Safety Analysis of Real-Time Discrete-Event and Hybrid Systems

Master 2 Internship Proposals

Context

More and more systems are safety-critical, e.g., medical devices, aircraft flight control, nuclear systems and, more recently, cyber-physical systems. Verifying at design stage safety properties is consequently crucial for their reliability. We are particularly interested in the diagnosability property [14], i.e. the ability to determine without ambiguity from the observations and within a given time delay that a given fault has occurred, i.e., to disambiguate faulty and normal trajectories from observations. Verifying diagnosability property boils down to prove the unsatisfiability of a logical formula [5, 13] expressing the existence of a so-called critical pair, i.e., a pair of faulty and normal trajectories, with enough long duration after the fault occurrence, sharing the same observations, which would violate diagnosability. For discrete-event systems, checking this formula can be done by using a Satisfiability (SAT) solver or a Satisfiability Modulo Theories [3] (SMT) solver (with Linear Real Arithmetic theory for dealing with time constraints) [7]. The major challenge for modeling and verifying these systems resides in their intrinsic complexity arising from the combination of a continuous part (analog physical processes) and a discrete part (digital computational processes) and the interaction between them. They can be modeled classically by hybrid automata [8], i.e., finite state machines with a finite set of continuous variables whose values are described by a set of ordinary differential equations, associated with the different states (or modes), the discrete transitions between states being in turn determined by the evolution of the continuous variables. Due to the continuous part, almost all problems, even the simplest such as reachability, are undecidable for general hybrid automata. This shows that the use of approximations is necessary to check safety properties of hybrid systems.

This is why we recently resorted to discrete qualitative abstractions (under-approximations) of a hybrid automaton [16], such that verifying the given safety property at their level is decidable and this property, if satisfied, is then satisfied also at the level of the hybrid automaton [18], providing thus a semi-decision for the property to be checked at its level. Such a qualitative abstraction can be constructed as an automaton or better still as a timed automaton [1] (to abstract also the temporal features induced by the continuous dynamics). If there is no decision for the property, the abstraction is refined (by constructing a finer partition into regions of the continuous space) and the process is iterated. Classically, this refinement is guided by a counterexample of the property (here, a critical pair) at the abstract level (deemed fallacious at the concrete level, otherwise it can be concluded that the property is violated at this level), so as to avoid it and similar examples at the finer level: it is the CounterExample-Guided Abstraction Refinement (CEGAR) technique [4, 17], which has been shown to be efficient at solving computationally difficult (e.g., NP or PSPACE)

problems. Now, as the diagnosability analysis for timed automata is in itself such a difficult problem (it has been proved to be PSPACE-complete [15]), we have also used approximations and a CEGAR-based approach to solve it [6]. Actually, inspired by a recent extension of the CEGAR framework, called Recursive Explore and Check Abstraction Refinement (RECAR) [9], we alternate the CEGAR technique for over- and for under-approximations of the problem. Applied to over- (resp., under-) approximations, this technique considers more constrained (resp., relaxed) versions of the problem, therefore with fewer (resp., more) solutions. Thus, if the over- (resp., under-) approximate problem is satisfiable (resp., unsatisfiable), so is the initial problem, providing thus sat and unsat shortcuts, respectively. Otherwise, the current approximation must be refined by relaxing (resp., constraining) it. Strategies for switching from one type of approximation to the other are defined based on the execution time of the current instance and its evolution.

Objectives

Depending on the skills and preferences of the candidate, different objectives may be pursued, giving rise to so many subjects.

1. *Approximation-based Diagnosability Analysis of Timed Automata*

   Our diagnosability analysis of timed automata with a RECAR-like framework improves the direct analysis in case of sat answer, i.e., when the system is non-diagnosable, thanks to an efficient over-approximation of the problem, mainly achieved by reducing the length of the critical pair that is searched. But it remains inefficient in case of unsat answer, i.e., when the system is diagnosable, due to the inefficiency of our under-approximations. So, the objective is to develop more efficient under-approximations of the problem and to test the whole analysis on more benchmarks, automatically generated.

   Requirements: Own or acquire skills in timed automata, diagnosability, approximations and CEGAR, SMT and use of the SMT solver Z3.

