10271 Abstracts Collection
Verification over discrete-continuous boundaries generate automatically — Dagstuhl Seminar —

Bernd Becker[1], Luca Cardelli[2], Holger Hermanns[3] and Sofiene Tahar[4]

[1] Universität Freiburg, DE
becker@informatik.uni-freiburg.de
[2] Microsoft Research UK - Cambridge, GB
luca@microsoft.com
[3] Universität des Saarlandes, DE
hermanns@cs.uni-sb.de
[4] Concordia Univ. - Montreal, CA
tahar@ece.concordia.ca

Abstract. From 4 July 2010 to 9 July 2010, the Dagstuhl Seminar 10271 "Verification over discrete-continuous boundaries" was held in Schloss Dagstuhl – Leibniz Center for Informatics. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. The first section describes the seminar topics and goals in general. Links to extended abstracts or full papers are provided, if available.

Keywords. Formal verification, cyber-physical systems, analog circuits, theorem proving, systems biology, mean-field methods

The seminar aimed at bringing together researchers working on the analysis of systems, where the analysis uses abstractions or embeddings from discrete to continuous or from continuous to discrete domains. Such analysis across discrete-continuous boundaries appears in a large spectrum of practical and industrially relevant applications. They often play a pivotal role to arrive at useful analysis results. On the other hand, they necessarily incur some error, and make the question how to give proper correctness guarantees for the system behavior a notoriously difficult one.

Seminar Context. Formal models of computation have for long been considered independent of the concrete world, viewing hardware and software as discrete models of computation. However, there is nowadays a striking need to incorporate continuous physical reality, caused by very different trends and challenges, including *embedded and cyber-physical systems*, *deep sub-micron effects*, *biology-inspired computation*, or *analog and mixed-signal circuits design*.

On the other hand there are many application areas of scientific computing, that have traditionally treated their matter as of a mostly continuous nature, but

are starting to see the need to consider discrete structures, e.g. in some parts of *cell biology* and *chemical kinetics*, in *numerical mathematics*, and in *distributed control*.

In these areas it also occurs more and more, that a shift from (or to) a discrete interpretation to (or from) a continuous interpretation is a major step in model analysis. Often analyzing a continuous system by computer aided tools requires to switch to an appropriately truncated discrete approximation. Conversely, there are cases where the opposite strategy has proven succesful: A prominent example of this is integer linear programming, where e.g. the cutting plane method proceeds via an iteration over LP problems working on a continuous domain. Other examples e.g. emerge in the area of *mean field analysis* applied to distributed computing, where the interaction of large quantities of discrete components is summarized by an averaging continuous value.

Seminar Objectives. In the future, but even nowadays, it is becoming rather common in modelling and analysis to switch between a discrete and a continuous view on a system. The consequences of such an abstraction step are often overlooked however, especially if several of these switches occur during the modelling. For instance, a fluid mixture of chemical substrates, consisting of a discrete number of molecules, is represented by a differential equation with real valued parameters, which are analyzed by simulating the system in a floating point representation and in discrete time steps. Each of the switches induces an error in the analysis, and the effect on the accuracy of the analysis results might be extreme.

This seminar aimed at bringing together, for the first time, researchers from independent areas working on the boundary of discrete and continuous modelling and verification, with the intention to cross-fertilize their individual research topics.

We were striving for a broad coverage of instances where one or several of these boundary crossings occur, paired with technical discussions about possibilities to quantify induced errors. This created impulses for a cross-fertilizing research agenda that relates scientific and industrial contexts.

Abstractions of Stochastic Hybrid Systems

Alessandro Abate (Delft University of Technology, NL)

Engineering systems like communication networks or automotive and air traffic control systems, financial and industrial processes like market and manufacturing models, and natural systems like biological and ecological environments exhibit complex behaviors arising from the composition and interactions between their hybrid components. The presence of uncertainty, which is unquestionable in many biological systems and often inevitable for engineering systems, naturally leads to the employment of stochastic hybrid models.

This contribution will concentrate on understanding a few theoretical and computational properties of stochastic hybrid systems, and will propose techniques to attain formal abstractions of these models.

Keywords: Stochastic Hybrid Systems, Verification, Abstractions

A Lazy SMT-Solver for a Non-Linear Subset of Real Algebra

Erika Abraham (RWTH Aachen, DE)

There are several methods for the synthesis and analysis of hybrid systems that require efficient algorithms and tools for satisfiability checking. For analysis, e.g., bounded model checking describes counterexamples of a fixed length by logical formulas, whose satisfiability corresponds to the existence of such a counterexample.

