Parametric model checking timed automata under non-Zenoness assumption

Hoang Gia Nguyen
LIPN, CNRS UMR 7030, Université Paris 13, Sorbonne Paris Cité, France

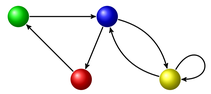
1. Context

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

Model checking [BK08] 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

(State: ● ; Transition: ⟶)



A model of the system

● is unreachable

A property to be satisfied

1.1 Timed systems checking question

- Does the model of the system satisfy the property?

Yes

No (Counterexample: ● → ● → ●)

1.2 Parametric timed systems checking question

- For which values of the parameters does the model of the system satisfy the property?

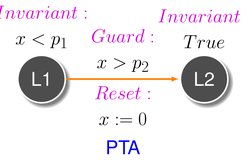
Some valuations

Empty

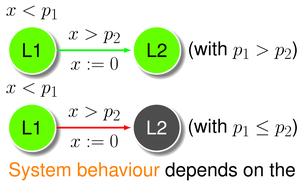
- This technique is used for modeling and verifying timed systems containing dense or unknown values

2. System model: Parametric timed automata - PTA

- A formalism to model and verify concurrent real-time systems [AHV93]
- 1 Parametric timed automaton (parameter) ↔ n Timed automata (concrete value)



PTA



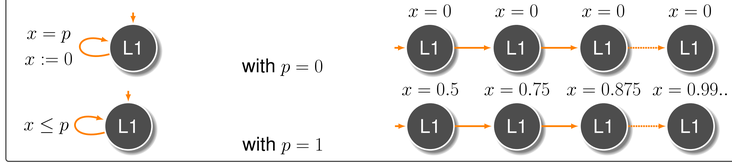
System behaviour depends on the values of parameters

x: Clock
p_1, p_2: Parameters with unknown values
K_0: Initial parameter contraint (e.g. $p_1 \leq p_2$ or $p_2 > p_1$)

3. Parametric model checking problem: Zeno run

A Zeno run is a run with an infinite number of actions within a finite time. Since such a behaviour is infeasible in practice and should not be considered as a counter-example!

- Run has a clock such that time cannot elapse or bounded by a parameter or a constant:



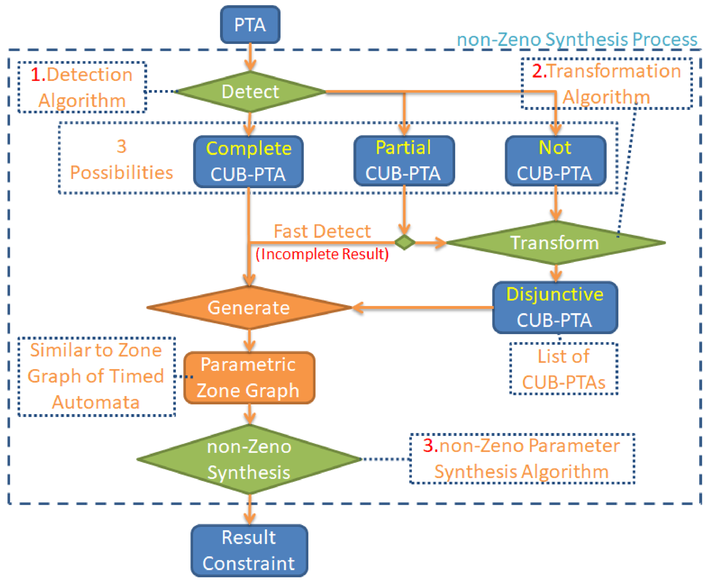
4. Non-Zeno model checking: CUB approach for PTA

CUB approach

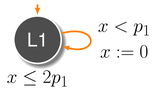
CUB [WSW+15] (Clock Upper Bound): an approach for solving the non-Zenoness problem on Timed Safety Automata

CUB-PTA definition

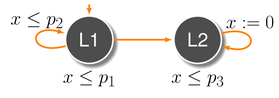
- A PTA $\mathcal{A}$ is a *CUB-PTA*, iff there exists a constraint $\mathcal{A}.K_0$ on parameters that guarantees every clock has a non-decreasing upper bound along any path before it is reset, for all parameter valuations satisfying the initial constraint $\mathcal{A}.K_0$
- A *disjunctive CUB-PTA* is a list of *CUB-PTA*s



4.1. CUB-PTA detection



Example 1: Not CUB-PTA
$\mathcal{A}.K_0 = (2p_1 < p_1)$ is False $(p1 \geq 0)$:
$\Rightarrow$ CUB-PTA for $\emptyset$



Example 2: Partial CUB-PTA
$\mathcal{A}.K_0 = p_1 \leq p_2 \wedge p_1 \leq p_3$:
$\Rightarrow$ CUB-PTA for $p_1 \leq p_2 \wedge p_1 \leq p_3$

Main idea

Given PTA $\mathcal{A}$, for each clock x on each edge with guard g from location l to l' we enforce a constraint with upper bound l_x less than or equal to g_x and l'_x (if x is not reset). If a conjunction of all constraints $\mathcal{A}.K_0$ contains some valuations then $\mathcal{A}$ is *CUB-PTA*.

