Internship proposal

Parametric Verification of Real Time Systems using Time Petri Nets

Étienne André

Laboratoire d'Informatique de Paris Nord, Université Paris 13

Context

The importance of real time systems has dramatically grown in the past decade. Some of them (plane or car control systems, banking systems, etc.) are critical in the sense that it is not acceptable that any failure occurs. Testing such a system can help detecting bugs, but not guarantee the absence of bugs. As a consequence, one needs methods such as model checking [5] in order to formally prove the correctness of the system.

Real time systems are characterized by a set of timing constants, such as the traversal delay of the electric current within a circuit, or the delay before retransmitting a data within a cellphone. Although techniques can be used to verify the system for one set of timing constants, it can be very time consuming to formally verify the system for many values of these constants. Verifying the system for dense (hence infinite) sets of the constants would even require an infinite number of verifications.

Therefore, it is often interesting to consider that the timing constants are unknown, viz., *parameters*, and synthesize a *constraint* on these parameters guaranteeing the correctness of the system. A method, called the *inverse method* [2], has been proposed in the framework of timed automata [1], a popular formalism extending finite state automata. Given a reference set of timing constants corresponding to a good behavior, this method automatically synthesizes a constraint on the parameters guaranteeing the same good behavior as for the reference set of timing constants. As a consequence, this guarantees that the system will also be correct for any value satisfying this constraint.

This method has been implemented within a tool, IMITATOR [4], which has been used to formally verify a model of an electronic circuit manufactured by ST-Microelectronics. The method also led to several extensions for timed, probabilistic or hybrid systems [3, 6].

Objective of the Internship

Another popular formalism for the verification of real time systems is time Petri nets [7]. Although quite close to timed automata, time Petri nets have a different

expressive power. Furthermore, the tools and methods dedicated to time Petri nets are different from those dedicated to timed automata. It would hence be interesting to adapt this inverse method to time Petri nets, in order to benefit from these tools and methods, and consider applications more specific to Petri nets. Decidability and complexity issues may also differ.

The internship will first consist in investigating timed automata, time Petri nets, and the inverse method. Then, the algorithm of the inverse method should be adapted to the framework of Petri nets, taking into account the specificities of this formalism. Finally, this algorithm should be implemented, either by creating a variant of IMITATOR (which is written in OCaml), or by developing a new tool in another language.

Depending on the intern's wishes, variants of the algorithm may also be defined, and theoretical questions such as the complexity or the termination of the new algorithm may also be studied.

Conditions

Applicants should be highly motivated students in Master 2 with strong autonomy and programming skills. Knowledge in either Timed Automata or Petri Nets would be appreciated, but not compulsory. The internship takes place at LIPN (Laboratoire d'Informatique de Paris Nord) in the University of Paris 13 (Villetaneuse, 20 minutes from Paris Gare du Nord), for about 3 to 6 months preferably during spring and summer 2012, although other periods may be possible as well.

Contact

Please address questions and applications (by email only) to Étienne André:
`Etienne.Andre (at) lipn.univ-paris13.fr`.

References

1. R. Alur and D.L. Dill. A theory of timed automata. *TCS*, 126(2):183–235, 1994.
2. É. André, T. Chatain, E. Encrenaz, and L. Fribourg. An inverse method for parametric timed automata. *International Journal of Foundations of Computer Science*, 20(5):819–836, 2009.
3. É. André, L. Fribourg, and J. Sproston. An extension of the inverse method to probabilistic timed automata. In *AVoCS'09*, volume 23 of *Electronic Communications of the EASST*, 2009.
4. Étienne André. IMITATOR II: A tool for solving the good parameters problem in timed automata. In *INFINITY'10*, volume 39 of *EPTCS*, pages 91–99, 2010.
5. E. M. Clarke, O. Grumberg, and D. A. Peled. *Model Checking*. MIT Press, 1999.
6. L. Fribourg and U. Kühne. Parametric verification and test coverage for hybrid automata using the inverse method. In *RP'11*, volume 6945 of *LNCS*. Springer, 2011.
7. Philip Meir Merlin. *A study of the recoverability of computing systems*. PhD thesis, University of California, Irvine, 1974.