Chapitre 1

Detailed scientific report : TEMPO team

Members

Team leader : Oded Maler, DR2 CNRS
Permanent members :
- Thao Dang, CR1 CNRS
- Goran Frehse, MdC UJF

Non permanent members :
- Goran Frehse, post-doc, UJF (10/2005-09/2006)
- Anoine Girard, post-doc, INP (10/2005-09/2006)
- Gregory Batt, post-doc UJF (10/2006-09/2007)
- Victor Schuppan, post-doc CNRS (10/2007-06/2008)
- Ramzi Ben Salah, post-doc, UJF
- Alexandre Donzé, post-doc, CNRS
- Noa Shalev, engineer, UJF
- Gabriel Vincent, technician, UJF

PhD Students :
- Abdelkarim Kerbaa, (defended 10/2006)
- Alexandre Donzé, (defended 06/2007)
- Ramzi Ben Salah, (defended 10/2007)
- Tarik Nahhal, (defended 10/2007)
- Dejan Nickovic (defended 10/2008)
- Scott Cotton
- Colas Le Guernic
- Aldric Degorre
- Julien Legriel
- Rajarshi Ray
- Jean-Francois Kempf
- Selma Saidi

Visitors :
- Avshalom Elitzur, invited professor, UJF (02/2008-04/2008)
- Nir Piterman, invited DR, CNRS (10/2008-12/2008)

1.1 General presentation

The group's focus can be characterized as *model-based analysis of systems* in the large sense without a priori attachment to a specific application domain. We are interested in phenomena that can be modeled as *dynamical systems* of various sorts that can benefit from analysis techniques originating from the domain of formal verification. The main thrust of the group is to bring these techniques to domains where the they are not known, to modify and extend them to fit the needs of these new domains while paying a special attention to the problem of scaling up, in order to be able to eventually treat systems which are not toy. The activities of the group can be roughly classified into two major categories : 1) *Hybrid Systems* : analysis of systems that admit *numerical state variables*, such as continuous dynamical systems defined by differential equations, discrete-time systems or hybrid automata ; 2) *Timed systems* : analysis of discrete systems where *quantitative timing information*, such as execution times or propagation delays, is represented explicitly. The group exhibits international excellence and leadership in this domain by having initiated some of the research directions, by participating in and leading international projects and by organizing international conferences.

1.2 Hybrid Systems

Analyzing the potential behaviors of dynamical models is a fundamental activity in both science and engineering. System models typically admit many behaviors depending on variations in initial states, environmental contexts, parameters and other modeling uncertainties. In finite-state systems this phenomenon is instantiated by a huge transition graph where paths in the graph correspond to behaviors induced by different input sequences. One way to analyze such an open/uncertain system is to sample the space of possible behaviors by *simulating* the system against a finite and non-exhaustive set of input sequences. Conclusions about correctness or other performance criteria based on such tests cannot be sound in the mathematical sense but are sometimes the best one can hope for many large real-life systems. Algorithmic verification (model checking) suggests an alternative and exhaustive way to analyze all behaviors of finite-state systems by conduction a set-based "breadth-first" simulation. The extension of these ideas to systems with state variables ranging over infinite (or just very large) domains is the major problem in software verification. Most of our work in the domain is concerned with the application of these insights to the analysis of *continuous* and *hybrid* dynamical systems. In addition we initiated two new research directions in this domain : *conformance testing* which shares some techniques with simulation-based validation and *monitoring* which provides means to specify desired extended temporal properties and check whether system trajectories satisfy them.

1.2.1 Continuous and Hybrid Verification

Computing reachable sets, or *set-based* numerical integration, is the direct adaptation of algorithmic formal verification to the continuous and hybrid domain. Our group is among the pioneers in this line of work and plays in important role in disseminating its principles and results in verification [ADF+06, DFGG08, Fre09, TD09] and synthesis which generalizes the verification into a two-payer game and can be solved using extended variants of verification techniques [Mal07]. Other directions of attack use techniques based on simulation of single trajectories.

Reachability for Linear Hybrid Automata Linear Hybrid Automata (LHA) are the simplest type of hybrid systems where the evolution of continuous variables is linear in each discrete state. They remain of interest as their behavior can be described and analyzed precisely using polyhedra, and interesting properties (such as the feasibility of a particular path) can be solved using linear programming. We have improved and extended corresponding analysis techniques, in particular as part of our work on CEGAR [FJK08]. A key component is that some of our over approximation techniques act as widening operators and accelerate termination [MFK09].