As an example for parameter synthesis, we can state the correctness of a parameterized system by a logical formula; the solution set of the formula gives us possible safe instances of the parameters.

For discrete systems, which can be described by propositional logic formulas, SAT-solvers can be used for the satisfiability checks. For hybrid systems, having mixed discrete-continuous behavior, SMT-solvers are needed. SMT-solving extends SAT with theories, and has its main focus on linear arithmetic, which is sufficient to handle, e.g., linear hybrid systems. However, there are only few solvers for more expressive but still decidable logics like the first-order theory of the reals with addition and multiplication – real algebra. Since the synthesis and analysis of non-linear hybrid systems requires such a powerful logic, we need efficient SMT-solvers for real algebra. Our goal is to develop such an SMT-solver for the real algebra, which is both complete and efficient.

Keywords: SMT-solving, Real Algebra, Hybrid Systems, Verification, Synthesis

Joint work of: Abraham, Erika; Corzilius, Florian; Loup, Ulrich; Sturm, Thomas

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2010/2790

Abstractions to manage the complexity of discrete and continuous verification

Jacob A. Abraham (Univ. of Texas at Austin, US)

Complexity is the primary stumbling block to the effective validation of hardware both during design and after the chips are fabricated. This talk describes the trends in integrated circuits, including the increasing integration of mixed-signal modules on the chip. Abstractions can be used to manage the complexity of verification. In the discrete domain, slicing of the high-level hardware design description for a specific property speeds up existing model checking tools by orders of magnitude. One trend which is complicating hardware verification is the increasing variation in the device parameters due to the manufacturing processes in nanoscale technologies. In the continuous domain, a new verification technique constructs adaptive regression models for blocks of a complex mixed-signal design using transistor-level simulation. Non-idealities in circuit behavior are captured from the data. In the simulation of an oversampling $\Delta\Sigma$ analog-to-digital converter, the high-level models speeds up conventional circuit simulation by three orders of magnitude, with negligible error.

Keywords: Hardware verification, abstractions, slicing, analog

Non-Coding RNAs: The Cell's Dark Matter

Rolf Backofen (Universität Freiburg, DE)

Biology as well as systems-biology concentrated mainly on Proteins to describe cell states. However, it has become clear that many aspects of the cell's states are regulated by non-coding RNA. We will give an overview of RNA-based regulation and investigate different computational problems (both discrete and continous)related to the analysis of RNA.

Mean-field method for large dynamic gossip networks

Rena Bakhshi (Vrije Universiteit - Amsterdam, NL)

Gossip protocols are designed to operate in very large, decentralised networks. A node in such a network bases its decision to interact (gossip) with another node on its partial view of the global system. Because of the size of these networks, analysis of gossip protocols is mostly done using simulations, that tend to be expensive in computation time and memory consumption.

In this talk, we present an abstraction method for the performance evaluation of such systems, called the mean-field approximation. This method allows us to easily evaluate systems with very large numbers of nodes, that is, systems of such a size that traditional performance evaluation methods would fall short. The talk covers some results we obtain by applying this method, and by automating it.

Keywords: Gossip protocols, mean-field method

Full Paper:
http://www.few.vu.nl/∼rbakhshi/papers/qest10.pdf

Two-Domain DNA Strand Displacement

Luca Cardelli (Microsoft Research UK - Cambridge, GB)

We investigate the computing power of a restricted class of DNA strand displacement structures: those that are made of double strands with nicks (interruptions) in the top strand. To preserve this structural invariant, we impose restrictions on the single strands they interact with: we consider only two-domain single strands consisting of one toehold domain and one recognition domain. We study fork and join signal processing gates based on these structures, and we show that these systems are amenable to formalization and to mechanical verification.

Keywords: DNA Computing, Process Algebra

Full Paper:
http://lucacardelli.name/Papers/Two-Domain DNA Strand Displacement (DCM'10).pdf

See also: Developments in Computational Models 2010.

Modular modelling, space and parallel simulation for systems biology

Lorenzo Dematte (Microsoft Research - University Trento, IT)

The main goal of systems biology goal is to understand how a system as complex as a living creature can work and exists. In order to bring us closer to this goal, new modelling tools, simulation and verification algorithms are needed.

In this talk I will present my research on modelling and simulation, which involves modularity, spatial aspects, different level of detail and execution speed. In particular, I will concentrate on space, a very important aspect in the simulation of biochemical models; complex and large models of biochemical systems need to deal with the movement of molecules, taking into consideration localised fluctuations, transportation phenomena and diffusion.

This level of detail often clashes with the need for fast simulations: models could become very complex, especially when using stochastic methods in conjunction with a high spatial resolution.

