Software Modeling and Verification

Staff

- **Professors**
  Prof. Dr. Ir. Joost-Pieter Katoen
  Prof. em. Dr. Klaus Indermark
  Prof. Dr. Erika Ábrahám
  http://moves.rwth-aachen.de/

- **Secretary**
  Elke Ohlenforst

- **Lecturer**
  AOR Priv.-Doz. Dr. Thomas Noll

- **Researchers**
  Dr. Henrik Bohnenkamp
  Xin Chen, M.Sc.
  Dr. Tingting Han
  Dipl.-Inform. Jonathan Heinen
  Dipl.-Inform. Christina Jansen
  Dipl.-Inform. Nils Jansen
  Dipl.-Inform. Daniel Klink (until Apr. 2010)
  Dipl.-Inform. Ulrich Loup
  Dr. Etienne Lozes
  Alexandru Mereacre, M.Sc.
  Dipl.-Inform. Johanna Nellen
  Dipl.-Inform. Martin Neuhäußer (until Jan. 2010)
  Viet Yen Nguyen, M.Sc.
  Dipl.-Inform. Maximilian R. Odenbrett
  Arpit Sharma, M.Sc.
  Falak Sher, M.Sc.
  Dipl.-Inform. Sabrina von Styp
  Dipl.-Inform. Haidi Yue

- **Technical Staff**
  Arnd Gehrmann

- **Diploma/Bachelor/Master Students**
  M. Bretsch
  S. de Carolis
  F. Corzilius
  C. Dehnert
  F. Fiedler
  F. Gretz

D. Guck
S. Herting
C. Jansen
M. Kampschulte
J. Nellen
M. R. Odenbrett
P. Richter
J. Scherer
F. Sher
L. von Büttner
S. von Styp
S. Wu

- **Student Researchers**
  B. Bruetsch
  C. Dehnert
  F. Dulat
  D. Guck
  S. Junges
  J. Katelaan
  M. Prümmer
  M. Scheffler
  M. Van de veire

- **Visiting Scientists**
  Dr. Alessandro Abate (TU Delft, NL)
  Benoit Barbot (ENS Cachan, F)
  Prof. Dr. Franck van Breugel (York University, CND)
  Prof. Dr. Stephane Demri (ENS Cachan, F)
  Muhammad Fadlisyah (University of Oslo, N)
  Dr. Colas Le Guernic (Verimag)
  Dr. Michael Huth (Imperial College, UK)
  Marijn Jongerden (Uni Twente, NL)
  Daniela Lepri (University of Oslo, N)
  Dr. Larissa Meinicke (Macquarie University, AUS)
  Prof. Dr. Peter Csaba Ölveczky (University of Oslo, N)
  Prof. Dr. Martin Steffen (University of Oslo, N)
  Mark Timmer (Uni Twente, NL)
  Dr. Olga Tveretina (Karlsruhe University, D)
  Ralf Wimmer (Universität Freiburg, D)
  Jun.-Prof. Dr. Verena Wolf (Saarland University, D)
  Dr. Ivan Zapreev (CWI, NL)

Overview

The year twenty-ten has been full of activities. The COMPASS project, a joint effort with FBK (Trento, I), and Thales Alennia Space (Cannes, F), funded by the European Space Agency (ESA), has been succesfully brought to an end. In April, an advanced toolset was completed supporting a rich plethora of analysis facilities for AADL models, e.g. model checking, fault tree analysis, and performability evaluation. Based on our results, ESA offered a project extension as well as the financial support for a PhD student (in their NPI programme). At the moment, several successors to COMPASS are considered by the ESA, indicating the relevance of this project.

Other worthwhile successes this year: a paper in the Communications of the ACM, Carsten Kern (former Ph.D student) received the Borchers Plakette from the RWTH Aachen University for his excellent dissertation, while Tingting Han (currently post-doctoral researcher at the chair) received the prize for the best dissertation in 2009 of the University of Twente! Besides, we received a top-cited award (over 2005-2010) for a paper in the journal Theoretical Computer Science.

New projects include an FP7 project on stochastic hybrid systems (with ETH Zurich, TU Delft, OFFIS Oldenburg, and Politecnico Milano). The challenge will be to join control theory, hybrid and probabilistic aspects. Other new projects include the exploitation of multi-core architectures for (probabilistic) model checking (with the University of Eindhoven) in the context of an NWO project. Continuing projects include the DFG-NWO project ROCKS, our participation in the research training group AlgoSyn and the DFG Excellence Cluster UMIC.

We were actively involved in the organisation of a special session at the ISOLA Symposium in October 2010, and co-organised a Spring School on Quantitative Model Checking, together with Kim G. Larsen (Aalborg, DK) in Copenhagen. The school attracted about 85 participants, the maximal capacity.

On the personnel side, several changes took place. Martin Neuhäußer and Daniel Klink successfully defended their Ph.D dissertation, and both left to industry. Six new Ph.D students started: Falak Sher, Arpit Sharma (thanks to an India4EU grant), Hongfei Fu (thanks to a CSC scholarship), Maximilian R. Odenbrett (who works in a joint project with the University of Eindhoven, NL), Sabrina von Styp (AlgoSyn), and Christina Jansen. Taolue Chen joined us as a guest researcher since August.

The embedded junior professorship "Theory of Hybrid Systems", led by Erika Ábrahám, has expanded its research activities in the last year.

The research area of the group covers modeling and analysis of hybrid systems, probabilistic systems in general and - by participation in the research training group AlgoSyn - the application of SMT-solving for real algebra in the synthesis and verification of hybrid systems.

The projects HySmart and CEBug started this year, furthermore the group participates in the ROCKS project.

The quality of the work is reflected in several publications. Several both national and international cooperations led to new promising approaches, e.g., by recent work together with the external PhD students Muhammad Fadlisyah and Daniela Lepri from the University of Oslo, co-supervised by Prof. Ábrahám.

The group is happy to welcome Johanna Nellen as a new research assistant. She will work in an interdisciplinary area in cooperation with the engineering department.

In addition to research, the group was very successful in co-organizing several events that aim at the motivation of interested pupils for the studies of computer science (Schüleruniversität, Ringvorlesung für Schüler, Girls' Day, Helle Köpfe). Details can be found at the corresponding section of the annual report.

Joost-Pieter Katoen.

Research Projects

Formal Models of Microcontroller Systems

Th. Noll, B. Schlich (i11), J. Brauer (i11)

Embedded systems usually operate in uncertain environments, giving rise to a high degree of nondeterminism in the corresponding formal models. Moreover they generally handle data spaces whose sizes grow with the memory and the word length of the respective microcontroller architectures. This, together with other effects, leads to the well-known state-space explosion problem, meaning that the models of those systems grow exponentially in size as the number of components increases. Careful handling of both nondeterminism and large data spaces is therefore crucial for obtaining efficient methods and tools for analysis and verification.

The goal of this project, carried out in close cooperation with the Embedded Software Laboratory of our department, is to develop formal computation models and abstraction techniques to tackle this problem. The first step was to set up a general automata-based model for microcontrollers, taking into account both the hardware, the software, and the environment of the system. During the period under report, this model was used to approach the state-space explosion problem as follows.

