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'09)*, pages 78–89. ACM, January 2009.

4 R. Lublinerman and S. Tripakis. Modular Code Generation from Triggered and Timed Block Diagrams. In *14th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS'08)*, pages 147–158. IEEE CS Press, April 2008.

5 R. Lublinerman and S. Tripakis. Modularity vs. Reusability: Code Generation from Synchronous Block Diagrams. In *Design, Automation, and Test in Europe (DATE'08)*, pages 1504–1509. ACM, March 2008.

6 V. Preoteasa, I. Dragomir, and S. Tripakis. A Nondeterministic and Abstract Algorithm for Translating Hierarchical Block Diagrams. *CoRR*, abs/1611.01337, November 2016.

7 V. Preoteasa, I. Dragomir, and S. Tripakis. Type Inference of Simulink Hierarchical Block Diagrams in Isabelle. *CoRR*, abs/1612.05494, December 2016.

8 V. Preoteasa and S. Tripakis. Refinement Calculus of Reactive Systems. In *Proceedings of the 14th ACM & IEEE International Conference on Embedded Software (EMSOFT'14)*, 2014.

9 V. Preoteasa and S. Tripakis, Towards Compositional Feedback in Non-Deterministic and Non-Input-Receptive Systems. 31st Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), 2016.

10 J. Reineke and S. Tripakis. Basic Problems in Multi-View Modeling. In *Tools and Algorithms for the Construction and Analysis of Systems – TACAS 2014*, 2014.

11 S. Tripakis, Compositionality in the Science of System Design, Proceedings of the IEEE, 104(5), pages 960–972, May 2016.

12 Compositional Model-Based System Design and Other Foundations for Mastering Change. Transactions on Foundations for Mastering Change, pages 113–129, vol. 1, LNCS 9960, Springer, 2016.

13 S. Tripakis, "Foundations of Compositional Model-Based System Design," in *Cyber-Physical Systems: From Theory to Practice*, D. Rawat, J. Rodrigues, and I. Stojmenovic, Eds. CRC Press, 2015.

14 S. Tripakis, D. Bui, M. Geilen, B. Rodiers, and E. A. Lee. Compositionality in synchronous data flow: Modular code generation from hierarchical SDF graphs. *ACM Trans. Embed. Comput. Syst.*, 12(3):83:1–83:26, March 2013.

15 S. Tripakis, B. Lickly, T. A. Henzinger, and E. A. Lee. A Theory of Synchronous Relational Interfaces. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 33(4), July 2011.

4.32 Applications of Taylor Methods in Astrodynamics

Alexander Wittig (ESA/ESTEC – Noordwijk, NL), Roberto Armellin, Franco Bernelli Zazzera, Pierluigi Di Lizia, and Alessandro Morselli

Joint work of Roberto Armellin, Franco Bernelli Zazzera, Martin Berz, Pierluigi Di Lizia, Kyoko Makino, Alessandro Morselli, Alexander Wittig
Main reference R. Armellin, P. Di Lizia, F. Bernelli Zazzera, M. Berz, "Asteroid Close Encounters Characterization using Diffferential Algebra: the Case of Apophis", Celestial Mechanics and Dynamical Astronomy, 107(4):451–470, Springer, 2010.
URL http://dx.doi.org/10.1007/s10569-010-9283-5
Main reference A. Wittig, P. Di Lizia, R. Armellin, K. Makino, F. Bernelli Zazzera, M. Berz, "Propagation of large uncertainty sets in orbital dynamics by automatic domain splitting", Celestial Mechanics and Dynamical Astronomy, 122(3):239–261, Springer, 2015.
URL http://dx.doi.org/10.1007/s10569-015-9618-3

In this presentation we will illustrate several real world applications of verified computation techniques using Taylor Model methods in the field of Aerospace engineering and astrodynamics.

In particular, we will present the case of asteroid 99942 Apophis, which when first observed in December 2004 was considered at a 2.7% risk of colliding with Earth due to the uncertainty in the initial observations. While later more precise observations ruled out any risk of collision with Earth on its first close encounter on April 13 2029, it was not until August 2006 that a later collision with Earth on April 13 2036 could be ruled out with high probability.