Therefore, we experimented with several spatial methods, at different level of details, and with different parallelization techniques.

Keywords: Stochastic, simulation, parallelism, modelling

Combining interval and Groebner methods for verification of digital systems

Alexander Dreyer (Fraunhofer ITWM - Kaiserslautern, DE)

We present an hybrid algebraic/interval approach for proving the behaviour of digital systems. By combining a polynomial formulation and Groebner methods from computational algebra with an interval arithmetic-based preprocessing we can formally verify systems which were intractable before.

In an interdisciplinary project of mathematics (AG Profs. G.-M. Greuel and G. Pfister) and information technology (AG Prof. W. Kunz) we developed algorithms and tools for formally verifying the correctness of system-on-chips data paths with complex arithmetic. We combine techniques from computational algebra and interval arithmetic. We showed that such problems can be formulated on the word-level as polynomial systems over finite rings of the form $Z/2^n$, where each variable stands for a Boolean value and n for the bit-width. The proof goal corresponds to the computation of a normal form with respect to a Groebner basis of the system.

In general the computation of a Groebner basis is the hardest part of this approach. But for many formal verification problems it is possible exploit the topological structure of the system to generate an optimized "topological" variable ordering in such a way, that the resulting polynomial system is already a Groebner basis. This is an important discovery since then the theory of Groebner basis allows us to avoid many unnecessary computations such that the proof goal can be verified efficiently.

Due to our very compact modelling on the word-level, the subcomponents have usually different bit-widths. To generate an overall system over one ring, additional variables have to be introduced which mimic component pins for a numerical carry-over. Unfortunately, this may render the problem undecidable, because the original system does not contain relations about those new variables. At this point, we reinterpret the affected polynomials as continuous functions. Since the range of each variable is bounded we can use ideas from interval arithmetic to compute sufficiently tight bounds for the value domain of the function. This yields additional insights which we use for eliminating surplus variables.

We integrated this together with Boolean and bit-level reasoning in a formal verification work-flow for solving industrial problems. This allowed us, for example, to prove the correctness of the design of the arithmetic unit of Infineon's upcoming TriCore processor (640 proof goals) which was not verifyable before.

Keywords: Formal verification, interval abstraction, Groebner

Joint work of: Dreyer, Alexander; Greuel, Gert-Martin

Network-driven Boolean Normal Forms

Alexander Dreyer (Fraunhofer ITWM - Kaiserslautern, DE)

We apply the PolyBoRi framework for Groebner bases computations with Boolean polynomials to bit-valued problems from algebraic cryptanalysis and formal verification.

First, we proposed zero-suppressed binary decision diagrams (ZDDs) as a suitable data structure for Boolean polynomials.

Utilizing the advantages of ZDDs we develop new reduced normal form algorithms for linear lexicographical lead rewriting systems.

The latter play an important role in modeling bit-valued components of digital systems.

Next, we reorder the variables in Boolean polynomial rings with respect to the topology of digital components. This brings computational algebra to digital circuits and small scale crypto systems in the first place. We additionally propose an optimized topological ordering, which tends to keep the intermediate results small. Thus, we successfully applied the linear lexicographical lead techniques to non-trivial examples from formal verification of digital systems.

Finally, we evaluate the performance using benchmark examples from formal verification and cryptanalysis including equivalence checking of a bit-level formulation of multiplier components. Before we introduced topological orderings in PolyBoRi, state of the art for the algebraic approach was a bit-width of 4 for each factor. By combining our techniques we raised this bound to 16, which is an important step towards real-world applications.

Keywords: Groebner, normal forms, Boolean polynomials, cryptanalysis, verification

Joint work of: Brickenstein, Michael; Dreyer, Alexander

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2789

SAT Modulo ODE : A Direct SAT Approach to Hybrid Systems

Andreas Eggers (Universität Oldenburg, DE)

In this talk, we present our approach to perform bounded model checking (BMC) of hybrid discrete continuous systems using constraint solving techniques. The BMC problem can be expressed by a Boolean combination of arithmetic constraints and ordinary differential equations (ODEs). While the Boolean, integer, and real-valued variables represent the state of the hybrid system, the constraint system describes traces characterized by their initial states, a transition relation connecting subsequent states by continuous flows or discrete jumps, and a target state whose reachability is to be analyzed. The reachability problem of the hybrid system therefore becomes a satisfiability problem of this type of formula.