2. *Timed Automata Abstractions of Hybrid Automata*

   The objective is to continue the preliminary work above about the definition and construction of under-approximations of hybrid automata as timed automata and their refinements. The states of such a timed automaton abstracting the given hybrid automaton are obtained by splitting the continuous space into a finite set of areas, each one being an approximation, in a given mode of the hybrid automaton, of the solution space of the differential equations attached to this mode. Its state invariants and transition guards are built from the sojourn duration in each mode. Refinement is obtained by splitting a given area into several ones. The automation of the construction of the initial abstraction and its successive refinements (guided by a spurious counter-example, here a critical pair, in a CEGAR framework) will be studied. A general framework will be adopted where an oracle provides lower and upper bounds of the sojourn duration in a mode. Then several methods will be studied for implementing such an oracle: exact computation in the easy case of the existence of a known analytical solution of the set of differential equations; simulation of the hybrid system (flowpipe calculation); use of neural networks, in particular, Physics-Informed Neural Networks (PINNs) [12]. The arbitrarily close approximation of hybrid systems by recurrent neural networks was theoretically proved in 1997 [2]. This convinces us it is worthwhile studying in

depth how to approximate hybrid systems with PINNs precisely and efficiently. Testing will be done on given benchmarks of hybrid systems.

Requirements: Own or acquire skills in timed automata, hybrid automata and simulation tools, abstractions and CEGAR, PINNs.

3. *Approximation-based Framework for ϵ-guarantee of Properties on Hybrid Automata*

   The objective is to define a general RECAR-like framework of over- and under-approximations of hybrid automata and their refinements in order to verify as close as required, i.e., by ϵ for a given positive real number ϵ, given safety properties of these hybrid systems, such as diagnosability. In addition to under-approximations defined as timed automata as above, over-approximations will have also to be defined and implemented. For this, recent results concerning the over-approximation of attainable states in hybrid systems [10] will be studied. The efficiency of the whole RECAR-like method (with a given timeout) will be tested on given benchmarks of hybrid systems. Then this RECAR-like procedure will be extended by considering ϵ-approximations [11], without which the termination and thus the correct verdict cannot be guaranteed. In particular, how to best exploit the certificates returned by the solver in each approximation case, when they do not allow a direct conclusion for the considered property of the initial system, will be studied. Precise definitions of an ϵ-approximation of a given hybrid automaton and of an ϵ'-validity of a formal property of such a hybrid automaton will have to be given and how to transform the validity of a property on an ϵ-approximation of the hybrid system into an ϵ'-validity of the same property on the hybrid system and vice versa will be studied.

   Requirements: Own or acquire skills in hybrid automata and simulation tools, approximations and CEGAR.

Location

Laboratoire Méthodes Formelles, Université Paris-Saclay, CNRS, ENS Paris-Saclay.

Supervision

Philippe Dague, professeur émérite Université Paris-Saclay (philippe.dague@universite-paris-saclay.fr) et Lina Ye, maîtresse de conférences CentraleSupélec (lina.ye@centralesupelec.fr).

References

[1] Rajeev Alur and David L Dill. "A theory of timed automata". In: *Theoretical computer science* 126.2 (1994), pp. 183–235.

[2] Andrew D. Back and Tian-Ping Chen. "Approximation of hybrid systems by neural networks". In: *Proc. of the International Conference on Neural Information Processing, ICONIP 1997, Denver, Colorado, USA*. Springer, 1997, pp. 326–329.

[3] Clark Barrett, Roberto Sebastiani, Sanjit A Seshia, and Cesare Tinelli. "Satisfiability Modulo Theories". In: *Handbook of satisfiability*. Ed. by Armin Biere, Marijn Heule, Hans van Maaren, and Toby Walsh. IOS Press, 2021. Chap. 33, pp. 1267–1329.

[4] Edmund M. Clarke, Orna Grumberg, Somesh Jha, Yuan Lu, and Helmut Veith. "Counterexample-guided abstraction refinement for symbolic model checking". In: *J. ACM* 50.5 (2003), pp. 752–794.