In the first activity, we developed static analysis methods for approximating the possible run-time values of data values. For this purpose, intervals have successfully been used for decades. Binary code on microcontroller platforms, however, is different from high-level code in that data is frequently altered using bit-wise operations and that the results of operations often depend on the hardware configuration. We therefore came up with a method that combines word- and bit-level interval analysis and integrates a hardware model by means of abstract interpretation in order to handle these peculiarities.

QUPES: Verification of Quantitative Properties of Embedded Software

T. Han, J.-P. Katoen, M. Neuhäußer

Embedded software typically executes on devices that, first and foremost, are not personal computers. Due to its embedded nature, its robustness is of prime importance, and timely reactions to stimuli from its -- mostly physical -- environment are essential. The aim of the QUPES project is to assess these quantitative aspects (e.g., timeliness and robustness) as an integral part of the embedded software validation phase.

To accomplish this, probabilistic model-checking techniques can be applied for models that are equipped with randomness and variants thereof which also exhibit nondeterminism. Based

on efficient numerical methods and abstraction techniques, quantitative properties can be checked automatically even on large state spaces with millions of states using dedicated tools. Opposed to, amongst others, the essential feature of model checking, where evidences will be provided on a property refutation, counterexample generation in probabilistic model checking is almost not developed. We provide the theoretical and algorithmic foundations for counterexample generation in probabilistic model checking, in particular for discrete-time Markov chains. One of the key principles is the casting of the concepts of strongest evidence and smallest counterexample as (variants of) shortest path problems. This enabled the use of efficient and well-studied graph algorithms for counterexample generation. These results can be extended to Markov chains with rewards, to Markov decision processes (MDPs), to LTL model checking, and have been recently been adopted in probabilistic counterexample-guided abstraction-refinement (CEGAR) techniques for MDPs as well as in counterexample generation for continuous-time Markov chains (CTMC) and cpCTL logic. Compact representation of a counterexample by regular expressions are also studied.

Further, compositional reasoning is a key strategy in analyzing complex systems as it allows the use of hierarchical and modular modeling formalisms like stochastic process algebras, stochastic activity networks or generalized stochastic Petri nets. Continuous-time Markov Decision processes (CTMDPs) are the nondeterministic counterpart of the aforementioned CTMCs and are well suited for compositional verification techniques. We define stochastic logics (like CSL) on CTMDPs and provide their measure-theoretic basis. Further, well-known equivalences like strong and weak bisimulation relations are adapted to CTMDPs which considerably reduce the state-space needed for quantitative analysis.

Verifying Pointer Programs with Unbounded Heap Structures

J. Heinen, C. Jansen, J.-P. Katoen, J. Nellen, Th. Noll, S. Rieger

The incorrect use of pointers is one of the most common sources of software errors. This especially applies to concurrent systems whose nondeterministic behavior rises additional challenges. Proving the correctness of concurrent pointer-manipulating programs with unbounded heap, let alone algorithmically, is a highly non-trivial task. This project attempts to develop automated verification techniques and accompanying tool support for concurrent programs with dynamic thread creation and memory allocation that handle linked data structures which are potentially unbounded in their size.

After considering (possibly cyclic) singly-linked list data structures, the approach was extended to analyze programs that handle more complex dynamic data structures. We developed a novel abstraction framework that is based on graph grammars, more precisely context-free hyperedge replacement grammars, as an intuitive formalism for abstractly modeling dynamic data structures. The key idea is to use the replacement operations which are induced by the grammar rules in two directions. By a backward application of some rule, a subgraph of the heap can be condensed into a single nonterminal edge, thus obtaining an abstraction of the heap. By applying rules in forward direction, certain parts of the heap which have been abstracted before can be concretized again, which avoids the necessity for explicitly defining the effect of pointer-manipulating operations on abstracted parts of the heap.

Two central issues in this context are correctness and efficiency. The first essentially boils down to the requirement that a nonterminal can always be concretized to the data structure from which it was abstracted. To ensure his property, we defined a novel normal form for hyperedge replacement grammars that is inspired by the well-known Greibach normal form for string grammars. Moreover we developed an algorithm for constructing a normalized grammar from a given hyperedge replacement grammar with bounded degree.

With regard to efficiency, two ideas were followed. The first concentrates on analyzing the (backward) confluence properties of graph grammars, which guarantees the uniqueness of abstractions and thus avoids the need to inspect several possible abstractions. The second is to adopt learning techniques to automatically derive abstraction grammars for the data structures occurring in the given program. This circumvents the complex and error-prone procedure of developing grammars manually.

The techniques were successfully applied to dynamic data structures such as doubly-linked lists, binary and ternary trees (also with connected leafs). In particular, after implementing a prototype tool is was possible to establish the termination, correctness, and completeness of the well-known Deutsch-Schorr-Waite traversal algorithm in a fully automatic way.

Correctness, Modeling and Performance of Aerospace Systems (COMPASS)

Joint project together with the groups of Alessandro Cimatti (Fondazione Bruno Kessler, Centre for Scientific and Technological Research, Trento, Italy), and Xavier Olive (Thales Alenia Space, On Board Software Department, Cannes, France)

In this project we develop a model-based approach to system-software co-engineering which is tailored to the specific characteristics of critical on-board systems for the space domain. The approach is supported by a System-Level Integrated Modeling (SLIM) Language in which engineers are provided with convenient ways to specify a.o. nominal hardware, as well as software operations, timed and hybrid behavior, (probabilistic) faults and their propagation, error recovery and degraded modes of operation. This language is based on the Architecture Analysis and Design Language (AADL) and its Error Model Annex which allows for the modeling of error behavior. A kernel of the SLIM Language is equipped with a formal semantics that provides the interpretation of SLIM specifications in a precise and unambiguous manner. Systems are considered as a hierarchy of (hardware and software) components which are defined by their type (interface) and implementation. Components interact via ports allowing for both message-oriented and continuous communication. The internal structure of a component implementation is specified by its decomposition into subcomponents, together with their HW/SW bindings and their interaction via connections over ports. Component behavior is specified by a textual description of mode-transition diagrams. System reconfiguration is supported by mode-dependent presence of subcomponents and their connections. Error behaviour is described by probabilistic finite state machines, where error delays may be governed by continuous random variables.