We extend our constraint solving algorithm iSAT to also handle the ODEs occurring in these formulae by using safe enclosures of the ODEs solution trajectories thereby coupling the structure of the DPLL procedure, which is used successfully in propositional satisfiability solving, with interval methods for arithmetic constraints and safe enclosure methods for the solutions of initial value problems. Our current work is focused (1) on exchanging our prototypical enclosure mechanism with Ned Nedialkov's VNODE-LP in order to obtain such enclosures more efficiently and (2) on storing once-deduced knowledge and potentially further information available on the solution trajectories persistently in the constraint system to avoid costly enclosures in the first place.

Keywords: Hybrid discrete continuous systems, automatic verification, satisfiability modulo theories, ordinary differential equations

Joint work of: Eggers, Andreas; Fränzle, Martin; Herde, Christian

Bio-Logic: The Challenges Facing Formal Modelling of Biology

Jasmin Fisher (Microsoft Research UK - Cambridge, GB)

As time goes by, it becomes more and more apparent that the puzzles of life involve more and more molecular pieces that fit together in increasingly complex ways. Biology is not an exact science. It is messy and noisy, and most often vague and ambiguous. We cannot assign clear rules to the way cells behave and interact with one another. And we often cannot quantify the exact amounts of molecules, such as genes and proteins, in the resolution of a single cell. To make matters worse (so to speak), the combinatorial complexity observed in biological networks (e.g., metabolic and signalling pathways) is staggering, which renders the comprehension and analysis of such systems a major challenge. Recent efforts to create executable models of complex biological phenomena entail great promise for new scientific discoveries, shading new light on the puzzle of life. At the same time, this Śnew wave of the futureŠ called Systems Biology forces Computer Science to stretch far and beyond, and in ways never considered before, in order to deal with the enormous complexity observed in biology. In this talk, I will summarize some of the major milestones on the way to conquer such complexity and to crack the logic behind biological processes - Bio-Logic.

Keywords: Biology, modelling, executable biology

Verification of Hybrid Systems with Piecewise Affine Dynamics using Support Functions

Goran Frehse (VERIMAG - Gières, FR)

Many questions about the behaviour of a dynamic system can be answered by computing its set of reachable states.

In the continuous domain, this computation suffers the inherent difficulty of representing and manipulating complex sets of continuous values. Recently, a technique has been developed that exploits an implicit representation of sets, their support function, and combines it with an explicit representation in the form of template polyhedra.

We present this technique and its implementation in the recently developed verification tool SpaceEx.

Keywords: Hybrid systems, verification, reachability, support functions, tools

Towards more Dependable Verification of Mixed-Signal Systems

Christoph Grimm (TU Wien, AT)

The verification of complex mixed-signal systems is a challenge, especially considering the impact of parameter variations. Besides the established approaches like Monte-Carlo or Corner-Case simulation, a novel semi-symbolic approach emerged in recent years. In this approach, parameter variations and tolerances are maintained as symbolic ranges during numerical simulation runs by using affine arithmetic. Maintaining parameter variations and tolerances in a symbolic way significantly increases verification coverage. In the following we give a brief introduction and an overview of research on semi-symbolic simulation of both circuits and systems and discuss possible application for system level verification and optimization.

Keywords: Affine Arithmetic, Range based methods, Verification, Semi-symbolic simulation

Joint work of: Schupfer, Florian; Grimm, Christoph

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2791

Towards Dependable Verification of Mixed-Signal Systems using Semi-Symbolic Simulation

Christoph Grimm (TU Wien, AT)

Verification of mixed-signal systems is a challenge, because errors are equally due to both inaccurate models, and insufficient verification coverage. Therefore, more and more accurate device models are used, and verification coverage is increased by automatically generating stimuli (e.g. corner cases). Unfortunately, both approaches increase simulation time and verification effort.

We propose a new approach that allows more dependable and yet abstract modeling using ranges, and semi-symbolic simulation based on Affine Arithmetics. We show that the approach is able to handle even analog circuits and complex signal processing methods, e.g. in control loops or communication systems.

Keywords: Affine Arithmetics, Semi-Formal Verification, Analog/Mixed-Signal Systems

Joint work of: Grimm, Christoph; Schupfer, Florian

Finite Automata As Time-Invariant Linear Systems: Observability, Reachability and More

Radu Grosu (SUNY - Stony Brook, US)

We show that regarding finite automata (FA) as discrete, time-invariant linear systems over semimodules, allows to: (1) express FA minimization and FA determinization as particular observability and reachability transformations of FA, respectively; (2) express FA pumping as a property of the FA's reachability matrix; (3) derive canonical forms for FAs. These results are to our knowledge new, and they may support a fresh look into hybrid automata properties, such as minimality. Moreover, they may allow to derive generalized notions of characteristic polynomials and associated eigenvalues, in the context of FA.