References

[AFKS12] Étienne André, Laurent Fribourg, Ulrich Kühne, and Romain Soulat. IMITATOR 2.5: A tool for analyzing robustness in scheduling problems. In *FM*, volume 7436 of *Lecture Notes in Computer Science*, pages 33–36, 2012.

[AHV93] Rajeev Alur, Thomas A. Henzinger, and Moshe Y. Vardi. Parametric real-time reasoning. In *STOC*, pages 592–601. ACM, 1993.

[ANPS17] Étienne André, Hoang Gia Nguyen, Laure Petrucci, and Jun Sun. Parametric model checking timed automata under non-zenoness assumption. In Clark Barrett, Misty Davies, and Temesghen Kahsai, 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, 2017.

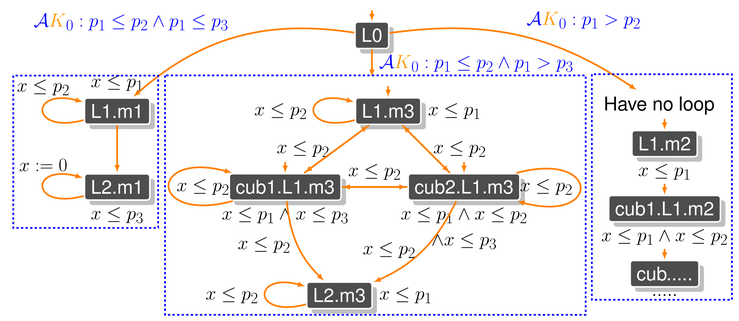
[BK08] C. Baier and J.P. Katoen. *Principles of Model Checking*. MIT Press, 2008.

[HSW12] Frédéric Herbreteau, B. Srivathsan, and Igor Walukiewicz. Efficient emptiness check for timed Büchi automata. *Formal Methods in System Design*, 40(2):122–146, 2012.

[TYB05] Stavros Tripakis, Sergio Yovine, and Ahmed Bouajjani. Checking timed Büchi automata emptiness efficiently. *Formal Methods in System Design*, 26(3):267–292, 2005.

[WSW+15] Ting Wang, Jun Sun, Xinyu Wang, Yang Liu, Yuanjie Si, Jin Song Dong, Xiaohu Yang, and Xiaohong Li. A systematic study on explicit-state non-Zenoness checking for timed automata. *IEEE Transactions on Software Engineering*, 41(1):3–18, 2015.

4.2. CUB-PTA transformation

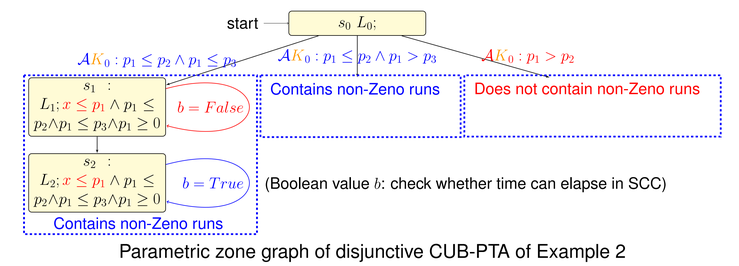


Disjunctive CUB-PTA of Example 2

Main idea

An PTA can be transformed into a disjunctive CUB-PTA by infering all possible $\mathcal{A}.K_0$. Then each copy of $\mathcal{A}$ (mX) will be transformed into CUB-PTA with lower upper bound locations (cubX) for each $\mathcal{A}.K_0$.

4.3. Non-Zenoness parametric model checking



(Boolean value b: check whether time can elapse in SCC)

Parametric zone graph of disjunctive CUB-PTA of Example 2

Emptiness non-Zeno check result:

- Example 1: Detection: Empty — Transformation: $0 < p_1$
- Example 2: Detection: $p_1 \leq p_2 \wedge p_1 \leq p_3$ — Transformation: $p_1 \leq p_2$ (more values)

Main idea

A *CUB-PTA* $\mathcal{A}$ contains a non-Zeno run iff:

- There exists parameter valuations such that the parametric zone graph $PZG(\mathcal{A})$ has a SCC containing an edge from location l to l' where time can elapse
- For every clock x in $\mathcal{A}$, if x is bounded by a constant or a parameter for some location in the SCC, there exists an edge in the SCC where x is reset

5. Implementation and experiments

- All our algorithms are implemented in IMITATOR [André, Fribourg, Kühne, Soulat, 2012] , a parameter synthesis tool for real-time systems
- For the experiment please find in our full paper: Parametric model checking timed automata under non-Zenoness assumption [ANPS17]

6. Conclusion and future works

- Proposed and implemented new Zeno-free parametric model synthesizing approaches in IMITATOR tool
- Implement other techniques such as yet to be defined parametric extensions of strongly non-Zeno TAs [TYB05] and guessing zone graph [HSW12]