Correctness properties, safety guarantees, and performance and dependability requirements are specified using requirement specification patterns which act as parameterized ``templates''

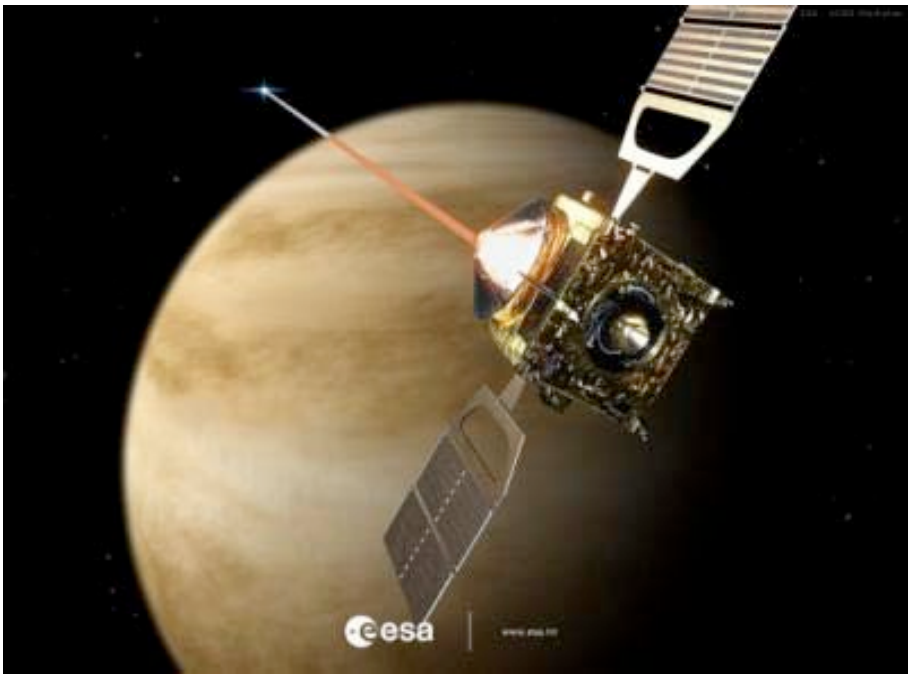
to the engineers and thus offer a comprehensible and easy-to-use framework for requirement specification.

The properties are checked on the SLIM specification using rigorous analysis methods. The precise character of these techniques together with the formal semantics of SLIM yield a trustworthy modeling and analysis framework for system and software engineers. The formal analysis is based on state-of-the-art model checking techniques such as bounded SAT-based and symbolic model checking, and extensions of model checking with numerical and simulative means to reason about quantitative requirements such as performance and dependability. The analysis facilities support, among others: automated derivation of dynamic (i.e., randomly timed) fault trees, Failure Modes and Effects Analysis (FMEA) tables, assessment of Fault Detection, Isolation, and Recovery (FDIR) measures, and observability requirements for effective diagnosability by FDIR.

The prototype of an integrated platform on top of state-of-the-art tools with an accompanying graphical user interface is available, and has been evaluated by Thales Alenia Space using several case studies involving critical on-board computer-based systems from the satellite domain. Another outcome of the project is an extension of AADL's Error Model Annex and the corresponding semantics.

Current activities concentrate on improving the applicability and efficiency of the toolset when analyzing systems that exhibit complex characteristics in terms of non-determinism, timed and hybrid behavior, and discrete and continuous-time probabilistic errors, see the following project. More information on COMPASS is available at

http://compass.informatik.rwth-aachen.de/.



Extending and Improving Formal Methods for System/Software Co-Engineering

J.-P. Katoen, V.Y. Nguyen, Th. Noll

The achievement of mission objectives and ultimate mission success relies on the safety and dependability of the space systems. During their operational lifetime, they have to overcome software and hardware failures autonomously, as communications to deep-space systems have long latencies. For this reason, it is imperative that these autonomous (and complex) systems operate correctly.

The aim of this project is to build upon the experiences from the previously described COMPOSS project and overcome several limitations of the current approaches to dependability and performance analysis. The first goal is to develop novel and advanced analysis techniques to enlarge the supported classes of system models by considering continuous-time (error) behaviour and non-determinism. The second goal is to enhance existing and develop new techniques that exploit the hierarchical and component-oriented structure of system descriptions. The plan is to provide prototypical realization of the developed techniques and apply them to small to moderately sized case studies and evaluate their feasibility.

Quasimodo

H. Bohnenkamp, H. Yue, J.-P. Katoen

The MOVES group participates in the European research project "Quasimodo", funded by the European Commission under the IST framework programme 7 for Information and Communication Technology, ICT. The objective of this project is to develop theory, techniques and tool components for handling quantitative (e.g. real-time, hybrid and stochastic) constraints in model-driven development of real-time embedded systems. Ultimate aim is to increase the competitiveness of European industrial companies which develop, implement and deploy embedded systems.

More specifically, the project aims are:

- Improving the modelling of diverse quantitative aspects of embedded systems.
- Providing a wide range of powerful techniques for analysing models with quantitative information and for establishing abstraction relations between them.
- Generating predictable code from quantitative models.
- Improving the overall quality of testing by using suitable quantitative models as the basis for generating sound and correct test cases.
- Applying the techniques to real-life case studies and disseminating the results to industry.

Project partners are universities, research institutes, and companies in Germany, The Netherlands, Denmark, Belgium, and France. The MOVES Group is currently working on a case study for a sensor-network gossiping protocol, which is posed by one of the industrial partners.

The MoDeST Tool Environment

H. Bohnenkamp, H. Yue, J.-P. Katoen

The specification language MoDeST covers a wide spectrum of modelling concepts, ranging from plain labelled transition systems to stochastic systems like Generalised Semi-Markov Decision Processes. MoDeST possesses a rigid, process-algebra style semantics, and yet provides modern and flexible specification constructs. MoDeST specifications constitute a coherent starting-point to analyse distinct system characteristics with various techniques, e.g., model checking to assess functional correctness and discrete-event simulation to establish the system's reliability. Analysis results thus refer to the same system specification, rather than to different (and potentially incompatible) specifications of system perspectives like in the UML.

The tool MoToR (MoDeST Tool enviRonment) aims to provide the means to analyse and evaluate MoDeST specifications. It is written in the C++ programming language. The tool provides (i) interfacing capabilities for connection to existing tools for specific projected models, and (ii) also means for enhancement by native algorithms for analysis of (classes) of MoDeST specifications. In earlier work, MoToR has been connected to Möbius, a performance evaluation tool suite that has been developed at the University of Illinois at Urbana-Champaign, US. The MoDeST/Möbius tandem is currently used and constantly improved in the Quasimodo project case studies.

Ultra High Speed Mobile Information and Communication

H. Yue, H. Bohnenkamp, J.-P. Katoen,

The evaluation of the quality-of-service of Wireless Sensor Networks is mostly done by simulation. In the context of the Quasimodo and UMIC projects, and in cooperation with the company CHESS, Haarlem, NL, we evaluated a gossiping MAC protocol (GMAC), a TDMA protocol for completely unconfigured wireless networks, which aims to improve message dissemination by collision avoidance between wireless nodes.

The GMAC protocol is designed with a specific radio model in mind, the Unit Disk Graph (UDG) model. Simulations, carried out with the MoDeST/Möbius tool set, show that GMAC has indeed a beneficial influence on the dissemination speed of a wireless network. Yet, the UDG model is very simple, and we investigated the possibility that it is perhaps too simple.

For this purpose, we evaluated GMAC using another radio model, the SINR model of Gupta/Kumar, which intuitively seems to be

more realistic. The results show that indeed GMAC performs much worse under the SINR model, and in fact we were able to show that the simple slotted ALOHA protocol, without any collision avoidance, can in some circumstances perform even better.

Or current research aims at gathering evidence that the SINR model is in fact realistic enough to allow the derivation of reliable measures for wireless sensor networks using simulation. For that we try to explain measurement data from CHESS by means of the SINR model.