Keywords: Finite automata, control theory, automata minimization, observability reduction

Full Paper:
http://www.cs.sunysb.edu/∼grosu/hscc09.pdf

See also: R. Grosu. Finite Automata as Time-Invariant Linear Systems: Observability, Reachability and More. In Proc. of HSCC'09, the 12th International Conference on Hybrid Systems: Computation and Control, San Francisco, USA, April, 2009, pp. 194-208, Springer, LNCS 5469

Safety Verification for Probabilistic Hybrid Systems

Ernst Moritz Hahn (Universität des Saarlandes, DE)

The interplay of random phenomena and continuous real-time control deserves increased attention for instance in wireless sensing and control applications. Safety verification for such systems thus needs to consider probabilistic variations of systems with hybrid dynamics. In safety verification of classical hybrid systems we are interested in whether a certain set of unsafe system states can be reached from a set of initial states. In the probabilistic setting, we may ask instead whether the probability of reaching unsafe states is below some given threshold. In this paper, we consider probabilistic hybrid systems and develop a general abstraction technique for verifying probabilistic safety problems. This gives rise to the first mechanisable technique that can, in practice, formally verify safety properties of non-trivial continuous-time stochastic hybrid systems—without resorting to point-wise discretisation. Moreover, being based

on arbitrary abstractions computed by tools for the analysis of non-probabilistic hybrid systems, improvements in effectivity of such tools directly carry over to improvements in effectivity of the technique we describe. We demonstrate the applicability of our approach on a number of case studies, tackled using a prototypical implementation.

Keywords: Hybrid, probabilistic, abstraction

Joint work of: Zhang, Lijun; She, Zhikun; Ratschan, Stefan; Hermanns, Holger; Hahn, Ernst Moritz

Full Paper:
www2.imm.dtu.dk/~lizh/papers/cav10.ps

Approaches to Formal Verification of Analog Circuits on Transistor Level

Lars Hedrich (Goethe-Universität Frankfurt am Main, DE)

Analog circuits on transistor level are important parts of integrated circuits. General modeling of them result in highly nonlinear DAE-Systems with 10 to 10000 equations and many continuous state variables.

Using the numeric common simulation techniques enable sampling based formal verification methods in state space. The talk will give an overview how to formally verify properties and equivalences.

An extension to model-checking of mixed signal-systems by coupling these method will be added.

Keywords: Formal Verification Analog Mixe-Signal Circuits Equivalence Model Checking

The Digital/Analog(ue) Divide

Kevin Jones (City University - London, GB)

To motivate the need for cross domain thinking, we address the problems of, and need for, systems composed of both digital and analog hardware. We discuss the different world views represented by digital and analog approaches to designing hardware, and the implications these have to the prospects for successful designs. We present the state of the art in both spaces, and talk about some open issues. A particular approach to analog verification is discussed and we show how the correct use of transformation can greatly enhance the verification process. We conclude with some suggestions for areas of future interest.

Observation and Implementation of Simple Continuous Time Properties in a Discrete Time Setting with Bounded Jitter

Mark Lawford (McMaster University - Hamilton, CA)

Many safety and control systems are required to detect continuous time behaviour and react in a timely fashion. Typically these systems are implemented as computer controlled systems that sample their inputs, update their state and write their outputs at discrete times. The sampling and processing times are often assumed to be uniformly spaced but in fact usually have some jitter (variation) in the actual implementation. We show how discrete time implementations necessitate tolerances on durations, timing resolution, processing time, and jitter in order to observe and react to even simple real-time requirements specified in a continuous time setting. We formalize the continuous time setting and different discrete time settings in PVS, stating and proving necessary and sufficient conditions on the tolerances for observing a simple continuous property in a discrete time implementation. The conditions show that some real-time requirements may be met at significantly reduced CPU bandwidth through reducing jitter. We show how to design a software component that can observe the continuous time requirement and then verify it in PVS. This pre-verified component is then used to guide the design of more complex components and to decompose their design verification into simple inductive proofs.

Keywords: Real-time Systems, tolerance, observability, implementability, formal methods, PVS

Joint work of: Lawford, Mark;Hu, Xiayong; Wassyng, Alan

Full Paper:
http://www.cas.mcmaster.ca/~lawford/papers/FMICS08.html

Mean Field Methods for Computer and Communication Systems

Jean-Yves Le Boudec (EPFL - Lausanne, CH)

We consider a generic model of N interacting objects, where each object has a state and interaction between objects is Markovian, i.e. the evolution of the system depends only on the collection of states at any point in time. This is quite a general modeling framework, which was successfully applied to model many forms of communication protocols. When the number of objects N is large, one often uses simplifying assumptions called "mean field approximation", "fluid approximation", "fixed point method" or "decoupling assumption". In this tutorial we explain the meaning of these four concepts and show that the first two,

namely mean field approximation and fluid approximation, are generally valid (but not always).