Reachability for Linear Systems Linear systems, where the dynamics is defined by linear differential equations are the most commonly studied in math and engineering. Our verification techniques allow to analyze their transient behavior (not only steady-state) and take into account nondeterminism due to parameters,

environment of initial condition. The paper [GLM06] was a major breakthrough in reachability computation for systems defined by linear differential equations. Prior to this work, verification tools could analyze systems with very few state variables. The algorithm presented in this paper combined the use of *zonotopes* to represent the reachable states in a semi-symbolic manner and a new algorithmic scheme based on the sharing of many terms in the representation of successive sets, systems with hundreds of state variables could be analyzed. The next step was the extension to hybrid automata by an efficient algorithm for zonotope/hyperplance intersection [GL08b] which has led later to series of works using *support functions* as a general symbolic representation [GL08a, LGG09b, LGG09a] which provides for easy-to-compute approximations which are tight in selected directions.

Reachability for Nonlinear Systems The real challenge in many application domains is to treat systems with nonlinear dynamics. Our efforts in adapting reahcability computation to this domain included the use of new types of geometric objects adapted to polynomial systems such as Bezier simplices [Dan06], Bernstein expansions [DS09] and box splines [Dan09], the approximation multi-linear systems by timed automata [MB08] and the use of template polyhedra whose inequalities have fixed expressions but with varying constant terms. Set operations such as intersection, union and post-condition (image) across discrete transitions over template polyhedra can be computed efficiently without using expensive vertex enumeration. For set integration, we use higher-order Taylor series approximations along with repeated optimization problems to bound the terms in the Taylor series expansion [SDI08a, SDI08b]. An alternative line of attack on nonlinear systems is general technique of *hybridization* [ADG07] which transforms *any* nonlinear system into a hybrid automaton with a different linearization of the dynamics in each state. This technique is based on partitioning the state space into a mesh of linearization domains and guarantees a conservative approximation of the reachable set and good convergence to the original nonlinear system as the mesh size decreases. Recently a new version of hybridization, based on overlapping linearization domains, has been used to analyze nonlinear models with up to 9 state variables [DGM09].

Abstraction Technique The use of abstractions and compositional reasoning to tackle the state explosion problem was investigated in [Fre06] where a simulation relation between a complex component was computed. To overcome some inherent problems in this approach we shifted our attention to generating abstractions as part of the analysis itself. *Counterexample guided abstraction refinement* (CEGAR) automatically refines an abstraction using spurious counterexamples and in [FJK08] we extended it to hybrid systems and to parameter synthesis. *Predicate abstraction* is a powerful technique for extracting finite-state models from infinite-state discrete programs. We have extended it for hybrid system by computing finite discrete quotient with based on the satisfaction of user-provided predicates. The algorithm of [ADI06b]. performs an on-the-fly exploration of the abstract system. In [ADI06a] we focused on identifying such predicates automatically by analyzing spurious counter-examples generated by the search in the abstract state-space. We developed a number of techniques for discovering new predicates that will rule out closely-related spurious counter-examples, implemented them and demonstrating the promise of the approach on case studies.

Simulation-based Approaches Simulation which will always remain an important part of the evaluation process for large and complex systems can be made more rigorous and systematic by improving and guaranteeing its coverage of the space of trajectories. *Sensitivity analysis* is the study of how the behaviors of a dynamical systems depends on its initial conditions and parameters. Efficient techniques exist to provide local sensitivity information around simulated trajectories with a small overhead in the computational cost. In [DM07], we observed that this information could be used to estimate reachable sets for nonlinear and hybrid systems using a finite number of numerical simulations. Thus it can be applied for systems with a high number of state variables, due to the scalability of simulation, and is limited only by the number of uncertain parameters. This technique was further developed in [Don07] and applied in particular to nonlinear oscillating analog circuits. In [DKR09] it was extended to work on Simulink models of embedded systems and in [DCLL09] it was applied to biological models from immunology. These ideas have been used for statistical model checking [CDL08, CDL09]. For the hard problem of sampling the input space we proposed a combination with the exploration technique technique described in Section 1.2.2 [DMS08].

The existence of metrics on the system state space, which is natural for continuous and hybrid systems, allows us to capitalize on the recently developed concept of *bisimulation metrics* and infer all the possible behaviors of the system in a neighborhood of a simulated trajectory. Hence, by a finite number of simulations one can produce results as strong as those obtained by exhaustive verification, such as deciding whether the systems is correct for all initial state and parameter value [FGP06]. Besides verification, bisimulation and behavioral metrics have been applied to the validation of embedded controllers implementation [NPGA06] and to hierarchical control synthesis for continuous systems [GP06].

