ETR 2017

August 28th, 2017
Paris

Parametric model checking timed automata under non-Zenoness assumption

Nguyễn Hoàng Gia

Supervisors: Étienne André , Laure Petrucci
+ Joint work with: Jun Sun (Singapore)

LIPN, Université Paris 13, CNRS, France

Outline

1 Context
- Context: model checking real-time systems
- Beyond model checking: parameter synthesis
- Parametric Timed Automata (PTA)

2 Zenoness
- Our goal: remove Zeno runs in parametric model checking

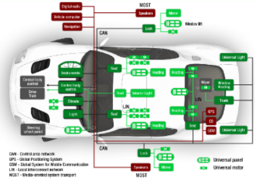
3 non-Zeno synthesis
- Our contribution: CUB-PTA approach

Outline

1. Context
   - Context: model checking real-time systems
   - Beyond model checking: parameter synthesis
   - Parametric Timed Automata (PTA)
2. Zenoness
   - Our goal: remove Zeno runs in parametric model checking
3. non-Zeno synthesis
   - Our contribution: CUB-PTA approach

Context: model checking real-time systems

Real-time systems are difficult to test and their failure leads to dramatic consequences

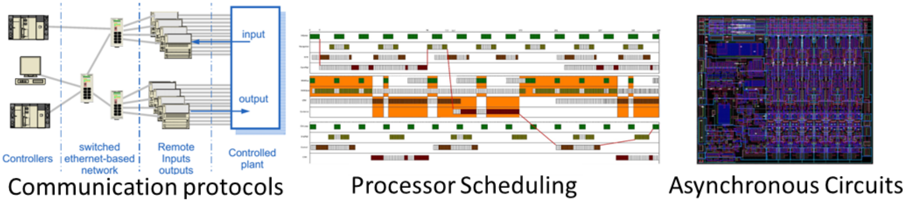


Model checking [Baier and Katoen, 2008] is an automatic verification technique to verify the correctness of the system model w.r.t. a property:

- **Verification** procedure: exhaustive search of the state space of the model

Beyond model checking: parameter synthesis

Verification techniques used for critical systems, timed systems where changes of time value is vital! such as:



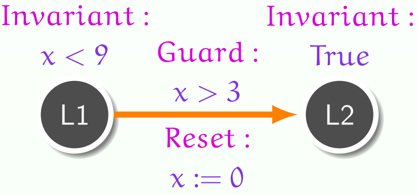
Communication protocols | Processor Scheduling | Asynchronous Circuits

1. Systems incompletely specified, some timing delays may not be known yet, or may change
2. Verifying system for numerous values of constants requires a very long time, or even infinite

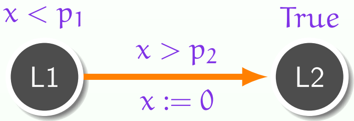
⇒ Use parameterised techniques, by using parameters instead of constants, then one can check many values at the same time, but also infer good valuations of these timing constants

Parametric Timed Automata (PTA)

PTA are a formalism to model and verify concurrent real-time systems [Alur et al., 1993]



Timed Automata-TA



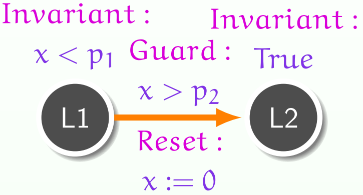
PTA

x: Clock

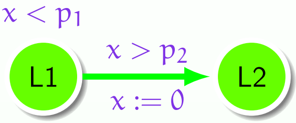
p: Parameters allow to represent unknown values

Parametric Timed Automata (PTA)

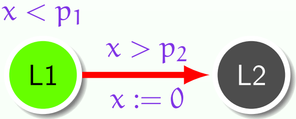
PTA are a formalism to model and verify concurrent real-time systems [Alur et al., 1993]



PTA



(with $p_1 > p_2$)



(with $p_1 \leq p_2$)