Invariant Generation for Probabilistic Programs

F. Gretz, J.-P. Katoen, A. McIver (Macquarie Univ, Sydney), L. Meinicke (Macquarie Univ, Sydney), C. Morgan (UNSW, Sydney)

Verification of sequential programs rests typically on the pioneering work of Floyd, Hoare and Dijkstra in which annotations are associated with control points in the program. For probabilistic programs, quantitative annotations are needed to reason about probabilistic program correctness. We generalise the method of Floyd, Hoare and Dijkstra to probabilistic programs by making the annotations real- rather than Boolean-valued expressions in the program variables. The crucial annotations are those used for loops, the loop invariants. Thus in particular we focus on real-valued, quantitative invariants: they are random variables whose expected value is not decreased by iterations of the loop.

One way of finding annotations is to place them speculatively on the program, as parametrised formula containing only first-order unknowns, and then to use a constraint solver to search for parameter instantiations that would make the associated “verification conditions” true. In this project, we aim to generalize and extend constraint-solving techniques for invariant generation to probabilistic programs. This allows for the verification of probabilistic programs that cannot be treated with currently available automated techniques such as abstraction refinement together with model checking. This work includes theory development as well as prototypical tool development to illustrate the feasibility.

Verification of Stochastic Hybrid Systems

J.-P. Katoen, A. Mereacre, F. Sher

In the context of the EU FP7-project "Modeling, verification and control of complex systems: From foundations to power network applications" (partners: ETH Zurich, TU Delft, University of Oldenburg, Politecnico Milano, and Honeywell), we propose novel methods for modelling, analysis and control of complex, large scale systems. Fundamental research is motivated by applied problems in power networks. We adopt the framework of stochastic

hybrid systems (SHS), which allows one to capture the interaction between continuous dynamics, discrete dynamics and probabilistic uncertainty. In the context of power networks, SHS arise naturally: continuous dynamics model the evolution of voltages, frequencies, etc. Discrete dynamics reflect changes in network topology, and probability represents the uncertainty about power demand and (with the advent of renewables) power supply. More generally, because of their versatility, SHS are recognized as an ideal framework for capturing the intricacies of complex, large scale systems.

Motivated by this, considerable research effort has been devoted to the development of modelling, analysis and control methods for SHS, in both computer science (giving rise to theorem proving and model checking methods) and in control engineering (giving rise to optimal control and randomized methods). Despite several success stories, however, none of the methods currently available is powerful enough to deal with real life large scale applications. We feel that a key reason for this is that the methods have been developed by different communities in relative isolation, motivated by different applications. As a consequence, synergies between them have never been fully explored.

In this project, we systematically explore such synergies. Our multi-disciplinary team, which brings together experts on all the state of the art SHS methods, will establish links between model checking, theorem proving, optimal control and randomized methods. Leveraging on their complementary strengths we will develop combined strategies and tools to enable novel applications to complex, large scale systems. Common power networks case studies will provide a testing ground for the fundamental developments, motivate them, and keep them focused.

SYRUP: SYmbolic RedUction of Probabilistic Models

J.-P. Katoen, M. Timmer, M. Stoelinga, J. van de Pol (all three from University of Twente, NL).

Efficient model-checking algorithms exist for qualitative and quantitative properties for a range of probabilistic models. Their popularity is due to the presence of powerful software tools, and their wide applicability; security, distributed algorithms, systems biology, dependability and performance analysis, to mention a few. The main deficiencies of probabilistic model checking are the state explosion problem and the restricted treatment of data.

The state space grows exponentially in the size of system components and data domains. Whereas most abstraction techniques obtain smaller models by collapsing sets of concrete states at the model level, this project takes a radically different approach. We will develop and implement symbolic reduction techniques for probabilistic models. These techniques aim to reduce models by model transformations at the language level in order to minimize state spaces prior to their generation while preserving functional and quantitative properties. Our symbolic reductions will support data as first-class citizens, i.e., we will develop techniques to symbolically reduce formalisms for modeling probabilistic systems that are equipped with rich data types, allowing, e.g., probabilistic choices parameterized with data.

Our approach is based on successful symbolic transformation techniques in the traditional and timed setting, viz. linear process equations (LPEs). We will generalize and extend these techniques to probabilistic automata (PA), a model akin to Markov Decision Processes that is tailored to compositional modeling. The LPE technique is applicable to large or even infinite systems, and will be equipped with symbolic transformations such as confluence reduction, bisimulation minimization and static analysis for PA.

Computing maximum reachability probabilities in Markovian Timed Automata

T. Han, A. Mereacre, J.-P. Katoen

We investigate a stochastic extension of timed automata, called Markovian timed automata (MTA). For this model, we study the problem of optimizing reachability probabilities. Two variants are considered: time-bounded and unbounded reachability. For each case, we propose Bellman equations to characterize the reachability probability. For the former, we provide two approaches to solve the Bellman equations, namely, a discretization and a reduction to Hamilton-Jacobi-Bellman partial differential equations, which can be solved by discretization. For the latter, we show that in the single-clock case, the problem can be reduced to solving a system of linear equations, whose coefficients are time-bounded reachability probabilities in continuous-time Markov decision processes (CTMDPs).

Testing of Systems with Time and Data

S. von Styp, H. Bohnenkamp, J.-P. Katoen

Testing is one of the most important methods to verify the correctness of software. Nevertheless, testing manually is time consuming and expensive. Therefore model based testing, which automatically generates test cases from a given formal model, has been developed. In model based testing the specification is given by a transition system. A conformance relation formally defines under which circumstances an implementation is correct with respect to the specification. Based on this relation test-cases are derived automatically and are used for testing the real implementation.

The goal of this project is to extend the existing test theory to allow real-time behaviour together with data-dependent control flow. We start by giving a formal definition in form of a transition system for representing systems that allow data-dependent control flow for inputs and outputs and real-time behaviour. Afterwards a symbolic trace semantic is defined. This semantic then is needed to define the conformance relation, which describes under which conditions an implementation is correct with respect to a given specification. Future steps will include to look at applications such as on the fly testing. This then shall be implemented in the test tool JTorX.

Synthesising of Model Based Testing for Process Control Engineering

S. von Styp, H. Bohnenkamp, J.-P. Katoen, Gustavo Quirós, U. Epple

In Process Control Engineering controllers for plants that are not correct with respect to their specification can cause fatal disasters, e.g. when tanks with acid run over, people get injured or high pressure can lead to explosions. Therefore an intensive testing of the controller is crucial but it consumes a lot of time and money. The specification of such controllers is usually formally given by sequential function charts.

This project is a cooperation with the Institute for Process Control Engineering and its aim is to apply the methods of model based testing on the plant controller in oder to reduce costs, time and therefore to automate and systematise the testing process. The specifications are given as sequential function charts, which are translated to transition systems. We will start testing using simple controllers, e.g. a motor controller, which allows us to use already existing theories such as ioco and tioco including the testing tool JTorX. Data-dependent control flow is an important feature of the plant controllers, e.g. the next action depends on the current filling level of a tank. The same holds for real-time behaviour. It is crucial that certain actions are executed within a certain time. In order to be able to consider these characteristics it is planed to use the results from the project "Testing of Systems with Time and Data" and finally to test controllers for hole plants.