Verification Tool Development We have implemented various techniques for verifying linear hybrid automata in an open-source tool called PHAVer [Fre08]. While we are not tracking downloads, we have received feedback from users in academic research and education, and even some in industry, for example : EDF R&D, General Motors India Science Lab - Bangalore (India), LAG - Grenoble, IRCCYN - Nantes, Carnegie Mellon University - Pittsburgh (USA), University of Pennsylvania - Philadelphia (USA), Columbia University - NY (USA), MIT - Boston (USA), RWTH Aachen (Germany), University of Braunschweig (Germany), University of Freiburg (Germany), University of Oldenburg (Germany), University of Paderborn (Germany), Max-Planck-Institut fur Informatik - Saarbruecken (Germany), University of Innsbruck (Austria), Hefei University of Technology (China), University of Verona (Italy), Instituto Militar de Engenharia - Rio de Janeiro (Brazil), IIT Mumbai (India), Tata Institute of Fundamental Research - Mumbai (India), University of Technology - Eindhoven (Netherlands), Aristotle Univeristy of Thessaloniki (Greece).

In addition we have developed prototype tools for novel techniques such as reachability using zonotopes and verification using sensitivity. To preserve and disseminate all this intellectual property we are currently developing a tool platform to implement our recent verification techniques for hybrid systems, and a report on the first version of the tool is being published [FR09]. In an effort to learn from our previous tool developments, the platform is designed to provide the basic infrastructure *common* to all our reachability algorithms and offer interfaces that allow us substitute different components such as set representations (polyhedra, zonotopes), time elapse algorithms or state exploration techniques. Our goal is to facilitate the implementation of new algorithms as well as the combination of different approaches into heterogenous algorithms (such as combining corner case simulation with set-based reachability).

1.2.2 Conformance Testing

Conformance testing provides a means to assess the correctness of an implementation with respect to a specification by performing experiments on the implementation and observing its responses. Extending classical model-based testing frameworks for discrete systems (such as digital circuits, communication protocols and software) to hybrid systems is particularly challenging, due to the infinite state and input spaces. We proposed a framework for conformance testing of hybrid systems, defined according to the international standard for formal conformance testing FMCT. It enabled us, on one hand, to formally reason about the conformance relation between a system under test and a specification, and on the other hand, to develop test generation algorithms [ND07a, ND07b]. We also proposed a novel test coverage measures based on geometric discrepancy notion [ND07b]. Our test generation algorithm is based on the RRT (Rapidly-exploring Random Tree) algorithm developed in the context of robotics motion planning, and guided by the coverage measure. Besides, we introduced a new notion of disparity between two point sets, in order to tackle "blocking" situations the RRT algorithms may enter [DN08]. We have implemented a tool for conformance testing of hybrid systems, called **HTG** and treated a number of case studies from control applications as well as analog and mixed signal circuits. The experimental results demonstrated that the tool **HTG** is applicable to systems with high dimensional systems with complex dynamics [DN09].

1.2.3 Monitoring

Monitoring (also known as *runtime verification* in the software context) is the process of checking whether *individual* behaviors (simulation traces) satisfy a temporal property expressed in a high-level formalism. Within the PROSYD project we have pioneered the extension of this methodology to systems whose behaviors are continuous or hybrid signals. To this end we have defined an extension of temporal logic (Signal Temporal Logic,

STL) which combines the dense-time logic MITL with static numerical predicates. We have then developed two monitoring procedures (offline and online) which handle the dense time aspects (see Section 1.3.3) and also treats the fact that continuous signals are represented by sampling points and other pragmatic issues [MNP08]. After having solved the semantic and algorithmic issues we have implemented a full-fledged tool (Analog Monitoring Tool, AMT [NM07]) that goes all the way from STL specification to monitoring signals which are given in various common formats or produced on-the-fly by numerical simulators such as Simulink or SPICE. The tool has generated a lot of spontaneous interest in the semiconductor and EDA industry and has undergone evaluation in Freescale, Rambus and Mentor Graphics. The logic STL plays a central role in the current discussions about extending the industrial-standard assertion language SVA toward analog and mixed-signal systems (AMS).

1.2.4 Applications

The hybrid analysis techniques developed in our group has been applied to problems and case studies from the following application domains.