System Behaviour depends on the values of parameters

Outline

1 Context

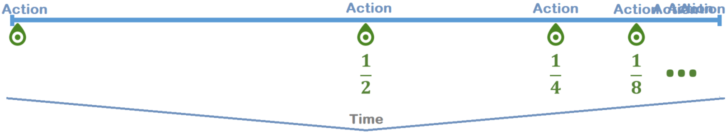
- Context: model checking real-time systems
- Beyond model checking: parameter synthesis
- Parametric Timed Automata (PTA)

2 Zenoness

- Our goal: remove Zeno runs in parametric model checking

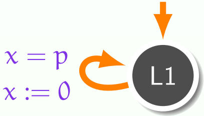
3 non-Zeno synthesis

- Our contribution: CUB-PTA approach

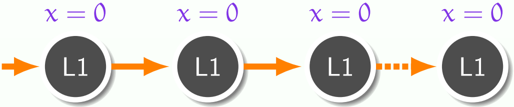


A Zeno run is a run with an infinite number of actions within a finite time.

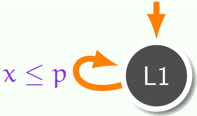
1. Run has a clock such that time cannot elapse



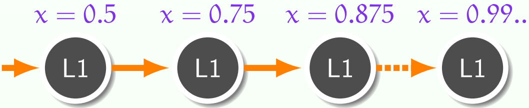
with
$p = 0$



2. Run has a clock bounded by a parameter or a constant



with
$p = 1$



In fact, this run is Zeno for any value of p

⇒ Infeasible in practice! Our goal is to design a method for parametric model checking that avoids to return Zeno runs as counterexamples

Outline

1 Context

- Context: model checking real-time systems
- Beyond model checking: parameter synthesis
- Parametric Timed Automata (PTA)

2 Zenoness

- Our goal: remove Zeno runs in parametric model checking

3 non-Zeno synthesis

- Our contribution: CUB-PTA approach

Our contribution

We define a CUB approach for PTA by:

1. Extend to PTA an approach CUB [Wang et al., 2015]("Clock Upper Bound") which solves the non-Zenoness problem on Timed Safety Automata (TA)
2. Propose a semi-algorithm for parameter synthesis for CUB-PTA
3. Implement in IMITATOR [André, Fribourg, Kühne, Soulat, 2012] and perform experiments

For more information please find our full paper:

- Parametric model checking timed automata under non-Zenoness assumption, 9th NASA Formal Methods Symposium - NFM'17 [André et al., 2017]

Bibliography

References I

Alur, R., Henzinger, T. A., and Vardi, M. Y. (1993).
Parametric real-time reasoning.
In *STOC*, pages 592–601. ACM.

André, É., Fribourg, L., Kühne, U., and Soulat, R. (2012).
IMITATOR 2.5: A tool for analyzing robustness in scheduling problems.
In *FM*, volume 7436 of *Lecture Notes in Computer Science*, pages 33–36. Springer.

André, É., Nguyen, H. G., Petrucci, L., and Sun, J. (2017).
Parametric model checking timed automata under non-zenoness assumption.
In Barrett, C., Davies, M., and Kahsai, T., editors, *NASA Formal Methods - 9th International Symposium, NFM 2017, Moffett Field, CA, USA, May 16-18, 2017, Proceedings*, volume 10227 of *Lecture Notes in Computer Science*, pages 35–51.

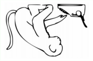
Baier, C. and Katoen, J. (2008).
Principles of Model Checking.
MIT Press.

Wang, T., Sun, J., Wang, X., Liu, Y., Si, Y., Dong, J. S., Yang, X., and Li, X. (2015).
A systematic study on explicit-state non-zenoness checking for timed automata.
IEEE Transactions on Software Engineering, 41(1):3–18.

Licensing

Source of the graphics used I

Title: Ocaml logo
Author: Amir Chaudhry
Source: https://commons.wikimedia.org/wiki/File:Smiley_green_alien_big_eyes.svg
License: CC BY-SA 4.0



Title: IMITATOR logo (Typing Monkey)
Author: Kater Begemot
Source: https://commons.wikimedia.org/wiki/File:Smiley_green_alien_big_eyes.svg
License: CC BY-SA 3.0

Title: PPL logo
Author: Unknown
Source: http://bugseng.com/files/ext/images/site/ppl_mm_8.png
License: GCC