However, we also show that the last two, namely fixed point method and decoupling assumption, require more care, as they may not be valid, even in simple cases. We give sufficient conditions under which they are valid. We illustrate the concepts with the analysis of the 802.11 WiFi protocol.

Keywords: Mean Field, Communication Systems, Decoupling Assumption

Full Paper:
http://infoscience.epfl.ch/getfile.py?recid=121369&mode=best

Exact Real Arithmetic

David Lester (University of Manchester, GB)

In this talk I present basic properties of the computable reals. This is followed by a discussion of the verification of a Haskell implementation in PVS, and an introduction to the problems of computable analysis.

Keywords: Computable Analysis, Computable Real Numbers, Haskell, PVS

Specification and Verification of Continuous Systems

Oded Maler (VERIMAG - Gières, FR)

The extension of formal verification to continuous and hybrid systems is a challenging task in which the semantical insights and algorithmics of discrete formal verification have to be combined with numerical analysis, computational geometry and other branches of mathematics. In the talk I will explain one of the major techniques, computing reachable sets for differential equations, and survey a decade of slow progress in this domain culminating in new techniques that can analyze linear systems with hundreds of state variables and medium size nonlinear systems.

In the rest of the talk I will speak about complementary methods that explore the state space systematically by simulations as well as the adaptation of temporal logic and its semantics to express properties of continuous trajectories.

Fast Adaptive Uniformization. Integration with the Stochastic Hybrid Model

Maria-Emanuela-Canini Mateescu (EPFL - Lausanne, CH)

Within systems biology there is an increasing interest in the stochastic behavior of biochemical reaction networks.

An appropriate stochastic description is provided by the chemical master equation, which represents a continuous-time Markov chain (CTMC).

The uniformization technique is an efficient method to compute probability distributions if the number of states of the Markov process is manageable.

However, the size of a Markov process that represents a biochemical reaction network is usually far beyond what is feasible.

In this paper we present an on-the-fly variant of uniformization, where we improve the original algorithm at the cost of a small approximation error. By means of several examples, we show that our approach is particularly well-suited for biochemical reaction networks.

Keywords: Chemical master equation, transient solution, biochemical reaction networks, uniformization

Joint work of: Mateescu, Maria-Emanuela-Canini; Didier, Frederic; Wolf, Verena; Henzinger, Thomas

Full Paper:
http://infoscience.epfl.ch/record/143070?ln=en

See also: HIBI '09 Proceedings of the 2009 International Workshop on High Performance Computational Systems Biology

Accounting for Continuity and Sensitivity in (mostly Continuous) Verification

Ian Mitchell (University of British Columbia - Vancouver, CA)

When discussing the verification of continuous and hybrid system models it is often the uncountably infinite sets from which states and times are drawn, and the consequential complexity of representing those states and times, that receives most of the attention. However, such models usually bring with them additional (sometimes implicit) constraints on continuity and/or sensitivity which must be considered – and can often be taken advantage of – in a computational context.

This talk illustrates such effects through three examples. First, continuity allows the Coho reachability tool to expend effort only along the boundary of the reachable set. Second, backward reachability can be used to demonstrate safety in a broader range of contexts than can forward reachability, but is more likely to fall prey to model sensitivity. Third, the continuity and sensitivity of matrix eigenvalues with respect to matrix elements as determined through matrix pseudospectra can be used to determine whether equilibria in a circuit model may or may not represent DC operating points.

Keywords: Reachability, sensitivity, hybrid systems, pseudospectra, verification, circuit analysis

Joint work of: Mitchell, Ian; Greenstreet, Mark; Yan, Chao; Zaki, Mohammed

Full Paper:
http://www.cs.ubc.ca/~mitchell/

See also: Mitchell, "Comparing Forward & Backward Reachability as Tools for Safety Analysis" in Hybrid Systems Computation and Control (HSCC), pp. 428-443 (April 2007); Yan & Greenstreet, "Verifying an Arbiter Circuit" in Formal Methods in Computer Aided Design (FMCAD), pp. 52-60 (November 2008); Zaki, Mitchell & Greenstreet, "DC Operating Point Analysis – A Formal Approach" in Formal Verification of Analog Circuits (May 2009)

Model Abstraction for Complex Systems

Chris J. Myers (Univ. of Utah - Salt Lake City, US)

In order to reason about systems, the construction of a model at the right level of abstraction is essential. Although the world is fundamentally discrete and stochastic, the modeling formalism of choice is often continuous and deterministic, namely differential equations. While this abstraction often yields significant reductions in analysis time, results may not accurately represent the systems behavior. Furthermore, the complexity of analysis may still be prohibitive. An alternative is to produce a higher-level discrete stochastic model which can produce representative results in substantially improved analysis time. This talk will present this method of abstraction as applied to examples both from analog/mixed-signal circuits and systems and synthetic biology.