Embedded Systems In [Dan05] we have applied reachability analysis to a model of automotive idle speed controller. In [DKR09], the simulation-based approach using sensitivity analysis has been applied to a models of a new type of helicopter designed with Simulink, a tool widely used in the industry. In [FM07] it was shown how linear hybrid automata can be used to model and analyze in a compositional manner networks of interconnected buffers. In [KLD$^+$08] we investigated the use of bisimulation functions for nonlinear systems (computed using sum of square programming) in conjunction with the JavaPathFinder model checker to verify continuous systems under the supervision of a discrete control program.

Analog and Mixed-Signal Circuits Verification of analog and mixed-signal circuits is a promising and challenging domain for hybrid verification techniques [Mal06]. In [CDL08, CDL09], a simulation-based probabilistic approach has been used to analyze the stability of discrete-time models of Delta-Sigma modulators, a family of analog to digital converters. The analog monitoring tool has been applied to a FLASH memory specification provided by STM [NM07] and to a DDR memory model provided by Rambus [JKN09]. Oscillation properties were formalized and verified against simplified circuit models in [FKRM06]. We have applied the test generation tool to a number of benchmark circuits, in particular the Delta-Sigma circuit,the diode bridge oscillator and the VCO circuit, described by a system of differential algebraic equations with 54 variables [DN08] .

Systems Biology Biochemical reactions are typically modeled using nonlinear differential equations with state variables representing concentrations and possibly with discrete transitions that model events such as gene activation. The abstraction technique of [MB08] was used to analyze a synthetic gene network, the cascade of transcriptional inhibitions built in E.coli. The dynamic hybridization method of [DGM09] has been applied to a model of the *lac operon* of E.Coli and to a model based on mitochondrial aging theory. In [DCLL09], the sensitivity-based approach has been used for parameter synthesis in models of the acute inflamatory response to a pathogen infection.

Other Applications In [Don05] the technique of reinforcement learning for optimal control was extended to continuous and hybrid systems and applied to problems in robotics. In [MFK09] we found bounds on errors due to floating point computations for programs with linear operators (no multiplication of variables) that can be modeled by a subclass of linear hybrid automata that admit more efficient analysis.

1.3 Timed Systems

The simplest way to characterize timed systems is as those represented by models similar to timed automata or other transition systems with clocks. This description, however, does some injustice to their importance. Timed systems represent an intermediate level of abstraction between continuous systems where processes are represented physically and quantitatively and discrete models where the information is purely qualitative. Timed models view the world as discrete processes that take some *quantitative time* to be completed. Such models

are used extensively in everyday life and form a basis to all our planning and scheduling activities. In the development of embedded systems they can be used for high level modeling of software and hardware components, abstracting away from actual code or hardware details, and modeling only execution times, durations, delays and input frequencies. They can thus serve for performance evaluation, either by exhaustive methods inspired by verification or by providing a basis for fast simulation and design space exploration. Our work in this domain consisted of developing general solution approaches to scheduling problems, in trying to fight the clock explosion problem in the analysis of timed automata, in studying theoretical aspects of real-time logics, timed automata and timed languages and in developing fast solvers for timing-related constraint satisfaction problems.

1.3.1 Scheduling and Synthesis

The paper [AAM06] summarizes our work on modeling and solving scheduling problems using timed automata. It shows that, for deterministic problems, finding shortest paths in timed automata is not better nor worse than other techniques for this NP-hard problem. For scheduling under temporal uncertainty, a strategy synthesis algorithm can produce adaptive schedules with very attractive features but the technique does not scale up. In [DG06] a geometric approach to scheduling multi-threaded programs has been developed using ideas form obstacle avoidance in robotic motion planning. The problem of synthesizing schedulers from the bounded fragment of the real-time logic MITL was solved in [MNP07]. In [DM08] we have defined a new dynamic model of recurrent scheduling where a request generator sends streams of structured jobs to be executed on a parallel execution platform and proved some basic results on scheduling strategies and pipelining. The handbook chapter [CM05] deals with real-time scheduling in the larger context of implementing control systems on computers. Our involvement in the ATHOLE project on multicore scheduling is currently the driving force behind the scheduling activity leading us to explore new variants of scheduling problems that involve multi-criteria optimization and use solution techniques based on SMT solvers [LM09].