The application of SMT-solving for real algebra in the synthesis and verification of hybrid systems

E. Ábrahám, U. Loup, F. Corzilius

Hybrid systems are a powerful model describing a discrete controller in a continuous, real-world setting. Thus it often applies in the context of AlgoSyn where control and process engineering are involved. Formal verification of certain properties of hybrid systems is already an ambitious task, but going one step further, the work of AlgoSyn aims at synthesis of hybrid systems, i.e., synthesis of controllers for real-world settings.

In both synthesis and the more modest approach of verification, highly tuned solvers for systems of equations and inequations over the real numbers are needed in order to cope with practical problems. In case such systems involve nonlinear equations and inequations, the verification or synthesis problem quickly becomes undecidable and only very few solvers can deal with still decidable fragments by exact arithmetic. Such a decidable fragment is real algebra, i. e., polynomial arithmetic over the real numbers.

The goal of this research project is to adapt two procedures for solving systems of real algebraic equations and inequations, known from prominent results on decidability of the first order theory of real algebra, to work in a modern satisfiability-modulo-theories (SMT) solver: 1. the virtual substitution method (VS) and 2. the cylindrical algebraic decomposition method

(CAD). We already succeeded in creating a prototypic implementation of an SMT-solver based on the first method. Since VS is restricted to low-degree polynomials we also want to integrate CAD which comes without degree restrictions. Since CAD is a very complex stand-alone procedure unaware of any features needed in the SMT-context, its modification is still a challenging aspect of this project. First little improvements on the theoretical basis were developed and are currently being implemented for testing.

CEBug

E. Ábrahám, J.-P. Katoen, N. Jansen, J. Katelaan, M. Scheffler, M. Van de veire, B. Becker (Albert-Ludwigs-University Freiburg), R. Wimmer (Albert-Ludwigs-University Freiburg)

For the correction of erroneous systems it is crucial to have counter examples at hand.

Counterexamples are system runs which lead to erroneous behavior. Previous research on the analysis of stochastic systems concentrated on the computation of the probability with which runs of a stochastic system satisfy a given property. If this probability does not lie within the admissible bounds, the available model checking algorithms provide the probability value, but no counterexample. First steps towards counterexample generation for stochastic systems consider discrete-time Markov chains, a relatively simple class of stochastic systems. The goal of this project is, on the one hand, to improve the available technologies for counterexample generation and, on the other hand, to develop and implement algorithms for more expressive properties and for richer classes of systems. We are going to demonstrate the practical applicability of our algorithms on a set of benchmarks.

HySmart

E. Ábrahám, J. Giesl, C. Fuhs, N. Jansen, P. Csaba Ölveczky, M. Steffen, M. Fadlisyah, D. Lepri (last four from University of Oslo)

The aim of this project is to bring together researchers from the field of rewriting techniques on the one hand, and hybrid systems on the other hand, to develop new rewriting-based techniques for the modeling and analysis of advanced real-time and hybrid systems beyond the reach of existing formal tools.

The functionality of many modern advanced computer systems – such as medical devices, control systems, embedded automotive and avionics systems, Internet protocols, etc. – is crucially dependent on the amount of time that passes during or between events. Such real-time systems are often critical systems that must be well understood before deployment. The use of formal methods in the early stages of the system development process has been advocated in order to arrive at a precise yet high-level mathematical model of the design of a complex system. The formal model can then be subjected to different kinds of mathematical analysis – preferably machine-assisted or entirely automated – to find errors in the design

and/or to prove the design correct. Advanced real-time computer systems pose a challenge to modeling formalisms, in that different aspects, such as, e.g., real-time and probabilistic behavior, advanced communication and interaction features, complex and unbounded data types, etc., must be captured. The most popular formal tools for real-time systems (UPPAAL, Kronos, and HyTech) are based on timed or hybrid automata. While the restrictive specification formalism of these tools ensures that interesting properties are decidable, they do not support well the specification of larger systems with different communication models and advanced object-oriented features.

In joint work with José Meseguer at the University of Illinois, Ölveczky has developed the Real-Time Maude formalism and analysis tool. Real-Time Maude can be seen as complementing timed automaton-based formal tools by emphasizing ease and generality of specification, including support for distributed real-time object-based systems. As mentioned below, Real-Time Maude has been successfully applied to a wide range of complex state-of-the-art systems that cannot be modeled using the standard formal real-time tools.

Verification of hybrid systems based on reachability analysis

E. Ábrahám, X. Chen, S. Junges

Since the reachability problem for hybrid systems is not decidable, we overapproximate the exact reachable sets in the property verification work. A significant task is to compare the current overapproximation representations. Since different representations are adepted at different cases, combining them in reasonable ways can handle a wide class of systems, and improvements can be derived from such comparison.

Controller synthesis for hybrid systems. Given a hybrid system, we compute or approximate the least restrictive controller for it such that the safety of the combined system (the hybrid system and its controller) is guaranteed. The task normally is carried out by a procedure of backward analysis with underapproximation methods, and we also need to consider the case that the hybrid system is partially observable.

Other Activities

J.-P. Katoen

- Member of the Steering Committee of ETAPS (European Joint Conferences on Theory and Practice of Software).
- Member of the Steering Committee of FORMATS (Formal Methods and Analysis of Timed Systems)
- Member of the Steering Committee of QEST (Quantitative Evaluation of Systems).
- Member of the Steering Committee of ERCIM Working Group MQLA
- Board Member of the Dutch Society on Theoretical Computer Science (NVTI)
- Senior member of the Association of Computing Machinery (ACM)
- Member of the IFIP Working Group 1.8 on Concurrency Theory
- Member of the EPSRC Review College (Engineering and Physical Sciences Research Council), UK
- Co-organiser of the PhD School on Quantitative Model Checking, Copenhagen (DK)
- Member of several external PhD committees.

Member of the Program Committee of the following events:

- Messung, Modellierung und Bewertung (MMB)
- Tools and Algorithms for the Construction and Analysis of Systems (TACAS)
- Reachability Problems (RP)
- Quantitative Evaluation of Systems (QEST)
- Modeling and Verification of Parallel Processes (MOVEP)
- Numerical Solution of Markov Chains (NSMC)
- International Verification Workshop (Verify)
- Workshop on Quantitative Stochastic Models in the Verification and Design of Software Systems (QUOVADIS)
- Workshop on Tool Building in Formal Methods (TBFM)
- Symposium On Leveraging Applications of Formal Methods, Verification and Validation (ISOLA)

Invited speaker at:

- Verification, Model Checking, and Abstract Interpretation (VMCAI)
- IFIP WG 2.2 on Programming Concepts and Methodology
- Formal Methods for Components and Objects (FMCO)
- Formal Methods Week (FMWEEK)
- Modeling and Verification of Parallel Processes (MOVEP)
- 3rd Interaction and Concurrency Experience (ICE)
- Workshop on Modeling and Logics for Quantitative Analysis (MLQA)