This example, however, shows one of most relevant problems in astrodynamics: based on rather inaccurate initial observations scientists need to make predictions and computations of impact risks in the near to mid term future. The dynamics governing the evolution of such a body are very complex, ranging from simple Newtonian forces of the main bodies in the solar system to higher order terms due to relativistic effects as well as the Yarkovsky effect due to uneven heating of the asteroid surface by the sun. All these effects can only be taken into account in numerical propagation of the initial conditions.

At the same time, the dynamics are highly sensitive to initial conditions, especially during close encounters with other planets. All these effects together lead to the question of how accurate classical non-verified numerical techniques are in actually predicting the impact risk. We employ the validated Taylor Model Integrator COSY VI by Makino and Berz to propagate the entire initial uncertainty set for 23 years until the first close encounter. This allows us to show in a rigorous fashion that there is no impact risk at the first close encounter with Earth.

After the close encounter the dynamics prove to be too difficult to continue with a validated integrator, so we instead propagate up to the second close encounter using a non-validated integrator. In the process, we employ automatic domain splitting (ADS), which, while not validated, still provides valuable information on the dynamics in phase space and in the initial conditions. From the splitting pattern it is possible to deduce which regions of the initial condition experience the most non-linear behavior during the propagation. We show that this can be equated with different classes of potential resonant trajectories with resonant returns in 2035 and 2036.

Besides the application of Taylor Models for validated integration, we also show an application for the use of the global optimizer COSY GO for rigorous determination of the minimum orbit intersection distance (MOID). This distance is used to compute collision risks of artificial Earth satellites and to plan evasive actions if required. Using validated bounds on the distance adds an additional layer of protection around this sensitive operational procedure.

Participants

- Erika Ábrahám
RWTH Aachen, DE
- Julien Alexandre dit Sandretto
ENSTA – Palaiseau, FR
- Roman Barták
Charles University – Prague, CZ
- Sergiy Bogomolov
Australian National University – Canberra, AU
- Martin Brain
University of Oxford, GB
- Mauricio Castillo-Effen
General Electric – Niskayuna, US
- Alexandre Chapoutot
ENSTA – Palaiseau, FR
- Xin Chen
University of Colorado – Boulder, US
- Chih-Hong Cheng
fortiss GmbH – München, DE
- Eva Darulova
MPI-SWS – Saarbrücken, DE
- Parasara Sridhar Duggirala
University of Connecticut – Storrs, US
- Georgios Fainekos
Arizona State University – Tempe, US
- Martin Fränzle
Universität Oldenburg, DE
- Mirco Giacobbe
IST Austria – Klosterneuburg, AT
- Eric Goubault
Ecole Polytechnique – Palaiseau, FR
- Michael W. Hofbaur
Joanneum Research – Klagenfurt/Wörthersee, AT
- Kyoko Makino
Michigan State University – East Lansing, US
- Marius Mikucionis
Aalborg University, DK
- Ned Nedialkov
McMaster University – Hamilton, CA
- Markus Neher
KIT – Karlsruher Institut für Technologie, DE
- Junkil Park
University of Pennsylvania – Philadelphia, US
- Pavithra Prabhakar
Kansas State University – Manhattan, US
- John D. Pryce
Cardiff University, GB
- Sylvie Putot
Ecole Polytechnique – Palaiseau, FR
- Nacim Ramdani
University of Orléans, FR
- Stefan Ratschan
The Czech Academy of Sciences – Prague, CZ
- Rajarshi Ray
NIT – Meghalaya, IN
- Anne Remke
Universität Münster, DE
- Karsten Scheibler
Universität Freiburg, DE
- Zhikun She
Beijing University of Aeronautics & Astronautics, CN
- Walid Taha
Halmstad University, SE
- Yuichi Tazaki
Kobe University, JP
- Tino Teige
BTC-ES AG – Oldenburg, DE
- Louise Travé-Massuyès
LAAS – Toulouse, FR
- Stavros Tripakis
University of California – Berkeley, US
- Alexander Wittig
ESA / ESTEC – Noordwijk, NL