1.3.2 Improving Timed Automata Technology

Verification of timed automata is notoriously difficult and for this reason it has not been used outside academic circles. In [BBM06] we have made an important contribution by removing *some* of the state explosion due to interleaving by observing that the union of zones reached by different interleavings of the same set of actions is convex, and by implementing a breadth-first exploration algorithm that takes advantage of this fact. Most of our efforts were directed at developing a novel abstraction technique for networks of timed components that preserves their observable qualitative semantics, over-approximates their timed semantics while reducing the number of clocks and states [BBM07b, Ben07, BBM09]. This technique, which can underly a compositional approach to performance anaysis, has been implemented into the IF toolbox. We have also shown that timed components can be used to add quantitative timing information to discrete models of genetic regulatory networks [BBM07a].

1.3.3 Real-Time Logics, Timed Automata and Timed Languages

As part of the work on monitoring temporal properties of continuous signals described in Section 1.2.3 we have developed a monitoring technique for the real-time logic MITL [MNP08] which led us to better understanding of the relation between the future and past fragments of the logic and deterministic timed automata [MNP05] and finally to a new modular translation procedure into timed automata based on the notion of timed temporal testers [MNP06, Nic08]. In [AD09b, AD09a] a new theory concerning the *volume* and *entropy* of timed languages has been developed, including algorithms for computing these measures from timed automata. These results have potential applications in information theory and in evaluating the quality of language approximations produced by timed abstraction techniques. Other investigation in quantitative aspects of formal languages were investigated in [ADMW09].

1.3.4 SAT and SMT Solving

Recent progress in Boolean satisfiability (SAT) solvers opened new horizons for solving constraint satisfaction and constrained optimization problems. The domain of SAT modulo theories (SMT) attempts to provide

satisfiability solvers (and decision procedures in general) for problems where propositions are inter mixed with constraints coming from various logical theories. For the theory of difference constraints of the form $x - y < c$, which are the fundamental constraints for scheduling problems, the algorithm of [CM06] is currently recognized as the most efficient and is implemented in leading SMT solvers. It has been recently used to solve a previously-unsolved job-shop scheduling problem. A radically-new approach for treating numerical variables directly as the objects of search for assignments has been proposed and implemented, for the theory of linear inequalities, in [Cot09] with a lot of potential applications in solving hard constraint optimization problems.

1.4 Projects and contracts

1.4.1 Onging Projects

- *Hybrid Models of Biological Systems*
  - Topic : developing hybrid system techniques for analyzing cancer-related pathways
  - Finance : French-Israeli Bioinformatics program
  - Partners : Weizmann Institute
  - Sum and duration : 50KEuro 2007-2009
  - Responsible : O. Maler
- *ATHOLE*
  - Topic : programming, mapping, scheduling and performance evaluation for stream-processing applications on low-power multicore processors
  - Finance : Minalogic
  - Partners : STM, CEA-LETI, Thales, CWS
  - Sum and duration : 830KEuro 2007-2010
  - Responsible : O. Maler
- *VAL-AMS*
  - Topic : validation and simulation of analog circuits
  - Finance : ANR
  - Partners : INRIA
  - Sum and duration : 108KEuro 2007-2009
  - Responsible : T. Dang
- *MULTIFORM*
  - Topic : verification platform for hybrid systems
  - Finance : Europe
  - Partners : Eindhoven, Dortmund, Aalborg, Aachen, CWI, VEMAC, CVCA
  - Sum and duration : 246KEuro 2009-2012
  - Responsible : G. Frehse

1.4.2 Terminated

- *CC*
  - Topic : verification and control for hybrid systems
  - Finance : Europe
  - Partners : ETH, CWI, Lund, Parades, EDF, ABB
  - Sum and duration : 509KEuro 2002-2005
  - Responsible : O. Maler (coordinator)
- *AMETIST*
  - Topic : timed automate and scheduling
  - Finance : Europe
  - Partners : Dortmund, Aalborg, Nijmegen, Twente, LIF, Axxom, Terma
  - Sum and duration : 271KEuro 2002-2005
  - Responsible : O. Maler
- *DECIDE!*

  - Topic : constraints and verification
  - Finance : RNTL
  - Partners : ILOG
  - Sum and duration : 197KEuro 2006-2008
  - Responsible : O. Maler
- *CORTOS*
  - Topic : control Synthesis
  - Finance : ACI CNRS
  - Partners : IRCCyN, LSV
  - Sum and duration : 25KEuro 2007-2008
  - Responsible : T. Dang

1.5 Production

Bibliographie

[AAM06] Yasmina Abdeddaïm, Eugene Asarin, and Oded Maler. Scheduling with timed automata. *Theor. Comput. Sci.*, 354(2) :272–300, 2006.