Erika Ábrahám:

- Program committee member of the 1st International Workshop on Rewriting Techniques for Real-Time System (RTRTS)
- Program committee member of the 4th IEEE International Symposium on Theoretical Aspects of Software Engineering (TASE)
- Member of the CS Commission for School and Pupils
- Member of the CS Commission Honor Class
- Member of the CS Commission Bundeswettbewerb Informatik
- Speaker of the RWTH young scientists' group AixCYR
- Member of the Commission Gender Activities in the Graduate Research Schools

Co-organization of:

- Schüleruniversität
- Ringvorlesung Informatik
- Grünenthal Bionik Wettbewerb
- Die hellen Köpfe der Informatik
- Projekt Cybermentor
- Girls' Day

Thomas Noll:

- Program committee member of the 4th International Workshop on Harnessing Theories for Tool Support in Software (TTSS 2010)
- Program committee member of the 5th International Workshop on Systems Software Verification (SSV 2010)
- Program committee member of the 1st International Workshop on Rewriting Techniques for Real-Time System (RTRTS 2010)
- Program committee member of the 4th IEEE International Conference on Secure System Integration and Reliability Improvement (SSIRI 2010)
- Program committee member of the 8th International Workshop on Rewriting Logic and its Applications (ETAPS/WRLA 2010)
- Program committee member of the Software Engineering Track at the 25th Annual ACM Symposium on Applied Computing (SAC 2010)
- Member of the examination boards for CS Bachelor and Master (until April 2010)
- Student advisor for the following applied subjects within CS: Electrical Engineering, Civil Engineering, and Medicine
- Member of CS Commission for Teaching Service

Talks and Publications

Talks

Erika Abraham. SMT-Solving in the Verification and Synthesis of Hybrid Systems. Invited talk, Dagstuhl, Germany, 2010.

Erika Abraham. SMT-Solving for the Reals. Invited talk, University of Karlsruhe, Germany, 2010.

Erika Abraham. Tutorial on Satisfiability Checking. Tutorial, AlgoSyn meeting, Rolduc, Germany, 2010.

Erika Abraham. SMT-Solving in the Verification and Synthesis of Hybrid Systems. Invited talk, University of Freiburg, Germany, 2010.

Erika Abraham. Informatik ungleich Computer. Talk, Schüleruniversität Informatik, RWTH Aachen University, Germany, 2010.

Erika Abraham. Informatik ungleich Computer. Talk, Ringvorlesung "Was ist Informatik?" für Oberstufenschüler, RWTH Aachen University, Germany, 2010.

Erika Abraham. Informatik ungleich Computer. Talk, MINT Winter School, RWTH Aachen University, Germany, 2010.

Henrik Bohnenkamp. A gossiping MAC protocol and the Gupta/Kumar Radio Interference model. Talk, Autumn ROCKS Meeting, Dresden, Germany, 2010.

Henrik Bohnenkamp. GMAC and the Gupta/Kumar Radio Interference model. Talk, Quasimodo Meeting, Saarbruecken, 2010.

Henrik Bohnenkamp. Analyzing Energy Consumption in the MYRIANED Gossip MAC Protocol. Talk, Conference on "Measurement, Modelling and Evaluation of Computing Systems, Essen, Germany, 2010.

Marco Bozzano. The ESA COMPASS Project: Correctness, Safety and Performability of AADL Models for Aerospace Systems. Talk, MISSA-CISEC Workshop on Model-Based Safety Assessment, 2010. Workshop Presentation.

Christina Jansen. Generierung von Hyperkantenersetzungsgrammatiken zur Heapabstraktion. Talk, KPS, Maria Taferl, 2009.

Nils Jansen. DTMC Model Checking by SCC Reduction. Talk, QEST, 2010. Conference Presentation.

Nils Jansen. SCC-based Markov Chain Abstraction. Talk, ROCKS Meeting, Molenhoek, Netherlands, 2010. Presentation.

Nils Jansen. DTMC Model Checking by SCC Reduction. Talk, AlgoSyn Seminar, 2010. Presentation.

Joost-Pieter Katoen, and Marco Bozzano. Correctness, Safety and Performability of AADL Models: The COMPASS Project. Talk, ESA Final Presentation Days, 2010. Workshop Presentation.

Joost-Pieter Katoen. Advancements in Probabilistic Model Checking. Invited tutorial at VMCAI, Madrid, Spain, 2010.

Joost-Pieter Katoen. Quantitative Modeling and Model Checking. Tutorial at Dagstuhl Seminar on Quantitative Analysis of Network Protocols, 2010.

Joost-Pieter Katoen. Abstraction of Markov Chains: Useful for Queueing Networks?. Talk at Queueing Colloquium at CWI, Amsterdam, 2010.

Joost-Pieter Katoen. GSPN Semantics: Simpler is Impossible. Talk at Quasimodo Workshop, Paris, LIAFA, 2010.

Joost-Pieter Katoen. Model Checking Continuous-Time Markov Chains. Invited lecture at Spring School on Quantitative Model Checking, Copenhagen, Denmark, 2010.

Joost-Pieter Katoen. Quantitative Model Checking. Invited talk at Microsoft Workshop on Formal Methods for Predictable Embedded Systems, 2010. Aachen.

Joost-Pieter Katoen. Ubiquitous Model Checking. Kolloquium Universität Magdeburg, 2010.

Joost-Pieter Katoen. Abstraction of Markov Chains. Seminar at Microsoft CoSBI Laboratories, Trento, Italy, 2010.

Joost-Pieter Katoen. Concurrency, Interaction, Abstraction, and Randomness . Keynote talk at ICE'10 - 3rd Interaction and Concurrency Experience, Amsterdam, 2010.

Joost-Pieter Katoen. Model Checking Probabilistic Systems. Invited tutorial at Summerschool on Modeling and Verification of Parallel Processes (MOVEP'10), Aachen, 2010.

Joost-Pieter Katoen. Invariant Generation for Linear Probabilistic Systems. Invited talk at Workshop on Models and Languages for Quantitative Analysis, FLOC Workshop, Edinburgh, Scotland, 2010.

Joost-Pieter Katoen. The Theory and Practice of Interactive Markov Chains. Invited talk at IFIP WG 2.2. Workshop, Warsaw, Poland, 2010.

Joost-Pieter Katoen. Model Checking Continuous-Time Markov Chains. Five lectures at International Summerschool on Model Checking, Beijing, China, 2010.

Joost-Pieter Katoen. Quantitative Verification: A Practical Experience Report. Talk at International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISOLA'10), Heraclion, Crete, 2010.

Joost-Pieter Katoen. Ubiquitous Model Checking. Kolloquium at the University of Bremen, 2010.

Joost-Pieter Katoen. Analysis and Semantics of Extended AADL Models. Talk at IFIP 1.8 Workshop on Formal Methods for Embedded Systems, 2009.

Joost-Pieter Katoen. Reachability in Randomly Timed Games. Talk at Quasimodo Workshop at FMWeek 2009, 2009.

Joost-Pieter Katoen. Ubiquitous Model Checking. Invited Talk at FMWeek Soiree, TU Eindhoven, The Netherlands, 2009.

