Checking Emptiness of Timed Büchi Automata using Non-Convex Abstractions

- **Advisors:** F. Herbreteau (fh@labri.fr) and I. Walukiewicz (igw@labri.fr)
- **Institution:** Laboratoire Bordelais de Recherche en Informatique (LaBRI)
- **Team:** Formal Methods team, Modeling & verification group
- **Funding:** 50% (ANR)

Subject

Timed automata [1] are finite automata extended with clocks that can be tested and reset on the transitions of the automaton. The clocks allow to constrain the delays between actions of the automaton. Timed automata have been successfully used to model and verify real-time systems. The tool UPPAAL [7] is used by critical software designers and numerous case studies have been reported [8].

The state-space of a timed automaton is uncountable. Verification algorithms thus use an abstract representation of the state-space. Coarser abstractions yield a smaller representation, hence more efficient verification algorithms. Several abstractions have been introduced [2,3] in an effort to define the coarsest abstraction possible. Till recently, it was believed that only convex abstractions could be used efficiently. We have recently proposed an algorithm that uses a non-convex abstraction that is moreover, in a sense, the coarsest abstraction, to check reachability properties of timed automata, in an efficient way [4,5].

Verifying properties on the infinite runs of timed automata is more involved. It amounts to finding an accepting run (w.r.t. Büchi accepting conditions) that is moreover non-Zeno. An infinite run is non-Zeno if the time that elapses on the run diverges. Otherwise, the run is Zeno. In the last years, we have proposed an approach to detect non-Zeno runs and to decide the emptiness of timed Büchi automata using convex abstractions [6].

The goal of this internship is to combine the algorithms in [4,5,6] in order to check the emptiness of timed Büchi automata more efficiently. The algorithm in [6] consists in detecting a strongly connected component in a graph that satisfies a given property. The main challenge is thus to detect strongly connected components using the covering test in [4,5] instead of the usual equality over nodes as in [6]. The expected outcome of the internship is a new efficient algorithm, a proof of its correctness, and an implementation of the algorithm in the verification tool that is under development in our group.

Bibliography

- [1] R. Alur and D. Dill. A Theory of Timed Automata. Theoretical Computer Science, 126: 183-235, 1994.
- [2] C. Daws and S. Tripakis. Model checking of real-time reachability properties using abstractions, TACAS, 1998.
- [3] G. Behrmann, P. Bouyer, K. G. Larsen and R. Pelanek. Lower and upper bounds in zone-based abstractions of timed automata, STTT, 8(3): 204-215, 2006.
- [4] F. Herbreteau, D. Kini, B. Srivathsan and I. Walukiewicz. Using non convex approximations for efficient analysis of timed automata, FSTTCS, 2011.
- [5] F. Herbreteau, B. Srivathsan and I. Walukiewicz. Better abstractions for timed automata, LICS, 2012.
- [6] F. Herbreteau, B. Srivathsan and I. Walukiewicz. Efficient Emptiness Check for Timed Büchi Automata, FMSD, 40(2): 122-146, 2012.

- [7] http://www.uppaal.org
- [8] http://www.it.uu.se/research/group/darts/uppaal/examples.shtml