M2 Research Internship

State space abstraction for timed systems

Supervisors: Étienne André and Kaïs Klaï
Email: {first.last}@univ-paris13.fr
Laboratory: LIPN, CNRS UMR 7030, Université Paris 13, Sorbonne Paris Cité, France

Context

Timed systems have become ubiquitous in the past few years. Some of them (e.g., automated plane and unmanned systems control, driverless cars) are critical in the sense that no error must occur. Testing these systems can possibly detect the presence of bugs, but not guarantee their absence. It is necessary to use formal methods such as model checking [BK08] so as to prove formally the correctness of a system.

One of the main formalisms used to specify and verify critical timed systems is timed automata [AD94]. Unfortunately, verifying large systems is often challenging due to the state space explosion problem. One way to prevent this problem is to build *abstractions* of the state space. Such an abstraction is generally guided by the property one wants to check.

Internship subject

Recently, Symbolic Observation Graphs [HIK04, KP08, DLKPTM11] have been proposed for *untimed* systems. This powerful abstraction significantly reduces the state space while preserving some interesting temporal properties (LTL). The main objective of this internship is to extend the SOG-based approach to timed systems.

An implementation may also be performed by the intern, so as to validate the proposed approach.

Keywords

Formal methods, model checking, timed automata, abstractions.

Skills

The following skills are not compulsory, but would be welcome: timed automata, model checking, temporal logics.

Conditions

Highly motivated applicants are being sought.

The internship will take place at LIPN (Laboratoire d'Informatique de Paris Nord), Université de Paris 13, Sorbonne Paris Cité (campus of Villetaneuse), France.

Standard remuneration.

Depending on the candidate's motivation and wishes, this internship can lead to a PhD thesis.

References

[AD94] Rajeev Alur and David L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, April 1994.

[BK08] Christel Baier and Joost-Pieter Katoen. *Principles of Model Checking*. MIT Press, 2008.

[DLKPTM11] Alexandre Duret-Lutz, Kais Klai, Denis Poitrenaud, and Yann Thierry-Mieg. Self-loop aggregation product - a new hybrid approach to on-the-fly ltl model checking. In *Automated Technology for Verification and Analysis, 9th International Symposium, ATVA 2011, Taipei, Taiwan, October 11-14, 2011. Proceedings*, volume 6996 of *Lecture Notes in Computer Science*, pages 336–350, 2011.

[HIK04] Serge Haddad, Jean-Michel Ilié, and Kais Klai. Design and evaluation of a symbolic and abstraction-based model checker. In *Proc. of ATVA'04*, volume 3299 of *LNCS*, pages 198–210. Springer, 2004.

[KP08] Kais Klai and Denis Poitrenaud. MC-SOG: An LTL model checker based on symbolic observation graphs. In *Proc. of Petri Nets'08*, volume 5062 of *LNCS*, pages 288–306. Springer, 2008.