Assume-Guarantee Verification for Probabilistic Systems

Gethin Norman (University of Glasgow, GB)

We present a compositional verification technique for systems that exhibit both probabilistic and nondeterministic behaviour. We adopt an assume-guarantee approach to verification, where both the assumptions made about system components and the guarantees that they provide are regular safety properties, represented by finite automata. Unlike previous proposals for assume-guarantee reasoning about probabilistic systems, our approach does not require that components interact in a fully synchronous fashion. In addition, the compositional verification method is efficient and fully automated, based on a reduction to the problem of multi-objective probabilistic model checking. We present asymmetric and circular assume-guarantee rules, and show how they can be adapted to form quantitative queries, yielding lower and upper bounds on the actual probabilities that a property is satisfied. Our techniques have been implemented and applied to several large case studies, including instances where conventional probabilistic verification is infeasible.

Keywords: Probabilistic model checking, compositional verification

Joint work of: Kwiatkowska, Marta; Norman, Gethin; Parker, David; Qu, Hongyang

Full Paper:
http://www.springerlink.com/content/v7723q0145175222/

See also: roc. 16th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'10), volume 6015 of LNCS, pages 23-37, Springer, 2010

Quantitative Abstraction Refinement

David Parker (University of Oxford, GB)

Probabilistic model checking has established itself as a valuable technique for formal modelling and analysis of systems that exhibit stochastic behaviour. It has been used to study quantitative properties of a wide range of systems, from randomised communication protocols to biological signalling pathways. In practice, however, scalability quickly becomes a major issue and, for large or even infinite-state systems, abstraction is an essential tool. What is needed are automated and efficient methods for constructing such abstractions.

In non-probabilistic model checking, this is often done using counterexample-guided abstraction-refinement (CEGAR), which takes a simple, coarse abstraction and then repeatedly refines it until it is amenable to model checking. This talk describes recent and ongoing work on quantitative abstraction-refinement techniques, which can be used to automate the process of building abstractions for probabilistic models. This has already been applied to probabilistic verification of real-time systems and of software, where abstraction is essential.

Programming Cells

Andrew Phillips (Microsoft Research UK - Cambridge, GB)

Cells are highly sophisticated organic machines. We can program cells using DNA, which is, in essence the machine code of life. In recent years, cells have been programmed using DNA taken from other cells or synthesized from scratch. However, programming cells in a reliable manner is extremely difficult and must be done with great care. In this talk we present a software tool for designing biological devices, simulating them on a computer, and compiling them to DNA code, which can then be inserted into living cells to program their behaviour. Given a design of a biological device and an extensive library of genetic parts, a compiler automatically selects the parts that satisfy the design constraints, allowing cells to be programmed more effectively. In future, cells could be programmed to help address important challenges in areas of food, medicine, energy and the environment.

Keywords: Synthetic Biology, Genetic Engineering, Stochastic Simulation, Programming Language, Logic Programming

Full Paper:
http://research.microsoft.com/gec

Temporal Refinement Using SMT and Model Checking with an Application to Physical-Layer Protocols

Lee Pike (Galois - Portland, US)

I demonstrate how to use a satisfiability modulo theories (SMT) solver together with a bounded model checker to complete highly-automated temporal refinement proofs. The method is demonstrated by refining a specification of the 8N1 Protocol, a widely-used protocol for serial data transmission. A nondeterministic finite-state 8N1 specification is refined to an infinite-state implementation in which interleavings are constrained by real-time linear inequalities. The refinement proof is via automated induction proofs over infinite-state transitions systems using SMT and model checking, as implemented in SRI International's Symbolic Analysis Laboratory (SAL).

Keywords: Infinite-state model-checking, temporal refinement

Full Paper:
http://www.cs.indiana.edu/~lepike/pub_pages/refinement.html

See also: Geoffrey Brown and Lee Pike. Temporal refinement using SMT and model checking with an application to physical-layer protocols. In Fifth ACM-IEEE International Conference on Formal Methods and Models for Codesign (MEMOCODE'2007), 2007.

Hybrid Systems Verification with HSolver

Stefan Ratschan (Academy of Science - Prague, CZ)

We will give an overview of the techniques employed in the tool HSolver (http://hsolver.sourceforge.net) that allows the verification of hybrid dynamical systems that contain non-linear ODEs, and that retains soundness even in the presence of floating point rounding errors. The talk will include a presentation of still unpublished techniques implemented in the latest version of HSolver.