[AD09a] Eugene Asarin and Aldric Degorre. Volume and entropy of regular timed languages : Analytical approach. In *FORMATS*, 2009.

[AD09b] Eugene Asarin and Aldric Degorre. Volume and entropy of regular timed languages : Discretization approach. In *CONCUR*, 2009.

[ADF+06] Eugene Asarin, Thao Dang, Goran Frehse, Antoine Girard, Colas Le Guernic, and Oded Maler. Recent progress in continuous and hybrid reachability analysis. In *CACSD 2006*, pages 1582–1587. IEEE, October 2006.

[ADG07] Eugene Asarin, Thao Dang, and Antoine Girard. Hybridization methods for the analysis of nonlinear systems. *Acta Inf.*, 43(7) :451–476, 2007.

[ADI06a] R. Alur, T. Dang, and F. Ivancic. Counter-example guided predicate abstraction of hybrid systems. *Theoretical Computer Science (TCS)*, 354(2) :250–271, 2006.

[ADI06b] R. Alur, T. Dang, and F. Ivancic. Reachability analysis of hybrid systems via predicate abstraction. *ACM transactions on embedded computing systems (TECS)*, 354(2) :250–271, 2006.

[ADMW09] Rajeev Alur, Aldric Degorre, Oded Maler, and Gera Weiss. On omega-languages defined by mean-payoff conditions. In *FOSSACS*, pages 333–347, 2009.

[BBM06] Ramzi Ben Salah, Marius Bozga, and Oded Maler. On interleaving in timed automata. In *CONCUR 2006*, volume 4137 of *LNCS*, pages 465–476. Springer, 2006.

[BBM07a] Grégory Batt, Ramzi Ben Salah, and Oded Maler. On timed models of gene networks. In *FORMATS*, volume 4763 of *Lecture Notes in Computer Science*, pages 38–52. Springer, 2007.

[BBM07b] Ramzi Ben Salah, Marius Bozga, and Oded Maler. On timed components and their abstraction. In *SAVCBS '07 : Proceedings of the 2007 conference on Specification and verification of component-based systems*, pages 63–71, New York, NY, USA, 2007. ACM.

[BBM09] Ramzi Ben Salah, Marius Bozga, and Oded Maler. Compositional timing analysis. submitted to EMSOFT 2009, 2009.

[Ben07] Ramzi Ben Salah. *On Timing Analysis of Large Systems.* PhD thesis, INP Grenoble, October 2007.

[CDL08] Edmund M. Clarke, Alexandre Donzé, and Axel Legay. Statistical model checking of mixed-analog circuits with an application to a third order delta-sigma modulator. In *Haifa Verification Conference*, volume 5394 of *Lecture Notes in Computer Science*, pages 149–163. Springer, 2008.

[CDL09] Edmund M. Clarke, Alexandre Donzé, and Axel Legay. Statistical model checking of mixed-analog circuits with an application to a third order delta-sigma modulator. *Formal Methods in System Design*, 2009.

[CM05] Paul Caspi and Oded Maler. From control loops to real-time programs. In *Handbook of Networked and Embedded Control Systems*, pages 395–418. Birkhäuser, 2005.

[CM06] Scott Cotton and Oded Maler. Fast and flexible difference constraint propagation for DPLL(T). In *SAT 2006*, volume 4121 of *LNCS*, pages 170–183. Springer, 2006.

[Cot09] Scott Cotton. *On Some Problems in Satisfiability Solving*. PhD thesis, University Joseph Fourier, 2009.

[Dan05] Thao Dang. A reachability-based technique for idle speed control synthesis. *International Journal of Software Engineering and Knowledge Engineering*, 15(2) :397–404, 2005.

[Dan06] Thao Dang. Approximate reachability computation for polynomial systems. In *HSCC 2006*, pages 138–152, 2006.

[Dan09] Thao Dang. Using box splines to approximate reachable sets of polynomial systems. In *Numerical Software Verification NSV-II*, 2009.

[DCLL09] A. Donzé, G. Clermont, C. J. Langmead, and A. Legay. Parameter synthesis in nonlinear dynamical systems : Application to systems biology. In *Proceedings of the 13th Annual International Conference on Research in Computational Molecular Biology RECOMB'09*, LNBI. Springer-Verlag, May 2009.

[DFGG08] Thao Dang, Goran Frehse, Antoine Girard, and Colas Le Guernic. Outils pour l'analyse des modèles hybrides. In Olivier Roux and Claude Jard, editors, *Approches formelles des systèmes embarqués communicants*, Traité IC2, série Informatique et systèmes d'information, pages 245–268. Hermes Lavoisier, 2008.

