2.3 Tempo team

2.3.1 Tempo team: Scientific production

The group is working mostly in the domain of hybrid systems, which mix discrete/logical transition dynamics with continuous dynamics defined by differential equations. For this class of dynamical systems we provide support for computer-aided engineering at various degrees of formality (and hence scalability). The scientific activities of the team during the period can be classified into the following list of major topics.

1. **Hybrid verification by reachability**: set-based simulation methods that export the ideas of algorithmic formal verification (model checking) toward continuous and hybrid systems;

2. **Hybrid verification by simulation**: complementary methods that try to systematize the generation of inputs (static and dynamic) to an open system so as to detect bugs and provide a good coverage of its reachable states;

3. **Monitoring temporal properties**: developing formalisms to define properties and performance measures for hybrid (mixed) signals together with monitors that can automatically detect violations of such properties;

4. **Conformance testing of hybrid systems**: using a notion of hybrid space coverage measure to develop algorithms and tools for generating test cases for hybrid systems. The developed results can be applied to validation of analog and mixed signal circuits.

5. **Optimization and evaluation of multi-core deployment**: using SMT solvers to pose and solve multi-criteria optimization problems concerning optimal deployment (mapping, scheduling, buffer allocation, etc.). Developing a tool for design-space exploration for abstract data-flow models of applications, experimental validation on multi-core platforms.

6. **Other Work**: theoretical and computational results not directly related to the above.

Much of the work on *reachability* is based on a significant improvement in the algorithmics of computing reachable states for *linear systems* that took place mostly in the preceding period. As a joint effort of the team, the tool **SpaceEx** has been developed, consolidating these achievements and providing many features that make a difference between a prototype tool developed during a thesis and a tool which is one step closer to real-life usability. **SpaceEx** has become the academic de facto standard for reachability computation with 164 citations in the last three years and a vibrant user community (247 users coming from 140 institutions, 10% of which are from industry).

Verification by *simulation* is an alternative method which explores the reachable state-space by sampling the uncertainty space (initial states, parameters, input signals) and conducting simulations. The applicability of this technique to systems not admitting nice mathematical models (e.g. program code) makes it very attractive for industrial users who see it a a sophisticated bug hunting technology. This technique has also been used extensively for parameter synthesis for biological models.

Unlike the above two approaches, *monitoring* is not concerned with coverage of the space of possible behaviors but in checking whether *individual* simulation traces satisfy temporal properties expressed in *signal temporal logic* (STL), an extension of standard LTL with dense time and predicates over real-valued variables. During the period we made various extensions to STL (frequency-domain properties, parametric identification, quantitative semantics), improved the algorithms and collaborated with industrial partners interested in integrating a similar technology in their tools.

While the applicability of formal methods is limited by the complexity of exhautive analysis, *testing* can be used for much larger systems. In order to measure testing quality, a notion of coverage is needed. Therefore, in the context of the PhD of Tarik Nahhal, we focused on *testing*, which was also motivated by the fact that testing is the main technique used in practice for *circuit validation*. Although testing has been well studied in the context of finite state machines and then extended to timed systems, it was not much investigated for continuous and hybrid systems. Our results have high impact that led to two industrial grants from Toyota Motor Engineering & Manufacturing North America, Inc. (TEMA) and United Technologies Corp. (Ireland). The goal of these grants is to investigate the possibilities of a transfer of our testing technology to these companies to improve the reliability of designs.

Much of the work on *optimal deployment* on *multi-cores* was done in the framework of the Minalogic Project ATHOLE (with ST and CEA as partners) which was a major source of financing of the team during the period, including the 4 theses (Legriel, Saidi, Kempf, Tendulkar). The project led to investigation of the proper ways to model applications (task graphs, split-join graphs) architectures (processors, interconnects, DMAs) and external event generators. A variety of methods have been used for optimization and evaluation including exhaustive timed verification, Monte-Carlo simulation, and most notably SMT solvers which have been used to explore feasible solutions in the design space. After the end of the project and the decision of ST to not to share the P2012 platform with the outside, work has been continued using the platform of Tilera and later of Kalray. A byproduct of the project was the introduction of a new research theme, namely multi-criteria optimization and approximation of Pareto fronts.