[5] Alban Grastien, Anbu Anbulagan, Jussi Rintanen, and Elena Kelareva. "Diagnosis of discrete-event systems using satisfiability algorithms". In: *Proceedings of the 22nd National Conference on Artificial Intelligence AAAI'07*. 2007, pp. 305–310.

[6] Lulu He. "Formal verification at design stage of diagnosis related properties for discrete event and real-time systems". PhD thesis. Université Paris-Saclay, 2022.

[7] Lulu He, Lina Ye, and Philippe Dague. "SMT-based Diagnosability Analysis of Real-Time Systems". In: *Proceedings of the 10th Symposium on Fault Detection, Supervision and Safety for Technical Processes, IFAC SAFEPROCESS 2018*. 2018.

[8] Thomas A Henzinger. "The theory of hybrid automata". In: *Verification of Digital and Hybrid Systems*. Springer, 2000, pp. 265–292.

[9] Jean-Marie Lagniez, Daniel Le Berre, Tiago de Lima, and Valentin Montmirail. "A Recursive Shortcut for CEGAR: Application To The Modal Logic K Satisfiability Problem". In: *Proc. of the 26th International Joint Conference on Artificial Intelligence, IJCAI 2017, Melbourne, Australia*. Ed. by Carles Sierra. ijcai.org, 2017, pp. 674–680.

[10] Meilun Li, Peter N. Mosaad, Martin Fränzle, Zhikun She, and Bai Xue. "Safe Over- and Under-Approximation of Reachable Sets for Autonomous Dynamical Systems". In: *Formal Modeling and Analysis of Timed Systems*. Ed. by David N. Jansen and Pavithra Prabhakar. Springer International Publishing, 2018, pp. 252–270.

[11] Anuj Puri, Vivek Borkar, and Pravin Varaiya. "ϵ-Approximation of differential inclusions". In: *Hybrid Systems III, Verification and Control*. Ed. by Rajeev Alur, Thomas A. Henzinger, and Eduardo D. Sontag. Vol. 1066. Lecture Notes in Computer Science. Springer, 1996, pp. 362–376.

[12] Maziar Raissi, Paris Perdikaris, and George Em Karniadakis. "Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations". In: *Journal of Computational Physics* 378 (2019), pp. 686–707.

[13] Jussi Rintanen and Alban Grastien. "Diagnosability testing with satisfiability algorithms". In: *Proceedings of the 20th International Joint Conference on Artificial Intelligence IJCAI'07*. 2007, pp. 532–537.

[14] Meera Sampath, Raja Sengupta, Stéphane Lafortune, Kasim Sinnamohideen, and Demosthenis Teneketzis. "Diagnosability of discrete-event systems". In: *IEEE Transactions on automatic control* 40.9 (1995), pp. 1555–1575.

[15] Stavros Tripakis. "Fault diagnosis for timed automata". In: *Proceedings of the International symposium on formal techniques in real-time and fault-tolerant systems*. Springer. 2002, pp. 205–221.

[16] Hadi Zaatiti, Lina Ye, Philippe Dague, and Jean-Pierre Gallois. "Automating Abstraction Computations of Hybrid Systems". In: *Formal Verification of Physical Systems FVPS 2018, workshop of the 11th Conference on Intelligent Computer Mathematics CICM 2018*. Hagenberg, Austria, Aug. 2018.

[17] Hadi Zaatiti, Lina Ye, Philippe Dague, and Jean-Pierre Gallois. "Counterexample-Guided Abstraction-Refinement for Hybrid Systems Diagnosability Analysis". In: *28th International Workshop on Principles of Diagnosis DX'17*. Ed. by Marina Zanella, Ingo Pill, and Alessandro Cimatti. Vol. 4. Kalpa Publications in Computing. EasyChair, 2018, pp. 124–143.

[18] Hadi Zaatiti, Lina Ye, Philippe Dague, Jean-Pierre Gallois, and Louise Travé-Massuyès. "Abstractions Refinement for Hybrid Systems Diagnosability Analysis". In: *Diagnosability, Security and Safety of Hybrid Dynamic and Cyber-Physical Systems*. Ed. by Moamar Sayed-Mouchaweh. Springer, 2018, pp. 279–318.