[DG06] T. Dang and Ph. Gerner. Scheduling for multi-threaded real-time programs via path planning. In S. L. Min and W. Yi, editors, *Proceedings of the 6th ACM & IEEE International conference on Embedded software, EMSOFT 2006*. ACM, 2006.

[DGM09] Thao Dang, Colas Le Guernic, and Oded Maler. Computing reachable states for nonlinear biological models. In *CMSB*, 2009.

[DKR09] A. Donzé, B. Krogh, and A. Rajhans. Parameter synthesis for hybrid systems with an application to simulink models. In *Proceedings of the 12th International Conference on Hybrid Systems : Computation and Control (HSCC'09)*, LNCS. Springer-Verlag, April 2009.

[DM07] Alexandre Donzé and Oded Maler. Systematic simulation using sensitivity analysis. In *HSCC*, volume 4416 of *LNCS*, pages 174–189, 2007.

[DM08] Aldric Degorre and Oded Maler. On scheduling policies for streams of structured jobs. In *FORMATS*, pages 141–154, 2008.

[DMS08] Thao Dang , Alexandre Donzé, Oded Maler, and Noa Shalev. Sensitive state space exploration. In *IEEE Conference on Decision and Control (CDC)*, dec 2008.

[DN08] Thao Dang and Tarik Nahhal. Using disparity to enhance test generation for hybrid systems. In *TestCom/FATES 2008*, LNCS, pages 54–69. Springer, 2008.

[DN09] Thao Dang and Tarik Nahhal. Coverage-guided test generation for continuous and hybrid systems. *Formal Methods in System Design*, 2009.

[Don05] Alexandre Donzé. On temporal difference algorithms for continuous systems. In *ICINCO*, pages 55–62. INSTICC Press, 2005.

[Don07] A. Donzé. *Trajectory-Based Verification and Controller Synthesys for Continuous and Hybrid Systems*. PhD thesis, University Joseph Fourier, June 2007.

[DS09] Thao Dang and David Salinas. Image computation for polynomial dynamical systems using the bernstein expansion. In A. Bouajjani and O. Maler, editors, *Computer Aided Verification CAV'09*, LNCS, pages 277–287. Springer, 2009.

[FGP06] Georgios E. Fainekos, Antoine Girard, and George J. Pappas. Temporal logic verification using simulation. In *FORMATS*, volume 4202 of *LNCS*, pages 171–186, 2006.

[FJK08] Goran Frehse, Sumit Kumar Jha, and Bruce H. Krogh. A counterexample-guided approach to parameter synthesis for linear hybrid automata. In *HSCC*, LNCS. Springer, 2008.

[FKRM06] Goran Frehse, Bruce H. Krogh, Rob A. Rutenbar, and Oded Maler. Time domain verification of oscillator circuit properties. *Electr. Notes Theor. Comput. Sci.*, 153(3) :9–22, 2006.

[FM07] Goran Frehse and Oded Maler. Reachability analysis of a switched buffer network. In *HSCC*, volume 4416 of *LNCS*, pages 698–701. Springer, 2007.

[FR09] Goran Frehse and Rajarshi Ray. Design principles for an extendable verification tool for hybrid systems. In *ADHS'09*, 2009.

[Fre06] Goran Frehse. On timed simulation relations for hybrid systems and compositionality. In *FORMATS 2006*, volume 4202 of *LNCS*, pages 200–214. Springer, 2006.

[Fre08] Goran Frehse. PHAVer : Algorithmic verification of hybrid systems past HyTech. *International Journal on Software Tools for Technology Transfer*, 10(3), jun 2008.

[Fre09] Goran Frehse. Tools for the verification of linear hybrid automata models. In J. Lunze and F. Lamnabhi-Lagarrigue, editors, *Handbook of Hybrid Systems Control, Theory – Tools – Applications*. Cambridge University Press, 2009. to appear.

[GL08a] Antoine Girard and Colas Le Guernic. Efficient reachability analysis for linear systems using support functions. In *IFAC World Congress*, 2008.

[GL08b] Antoine Girard and Colas Le Guernic. Zonotope/hyperplane intersection for hybrid systems reachability analysis. In *HSCC*, LNCS. Springer, 2008.