2.3.1.1 Hybrid Verification by Reachability

Computing the states reachable by all trajectories of an open, continuous or hybrid, dynamical system is the natural extension of symbolic model-checking to the continuous domain [**T-C47, T-C39, T-C13**]. The work can be classified according to the type of dynamics considered.

For the so called linear hybrid automata (LHA), where the derivative of the continuous variables in each discrete state is constant, the tool PHAVer (currently implemented as a scenario on **SpaceEx**) represents the state-of-the art in the domain. It has been recently applied [CJL$^+$09, BMP10] and extended for synthesis [BFM13] and probabilistic systems [ZSR$^+$10]. The techniques to efficiently compute with sets that have been developed for PHAVer can also be applied in other domains; promising preliminary results have been obtained in program verification [**T-C52**].

Most of the work was focused on *linear* and *piecewise-linear* systems where new computational results using support functions [**T-C51**] and polytopes [**T-C35**] allowed us to increase the dimensionality of analyzed systems by more than an order of magnitude. The approach based on support functions has been implemented in the **SpaceEx** tool [**T-C25**] with a lot of efforts in algorithmics, design and implementation to make the tool robust. Further gains in both precision and speed have been achieved by improvements on computing the intersection operation [**T-C20**] and led to a thesis [**T-P3**]. As progress in the scalability of reachability algorithms has allowed us to work on systems with hundreds of variables, it became apparent that the number of convex sets computed can exhibit an explosive growth. This is inherent to all classic approaches to reachability for piecewise-linear systems, since a non convex set is covered by convex sets. A way to quantify this convexification error was developed and a sub-optimal algorithm for computing a minimal cover was published in [**T-C11**] and integrated in **SpaceEx**. High-level improvements to guide the search of the reachability algorithms have been developed in collaboration with the chair of Software Engineering of A. Podelski at the University of Freiburg [**T-C16, T-B3**].

An important research frontier in reachability computation is the treatment of nonlinear systems. We developed a method for dynamic hybridization (piecewise-linearization) which improves upon previous versions of the idea by avoiding the need for intersection. This has been applied to models of biochemical reactions [**T-J7**] and later improved in [**T-C34, DT11**] by taking into account the curvature of the vector field while choosing size and shape of linearization domains. Another class of methods used domain-specific techniques specialized for polynomial systems, such as using box splines [**Dan09**], the Bernstein expansion [**DS09, T-J3**][STDG12] and they were successfully applied to the analysis of biological models [**T-C18**]. The results have been implemented in the library **NLTOOLBOX** [**T-C6**] and have been the subject of the thesis [**T-P2**]. Another application of nonlinear systems reachability algorithms is parameter synthesis for biological models [**T-C2**].

In order to efficiently perform unbounded time verification, we also applied the *abstract interpretation* framework (developed in program analysis) to the computation of *invariants* and *abstract semantics* for affine hybrid automata w.r.t. a given set of linear templates [**T-C23**]. This can then be used to yield an over-approximation of the unbounded time reachable set. We also make use of a *max-strategy improvement algorithm* that allows us to precisely compute these abstract semantics. In addition, we extended this result by adding uncertainty to the model [**T-C24**]. The invariant computation was also combined with the Bernstein technique for polynomial systems and applied to verification of embedded control programs [**DJT13**].