Bounding the Equilibrium Distribution of Markov Population Models

David Spieler (Universität des Saarlandes, DE)

The equilibrium distribution of continuous-time Markov chains can reveal interesting properties. For example in biological systems, bistability of a chemical reaction network can hint at its function as a biological switch. Unfortunately, the state space of these systems is infinite in most cases, preventing the use of traditional steady state solution techniques.

In this talk we will develop a new approach to tackle this problem by first retrieving geometric bounds enclosing a major portion of the steady state probability mass, followed by a more detailed analysis revealing state-wise bounds.

Keywords: Geometric Bounds, Equilibrium, Stochastic Complement, Markov Population Model

Formal Analysis of Probabilistic Systems using HOL Theorem Proving

Sofiene Tahar (Concordia Univ. - Montreal, CA)

Probabilistic analysis is a tool of fundamental importance to virtually all scientists and engineers as they often have to deal with systems that exhibit random or unpredictable elements. Traditionally, computer simulation techniques are used to perform probabilistic analysis. However, they provide less accurate results and cannot handle large-scale problems due to their enormous computer processing time requirements. To overcome these limitations, we propose to perform formal probabilistic and statistical analysis using higher-order logic theorem proving. We provide a framework for the formalization of both discrete and continuous random variables and the ability to formally verify system's probabilistic and statistical properties. The analysis carried out in this way is free from any approximation or precision issues due to the mathematical nature of the models and the inherent soundness of the theorem proving approach. In order to illustrate the practical effectiveness of the proposed framework, we present the probabilistic analysis of four examples across three application areas: the Coupon Collector's problem (software), the Stop-and-Wait protocol (telecommunications), the reliability of memory arrays (microelectronics), and floating-point error analysis (computer hardware).

Stochastic Modeling and Simulation of Chemical Dynamics

Verena Wolf (Universität des Saarlandes, DE)

We present a numerical approximation technique for the analysis of continuous-time Markov chains that describe networks of biochemical reactions and play an important role in the stochastic modeling of biological systems.

Our approach is based on the construction of a stochastic hybrid model in which certain discrete random variables of the original Markov chain are approximated by continuous deterministic variables.

We compute the solution of the stochastic hybrid model using a numerical algorithm that discretizes time and in each step performs a mutual update of the transient probability distribution of the discrete stochastic variables and the values of the continuous deterministic variables.

We implemented the algorithm and we demonstrate its usefulness and efficiency on several case studies from systems biology.

Keywords: Stochastic hybrid, Markov model, chemical reactions

Circuit Verification: Reachability Analysis Approach

Chao Yan (University of British Columbia - Vancouver, CA)

Formal verification is a promising method for validating circuit designs. We proposed a reachability analysis based technology to verify circuits using continuous models. Our method models a circuit as a system of ODEs and specifies analog signals by Brockett's annuli, it represents reachable regions by "projectagons" and approximates nonlinear dynamic by linear differential inclusion.

These algorithms are implemented in a reachability analysis tool: Coho. The tool has been applied to several circuits including synchronous, asynchronous, and analog circuits. These examples show that reachability analysis can formally verify properties of analog circuits in the continuous domain. Lessons of our experience and open problems will be discussed at the end.

Keywords: Circuit Verification, Reachability Analysis

DC Operating Point Analysis - A Formal Approach

Mohamed Zaki (University of British Columbia - Vancouver, CA)

Embedded systems are becoming a core technology in a growing range of electronic devices. Cornerstones of embedded systems are analog and mixed signal designs, which are integrated circuits required at the interfaces with the physical environment. A fundamental problem in the study of circuits is DC operating point analysis: what voltages will the nodes of the circuit settle to if the inputs to the circuit remain indefinitely at their quiescent values? Many critical properties of a circuit's behavior are directly connected to analyzing its DC operating point(s). In this talk, we describe a procedure that uses symbolic circuit models generated from a netlist level circuit description to rigorously locate and classify all of the equilibria of a circuit model in order to determine the existence, location and number of DC operating points. Implemented with a collection of public tools and our own Matlab circuit modeling toolbox OOmspice, we demonstrate that the technique can deduce several interesting properties like the hysteresis of a Schmitt trigger, the lack of DC operating points for ring oscillators with an odd number of stages and the transistor sizing requirements for the Rambus oscillator.

Keywords: Analog and mixed signal, stability analysis, verification, Matlab

Joint work of: Zaki, Mohamed H.; Mitchell, Ian; Greenstreet, Mark