[GLM06] Antoine Girard, Colas Le Guernic, and Oded Maler. Efficient computation of reachable sets of linear time-invariant systems with inputs. In *HSCC 2006*, volume 3927 of *LNCS*, pages 257–271. Springer, 2006.

[GP06] Antoine Girard and George J. Pappas. Hierarchical control using approximate simulation relations. In *45th IEEE Conference on Decision and Control (CDC)*, pages 264–269, 2006.

[JKN09] Kevin Jones, Victor Konrad, and Dejan Nickovic. Analog property checkers : a DDR2 case study. *Formal Methods in System Design*, 2009.

[KLD+08] J. P. Kapinski, F. Lerda, A. Donzé, B. Krogh, H. Maka, and S. Wagner. Control software model checking using bisimulation functions for nonlinear systems. In *Proceedings of the 47th IEEE Conference on Decision and Control (CDC'08)*, December 2008.

[LGG09a] Colas Le Guernic and Antoine Girard. Reachability analysis of hybrid systems using support functions. In *CAV*, 2009.

[LGG09b] Colas Le Guernic and Antoine Girard. Reachability analysis of linear systems using support functions. *Nonlinear Analysis : Hybrid Systems*, 2009.

[LM09] Julien Legriel and Oded Maler. Meeting deadlines cheaply. submitted to EMSOFT 2009, 2009.

[Mal06] Oded Maler. Analog circuit verification : a state of an art. *Electr. Notes Theor. Comput. Sci.*, 153(3) :3–7, 2006.

[Mal07] Oded Maler. On optimal and reasonable control in the presence of adversaries. *Annual Reviews in Control*, 31(1) :1–15, 2007.

[MB08] Oded Maler and Grégory Batt. Approximating continuous systems by timed automata. In *FMSB*, pages 77–89, 2008.

[MFK09] Hitashyam Maka, Goran Frehse, and Bruce H. Krogh. Polyhedral domains and widening for verification of numerical programs. In *NSV-II : Second International Workshop on Numerical Software Verification*, 2009.

[MNP05] Oded Maler, Dejan Nickovic, and Amir Pnueli. Real time temporal logic : Past, present, future. In *FORMATS 2005*, volume 3829 of *LNCS*, pages 2–16. Springer, 2005.

[MNP06] Oded Maler, Dejan Nickovic, and Amir Pnueli. From MITL to timed automata. In *FORMATS 2006*, volume 4202 of *LNCS*, pages 274–289. Springer, 2006.

[MNP07] Oded Maler, Dejan Nickovic, and Amir Pnueli. On synthesizing controllers from bounded-response properties. In *CAV*, volume 4590 of *Lecture Notes in Computer Science*, pages 95–107. Springer, 2007.

[MNP08] Oded Maler, Dejan Nickovic, and Amir Pnueli. Checking temporal properties of discrete, timed and continuous behaviors. In *Pillars of Computer Science*, pages 475–505, 2008.

[ND07a] Tarik Nahhal and Thao Dang. Guided randomized simulation. In *HSCC*, volume 4416 of *LNCS*, pages 731–735. Springer, 2007.

[ND07b] Tarik Nahhal and Thao Dang. Test coverage for continuous and hybrid systems. In *CAV*, volume 4590 of *Lecture Notes in Computer Science*, pages 449–462. Springer, 2007.

[Nic08] Dejan Nickovic. *Checking Timed and Hybrid Properties : Theory and Applications.* PhD thesis, University Joseph Fourier, 2008.

[NM07] Dejan Nickovic and Oded Maler. AMT : A property-based monitoring tool for analog systems. In *FORMATS*, volume 4763 of *Lecture Notes in Computer Science*, pages 304–319. Springer, 2007.

[NPGA06] Truong Nghiem, George J. Pappas, Antoine Girard, and Rajeev Alur. Temporal logic verification using simulation. In *EMSOFT*, pages 2–11, 2006.

[SDI08a] Sriram Sankaranarayanan, Thao Dang, and Franjo Ivancic. A policy iteration technique for time elapse over template polyhedra. In *Hybrid Systems : Computation and Control HSCC'08*, LNCS, pages 654–657. Springer, 2008.

[SDI08b] Sriram Sankaranarayanan, Thao Dang, and Franjo Ivancic. Symbolic model checking of hybrid systems using template polyhedra. In *TACAS'08*, LNCS, pages 188–202. Springer, 2008.

[TD09] Stavros Tripakis and Thao Dang. *Model-based Design of Heterogeneous Systems*, chapter Modeling, Verification and Testing using Timed and Hybrid Automata. CRC Press, 2009.