2.3.1.2 Hybrid Verification by Simulation

The alternative approach to verification is based on simulation/testing based while sampling of the uncertainty space of the system [**T-C32**]. There are two major classes of techniques depending on the type of uncertainty. For static uncertainty (values of parameters or initial states) to tool Breach [**T-C33**] implements a technique for parameter-space exploration using local sensitivity information provided by the numerical simulator. This information is used for an intelligent search in the space of parameters which can trace or approximate the boundaries between regions of the parameter-space that lead to satisfaction or violation of an STL property. The tool and the technique have been used in a variety of applications ranging from analog circuits [**T-J9**] via embedded control systems [**T-C48**] to systems biology [**T-J10, T-J8, T-J2**]. It is fair to say that the whole methodology based on Breach and STL served as our major entry point into fruitful collaborations with researchers from the life sciences.

2.3.1.3 Monitoring Temporal Properties

Signal temporal logic (STL) and its associated monitoring tool AMT [**T-J6**], developed during the thesis of D. Nickovic (2008), has generated industrial interest since its publication, as is manifested by the ongoing CIFRE thesis with Mentor Graphics. The intended application domain was assertion-based verification of analog circuits [**T-C38**], but the expressivity of the language turned out to be useful also for control systems [**T-C48**] and biological models [**T-C49, T-J8, T-J2**].

In [**T-C37**] the logic has been endowed with a quantitative semantics which allows to quantify the robustness of satisfaction or violation. This measure can serve in guiding the search for bugs in a simulation-based exploration. In [**T-C10**] an efficient algorithm for computing the robustness degree, linear in the size of the input signal was proposed. In [**T-C28**] we partially solved the following inverse problem: given a parameterized STL formula and a set of traces, find the range of parameters that render the formula satisfied. In [**T-C19**] we extended STL with frequency-domain properties using a shifting window Fourier transform that produces spectral signals whose temporal evolution can be referred to using the usual STL operator. This combination of time and frequency allowed us to express and check music-related properties of signals.

On the implementation side, the robust semantics has been implemented in the tool Breach [**T-C33**], and a new version of AMT has been rewritten by O. Lebeltel using Java. Further developments are the subject of a joint project with the Austrian Institute of Technology.

2.3.1.4 Conformance Testing of Hybrid Systems

Test coverage is a way to characterize the relation between the number and the type of tests to execute and the portion of the system's behavior effectively tested. The classical notions of coverage for software testing (such as statement and path coverages) are unsuitable for the behaviors of a hybrid system. We thus proposed a *novel coverage measure*, which on one hand reflects the testing objectives and, on the other hand, can be efficiently computed to guide the test generation process. It is based on the *star discrepancy notion* from statistics that measures the equidistribution degree of a set of states over the state space.

Based on the RRT algorithm (Rapidly exploring Random Trees) for robotic motion planning, we developed the **gRRT** algorithm, one of the first *coveraged-guided test generation* algorithms for hybrid systems [**T-J11, T-C54, T-C53**]. While the coverage-guided algorithm tends to produce test suites with a "uniform" coverage over the whole state space, in order to bias the exploration towards some critical paths we proposed a new *property-guided sampling method*, which uses a random walk on a discrete abstraction (reflecting the exploration objective) of the original system.

In addition, to address practical settings with *partial observability*, it is necessary to reconstruct the trajectory of the system under test in order to produce a verdict. To this end, we proposed to use a *hybrid Newton observer* that can provide an estimate for the current location and the continuous state based on the information on the input and the output of the system under test [**T-C17**]. These results have been implemented in the tool **HTG** for hybrid systems test generation which can handle, in addition to hybrid automata, electrical circuits specified in SPICE [**T-C53**]. The approach was also applied to the property falsification problem [**T-C7**].

2.3.1.5 Optimization for Multi-Core Deployment

The team has been involved in the past in numerous attempts to fight the clock explosion in reachability-based verification of timed automata [**T-C44**] and make timing verification, evaluation and optimization feasible. During the ATHOLE project we tried other types of techniques. In [**T-C30**] we used an SMT solver to find optimal schedules for task-graphs on multi-cores while treating the number of processors used as a constraint. We then realized that a more useful approach is to move to *multi-criteria optimization* (MCO) where trade-offs between latency, cost and other features are presented to the decision maker. We developed two methods for approximating the Pareto front of such problems, the first one based on conducting a generalized multi-dimensional binary search with an SMT solver used as a query oracle [**T-C40, T-C31**], and one based on stochastic local search [**T-C29**]. The results are summarized in the thesis [**T-P5**] and further research on MCO is now conducted in a new thesis.