Ulrich Loup. Actuating Symbolically - A Case Study. Talk, AlgoSyn seminar, 2010.

Ulrich Loup. Tutorial on Abstract DPLL. Talk, AlgoSyn workshop, Rolduc, 2010.

Ulrich Loup. Tutorial on Decision Procedures for Real Algebra. Talk, AlgoSyn workshop, Rolduc, 2010.

Ulrich Loup. Tutorial on Quotations and BibTeX. Talk, Gemeinsamer Workshop der Informatik-Graduiertenkollegs und Forschungskollegs, 2010.

Ulrich Loup. Podcastproduktion als kollaborativer Zugang zur theoretischen Informatik. Talk, DeLFI, Duisburg, 2010.

Ulrich Loup. Podcast Production as Collaborative Access to Theoretical Computer Science. Talk, AlgoSyn seminar, 2010.

Viet Yen Nguyen. Performance Evaluation and Verification of System-Level Architecture Models. Talk at University of Oxford, 2010.

Viet Yen Nguyen. Formeel Modelleren en Analyseren van Ruimtevaartsystemen. Talk at Radboud University Nijmegen, 2010.

Viet Yen Nguyen. Slicing AADL Specifications for Model Checking. Talk at NASA Formal Methods Symposium (NFM 2010), 2010.

Viet Yen Nguyen. Model Checking Markov Chains using Krylov Subspace Methods: An Experience Report. Talk at EPEW 2010, 2010.

Thomas Noll. Interval Analysis of Microcontroller Code using Abstract Interpretation of Hardware and Software. Talk, 13th International Workshop on Software and Compilers for Embedded Systems (SCOPES 2010), 2010.

Thomas Noll. Formal Verification and Validation of AADL Models: The COMPASS Project. Talk, ESA Workshop on Avionics Data, Control and Software Systems (ADCSS 2009), 2009.

Maximilian R. Odenbrett: Slicing AADL specifications for model checking. Talk, MoVeP, Aachen, 2010.

Falak Sher. Abstraction and Refinement of Probabilistic Automata. Talk, Autumn ROCKS Meeting, Dresden, Germany, 2010.

Falak Sher. Abstraction and Refinement of Probabilistic Automata. Talk, YR CONCUR, Paris, 2010.

Sabrina von Styp. Towards a Theory for Timed and Symbolic Testing. Talk, Quasimodo Meeting, 2010.

Sabrina von Styp. A Conformance Testing Relation for Symbolic Timed Automata. Talk, FORMATS, 2010.

Sabrina von Styp. Towards a Theory for Timed Symbolic Testing. Talk, FM, 2009.

Publications

Alessandro Abate, Joost-Pieter Katoen, John Lygeros, and Maria Prandini. Approximate model checking of stochastic hybrid systems. European Journal of Control, 2010.

Erika Abraham. SAT-Modulo-Theories Solving in the Context of Bounded Model Checking. Invited talk, CWI Amsterdam, Amsterdam, The Netherlands, 2009.

Erika Abraham, and Ulrich Loup. SMT-Solving for the First-Order Theory of the Reals. In Algorithms and Applications for Next Generation SAT Solvers, Dagstuhl Seminar Proceedings. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany, 2009.

Erika Abraham, Nils Jansen, Ralf Wimmer, Joost-Pieter Katoen, and Bernd Becker. DTMC Model Checking by SCC Reduction . In 7th Int. Conf. on Quantitative Evaluation of Systems (QEST'10). IEEE CS Press, 2010.

Erika Abraham, Philipp Brauner, Nils Jansen, Thiemo Leonhardt, Ulrich Loup, and Ulrik Schroeder. Podcastproduktion als kollaborativer Zugang zur theoretischen Informatik. In Interaktive Kulturen — Die 8. E-Learning Fachtagung Informatik (DeLFI'10). Gesellschaft für Informatik, 2010.

Erika Abraham, Ulrich Loup, Florian Corzilius, and Thomas Sturm. A Lazy SMT-Solver for a Non-Linear Subset of Real Algebra. 8th International Workshop on Satisfiability Modulo Theories (SMT'10), 2010.

Erika Abraham, Ulrich Loup, Florian Corzilius, and Thomas Sturm. SMT-Solving in the Analysis and Synthesis of Hybrid Systems. In Verification over Discrete-Continuous Boundaries, Dagstuhl Seminar Proceedings. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany, 2010.

Erika Abraham, Ulrich Loup, Ralf Wimmer, and Joost-Pieter Katoen. On the Minimization of Hybrid Automata. In Nordic Workshop on Programming Theory (NWPT'10). 2010.

Christel Baier, Boudewijn R. Haverkort, Holger Hermanns, and Joost-Pieter Katoen. Performance Evaluation and Model Checking Join Forces. Communications of the ACM, 53(9):76-85, 2010.

Christel Baier, Lucia Cloth, Boudewijn R. Haverkort, Holger Hermanns, and Joost-Pieter Katoen. Performability Assessment by Model Checking of Markov Reward Models. Formal Methods in Systems Design, 36(1):1-36, 2010.

Benedikt Bollig, Joost-Pieter Katoen, Carsten Kern, and Martin Leucker. Learning Communicating Automata from MSCs. IEEE Transactions on Software Engineering, 36(3):390-408, 2010.

Benedikt Bollig, Joost-Pieter Katoen, Carsten Kern, and Martin Leucker. SMA: The Smyle Modeling Approach. Computing and Informatics, 29:45-72, 2010.

Benedikt Bollig, Joost-Pieter Katoen, Carsten Kern, Martin Leucker, Daniel Neider, and David Piegdon. libalf: the Automata Learning Framework. In Computer-Aided Verification (CAV). Pages 360-364. Volume 6174 of LNCS. Springer-Verlag, 2010.

Kai Bollue, Michaela Slaats, Erika Abraham, Wolfgang Thomas, and Dirk Abel. Synthesis of Behavioral Controllers for DES: Increasing Efficiency. In 10th Int. Workshop on Discrete-Event Systems (WODES'10). IFAC, 2010.

Marco Bozzano, Roberto Cavada, Alessandro Cimatti, Joost-Pieter Katoen, Viet Yen Nguyen, Thomas Noll, and Xavier Olive. Formal Verification and Validation of AADL Models. In Proc. Of Embedded Real Time Software and Systems Conf. (ERTS2 2010). 2010.

Marco Bozzano, Alessandro Cimatti, Joost-Pieter Katoen, Viet Yen Nguyen, Thomas Noll, and Marco Roveri. Safety, Dependability, and Performance Analysis of Extended AADL Models. The Computer Journal, doi: 10.1093/com, 2010.

Marco Bozzano, Alessandro Cimatti, Joost-Pieter Katoen, Viet Yen Nguyen, Thomas Noll, Marco Roveri, and Ralf Wimmer. A Model Checker for AADL. In Proc. of 22nd Int. Conf. on Computer Aided Verification (CAV 2010). pages 562-565. Volume 6174 of LNCS. Springer, 2010.