The applications investigated in the ATHOLE project exhibited a lot of data parallelism (video encoding/decoding) and we studied the problem of partitioning a data array into chunks of optimal size and shape for efficient utilization of the DMA machinery between main memory and the cores. The results were published in [**T-J4, T-J1**] and are the object of the thesis [**T-P4**]. An abstract model of scheduling under uncertainty where different jobs arrive dynamically has been investigated in [DM08]. Within the ATHOLE project a prototype tool **DespEx** (the design-space explorer) has been developed which, based on a high-level system description (architecture, application, environment and deployment), evaluates system performance using mostly simulation. This high-level approach [**T-C1**] which provides much more efficient simulation than what is common in many hardware and software circles, is described in the thesis [**T-P1**]. Some reflections on the the lessons learned from the ATHOLE experience and on the importance and usability of timed models in general appear in [**T-B1**].

More recently we started a collaboration with Kalray and acquired their new platform. We studied the efficient deployment of split-joint graphs on this platform. These graphs which are a subclass of SDF (synchronous data-flow) provide a compact way to encode data-parallelism and consequently lead to very large task-graphs that need special symmetry breaking predicates [**T-C5**] to handle by a solver. An extensive infra-structure development and experimental evaluation work has been conducted on the Kalray platform and is reported in the forthcoming thesis of P. Tendulkar.

2.3.1.6 Other Results

Moving from set-theoretic to probabilistic non-determinism in verification and synthesis is a current trend as demonstrated in the recent popularity of *statistical model checking* to which A. Donze, a non-permanent member and alumni of the team, made a significant contribution [**T-J9**]. We developed timed automata models, *duration probabilistic automata* (DPA) where timing is not given by an interval but by a *uniform* distribution over this interval. Continuous-time models have been used extensively elsewhere but they rarely use distributions other than the easy case of exponential where no clocks are needed. In [**T-C41**] we presented en extension to zone-based reachability to DPA using density transformers. In [**T-C27**] we developed a clock-free method for computing probabilities over qualitative paths of the DPA. This allows us to compute and compare the expected performance of different schedulers. In [**T-C12**] we showed how the problem of synthesizing expected-time optimal schedulers on this model can be solved using an adaptation of dynamic programming.

In [**T-C43, T-O1**] new concepts and results concerning the entropy of timed languages were established. These results underly a large part of the ANR project Eqinocs in which we currently participate. The paper [**T-C42**] investigates games with mean-payoff and characterizes their expressive power. In [**T-C3**] we extend Angluin's algorithm for learning regular languages to deal with large alphabets. In [**T-C36**] we presented a modern exposition of the classical Krhon-Rhodes theorem about the cascaded decomposition of automata. In [**T-B2**] together with biologists we summarized the insights from our collaboration on modeling the specialization of blood cells. In [**T-C14**] we investigate models of mass action systems and in particular their sensitivity to initial spatial distribution of the various species.

2.3.2 Tempo team: Scientific influence

2.3.2.1 Hybrid Systems

The group is one of the leading groups worldwide in the domain of hybrid systems. O. Maler is among the founders and members of the steering committee of the conference series HSCC (today part of CPSWeek). In this domain the group has promoted research directions (continuous reachability, controller synthesis, systematic simulation, monitoring temporal properties) that proved useful and popular. Other members of the group, T. Dang and G. Frehse are well recognized by the hybrid community due to their work on reachability, test generation and development of robust tools. T. Dang was the PC chair of HSCC in 2013.

2.3.2.2 Timed Systems

In the past, previous incarnations the group were instrumental in the study of timed automata, providing pioneering results and tools for verification and controller synthesis with applications to scheduling. The conference series FORMATS, initiated by O. Maler who currently chairs the steering committee is an established venue for presenting results in the domain.

2.3.2.3 Analog Verification

Members of the team were among the first to identify verification of analog and mixed-signal circuits as an application domain for hybrid technology. The workshop FAC (formal verification of analog circuits) was initiated by O. Maler and has been recently extended in scope and renamed *frontiers in analog CAD* and draws academic and industrial participants from both sides of the Atlantic. T. Dang was a PC chair in 2013, and G. Frehse is the organization chair for the 2014 workshop in Grenoble.

2.3.2.4 Systems Biology

The inter-disciplinary difficulties associated while interacting with people from control, scheduling and circuit design, pale compared to those encountered while trying to communicate with life scientists. The group organized two inter-disciplinary meetings in Grenoble under the title *Towards System Biology*, the second in 2011, which gathered biologists, physicists mathematicians and computer scientist. The group was involved in the new conference series HSB, *hybrid systems biology* for which T. Dang was a PC chair in 2013 and O. Maler in 2014.

2.3.2.5 Verification in General

O. Maler was a PC co-chair of CAV 2009, the major venue for formal verification. Members of the team participated in program committees of conferences outside the specific timed and hybrid context, including CAV, FMCAD, CMSB, RV, ICALP, PODC and ATVA.

2.3.3 Tempo team: Interaction with the economic, social and cultural environment

In recent years, with the maturation of the computational techniques developed in the group, there is an increase in collaborations with industrial partners, detailed below.

1. **STMicroelectronics**: During the ATHOLE project on multi-cores, ST granted two CIFRE contracts to the group. Today we have strong ties with ST Crolles on analog CAD, culminating in 2 joint Nano2017 projects waiting for final approval;

2. **Mentor Graphics**: There is currently a CIFRE contract on the integration of AMS assertions in Mentor's simulation tools;

3. **Atrenta**: Two alumni of the group, S. Cotton and J. Legriel, work in Atrenta and there is an ongoing CIFRE contract on switching and power reduction in digital circuits.

4. **Kalray**: We had two contracts for testing our deployment optimization tools on their MPPA platform;
5. **Toyota USA**: We have an ongoing contract about simulation-based verification of engine models;
6. **United Technology Research Center**: We are finalizing a contract on simulation-based verification of HVAC (heating, ventilation, air-conditioning) systems;
7. **Bosch**: The SpaceEx verification tool has been used to verify an electro-mechanical breaking system. The timing effects of a software controller were studied in combination with a model of the physical plant, and the results have been published at RTSS 2014.
8. **Mathworks**: One of the group alumni, J-F. Kempf, works there and O. Maler participated in their annual faculty summit in, June 2014.
9. **Easii-IC**: We have a joint project (together with the Austrian Institute of Technology) and pending joint submissions to H2020 and Nano2017.

2.3.4 Tempo team: Internal organization and life of the team

The group is rather small and does not necessitate a strict hierarchical structure. A group seminar is held more or less regularly, in which researchers, students and visitors present their results. Seminars are held in English, partly due to presence of non-natives and partly to train French students to feel more comfortable in English. Long-term software development (outside PhD theses) is done either by the group's research engineer O. Lebeltel or by the current post-doc S. Minopoli. There are many ad-hoc meetings around research problems, preparation of proposals and visitors, involving the relevant subsets of the team.

2.3.5 Tempo team: Training through Research

During the period, members of the team gave the following courses: Implementation of Control Systems and Realistic modelling and Multi-task implementation of control systems (by Thao Dang at ENSIMAG, Grenoble University of Technology INPG)

In addition the following, advanced mini-courses where given in international schools and events: PhD School on Quantitative Model Checking (Copenhagen, 2010), Spring school of the French Society for Theoretical Biology (St Flour, 2012), International school on formal methods (Bertinoro, 2013), Advanced course on cyber-physical systems (Technical university of Vienna, 2013), Nano-Terra summer school (Aix-les-Bains, 2013).