Jörg Brauer, Thomas Noll, and Bastian Schlich. Interval Analysis of Microcontroller Code using Abstract Interpretation of Hardware and Software. In Proc. 13th International Workshop on Software and Compilers for Embedded Systems (SCOPES 2010). Digital Library. ACM, 2010.

Jörg Brauer, Volker Kamin, Stefan Kowalewski, and Thomas Noll. Loop Refinement Using Octagons and Satisfiability. In Proc. Of 5th International Workshop on Systems Software Verification (SSV 2010). 2010.

Falko Dulat, Joost-Pieter Katoen, and Viet Yen Nguyen. Model Checking Markov Chains using Krylov Subspace Methods: An Experience Report. In Proceedings of 7th European Performance Engineering Workshop (EPEW 2010). LNCS. Springer, 2010.

Muhammad Fadlisyah, Erika Abraham, Daniela Lepri, and Peter Csaba Ölveczky. A Rewriting-Logic-Based Technique for Modeling Thermal Systems. In Proc. of the 1st Int. Workshop on Rewriting Techniques for Real-Time Systems (RTRTS'10). Electronic Proceedings in Theoretical Computer Science. 2010.

Muhammad Fadlisyah, Erika Abraham, and Peter Csaba Ölveczky. Rewriting-Logic-Based Formal Modeling and Analysis of Interacting Hybrid Systems. In Proc. of the Nordic Workshop on Programming Theory (NWPT'10). 2010.

Muhammad Fadlisyah, Peter Csaba Ölveczky, and Erika Abraham. Adaptive-Step-Size Numerical Methods in Rewriting-Logic-Based Formal Analysis of Interacting Hybrid Systems. In Int. Workshop on Harnessing Theories for Tool Support in Software (TTSS'10). ENTCS. 2010.

Markus Geimer, Felix Wolf, Brian J. N. Wylie, Erika Abraham, Daniel Becker, and Bernd Mohr. The Scalasca Performance Toolset Architecture. Concurrency and Computation: Practice and Experience, 22(6):702-719, 2010.

Holger Hermanns, and Joost-Pieter Katoen. The How and Why of Interactive Markov Chains. In Formal Methods for Components and Objects (FMCO). pages 311-337. Volume 6286 of LNCS. Springer-Verlag, 2010.

Marijn R. Jongerden, Alexandru Mereacre, Henrik Bohnenkamp, Boudewijn R. Haverkort, and Joost-Pieter Katoen. Computing Optimal Schedules for Battery Usage in Embedded Systems. IEEE Transactions on Industrial Informatics, 6(3), 2010.

Natalia Kalinnik, Erika Abraham, Tobias Schubert, Ralf Wimmer, and Bernd Becker. Exploiting Different Strategies for the Parallelization of an SMT Solver. In Proc. of 13. Workshop Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen (MBMV'10). 2010.

Joost-Pieter Katoen. Advances in Probabilistic Model Checking. In Verification, Model Checking, and Abstract Interpretation (VMCAI). pages 25-25. Volume 5944 of Lecture Notes in Computer Science. Springer-Verlag, 2010.

Joost-Pieter Katoen, Jaco van de Pol, Marielle Stoelinga, and Mark Timmer. A Linear Process Algebraic Format for Probabilistic Systems with Data. In Applications of Concurrency to System Design (ACSD). IEEE CS Press, 2010.

Joost-Pieter Katoen, Annabelle McIver, Larissa Meinicke, and Carroll Morgan. Linear-Invariant Generation for Probabilistic Programs. In Static Analysis Symposium (SAS). pages 390-406. Volume 6337 of LNCS. Springer-Verlag, 2010.

Joost-Pieter Katoen, Ivan S. Zapreev, E. Moritz Hahn, Holger Hermanns, and David N. Jansen. The Ins and Outs of the Probabilistic Model Checker MRMC. Performance Evaluation, , 2010.

Daniel Klink. Three-Valued Abstraction for Stochastic Systems. PhD Thesis, RWTH Aachen University, 2010.

Daniel Klink, Anne Remke, Boudewijn R. Haverkort, and Joost-Pieter Katoen. Time-Bounded Reachability in Tree-Structured QBDs by Abstraction. Performance Evaluation, , 2010.

Daniela Lepri, Peter Csaba Ölveczky, and Erika Abraham. Model Checking Classes of Metric LTL Properties of Object-Oriented Real-Time Maude Specifications. In Proc. of the 1st Int. Workshop on Rewriting Techniques for Real-Time Systems (RTRTS'10). Electronic Proceedings in Theoretical Computer Science. 2010.

Angelika Mader, Henrik Bohnenkamp, Yaroslav S. Usenko, David N. Jansen, Johann Hurink, and Holger Hermanns. Synthesis and Stochastic Assessment of Cost-Optimal Schedules. Software Tools for Technology Transfer, 12(5):305-318, 2010.

Martin R. Neuhäußer. Model Checking Nondeterministic and Randomly Timed Systems. PhD Thesis, RWTH Aachen University and University of Twente, 2010.

Martin R. Neuhaußer, and Lijun Zhang. Time-Bounded Reachability Probabilities in Continuous-Time Markov Decision Processes. In Quantitative Evaluation of Systems (QEST). IEEE CS Press, 2010.

Maximilian R. Odenbrett, Viet Yen Nguyen, and Thomas Noll. Slicing AADL Specifications for Model Checking. In Proc. of the 2nd NASA Formal Methods Symp. (NFM 2010). pages 217-221. NASA Conference Proceedings. 2010.

Sabrina von Styp. Towards a theory for timed symbolic testing. In Proceedings of Formal Methods 2009 Doctoral Symposium. pages 39-45. Volume 09-15 of CS-Report. Technical University Eindhoven, 2009.

Sabrina von Styp, Henrik Bohnenkamp, and Julien Schmaltz. A Conformance Testing Relation for Symbolic Timed Automata. In Proc. FORMATS 2010. Volume 6246 of LNCS. Springer-Verlag, 2010.

Haidi Yue, Henrik Bohnenkamp, and Joost-Pieter Katoen. Analyzing Energy Consumption in a Gossiping MAC Protocol . In Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance (MMB/DFT). pages 107-119. Volume 5987 of LNCS. Springer-Verlag, 2010.

Haidi Yue, and Joost-Pieter Katoen. Leader Election in Anonymous Radio Networks: Model Checking Energy Consumption. In 17th International Conference on Analytical and Stochastic Modelling Techniques and Applications (ASMTA). pages 247-261. Volume 6148 of LNCS. 2010.

Lijun Zhang, and Martin R. Neuhäußer. Model Checking Interactive Markov Chains. In Proceedings of the 16th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS). pages 53-68. Volume 6015 of Lecture Notes in Computer Science. Springer, 2010.

Technical Reports

Taolue Chen, Tingting Han, Joost-Pieter Katoen, and Alexandru Mereacre. Computing Maximum Reachability Probabilities in Markovian Timed Automata. Technical Report AIB-2010-06, Computer Science Department, RWTH Aachen University, 2010.

Martin R. Neuhäußer, and Lijun Zhang. Time-Bounded Reachability in Continuous-Time Markov Decision Processes. Technical Report 2009-12, RWTH Aachen, Department of Computer Science, 2009.