Séminaire LoVe

11 mars 2022

Lightweight (yet efficient) verification of cyber-physical systems

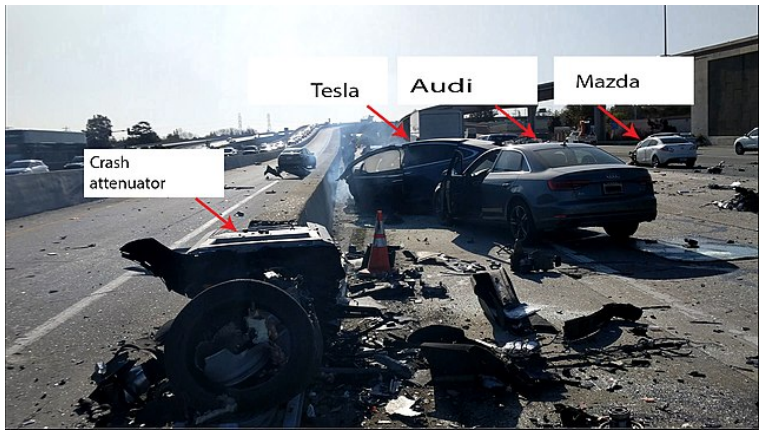
Étienne André

Université de Lorraine, CNRS, Inria, LORIA, Nancy, France
Joint work with Masaki Waga and Ichiro Hasuo

CC BY SA

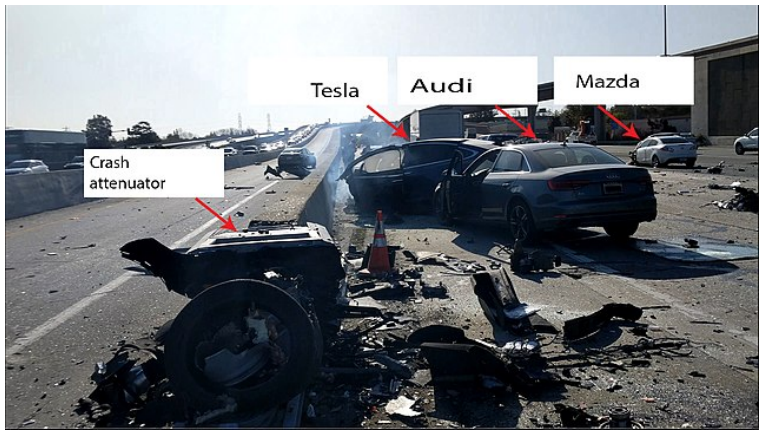
Outline

Context : safety-critical cyber-physical systems



Images illustrating Tesla fatal crashes : Williston, Florida, USA [May 7, 2016]; Mountain View, California, USA [March 23, 2018]

Context : safety-critical cyber-physical systems



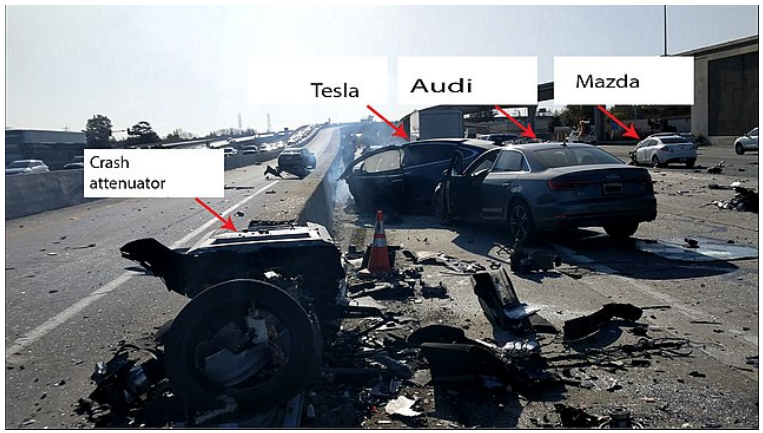
Images illustrating Tesla fatal crashes : Williston, Florida, USA [May 7, 2016]; Mountain View, California, USA [March 23, 2018]

Formal verification of complex cyber-physical systems : out of reach ?

Lightweight verification

- Testing
- Monitoring, runtime verification

Context : safety-critical cyber-physical systems



Images illustrating Tesla fatal crashes : Williston, Florida, USA [May 7, 2016]; Mountain View, California, USA [March 23, 2018]

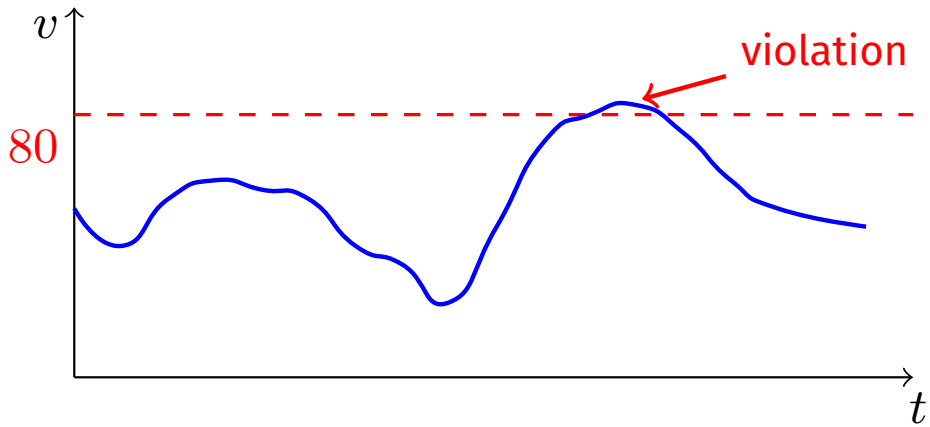
Formal verification of complex cyber-physical systems : out of reach ?

Lightweight verification

- Testing
- Monitoring, runtime verification

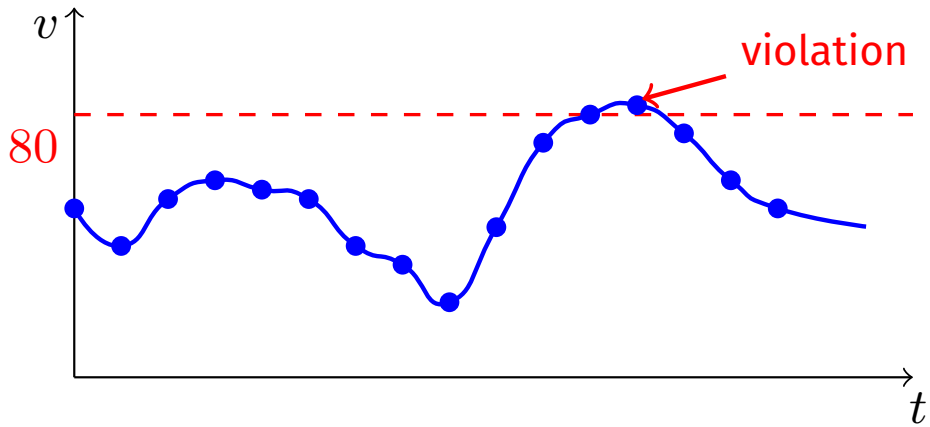
Monitoring cyber-physical systems

Specification : $\neg(v > 80)$



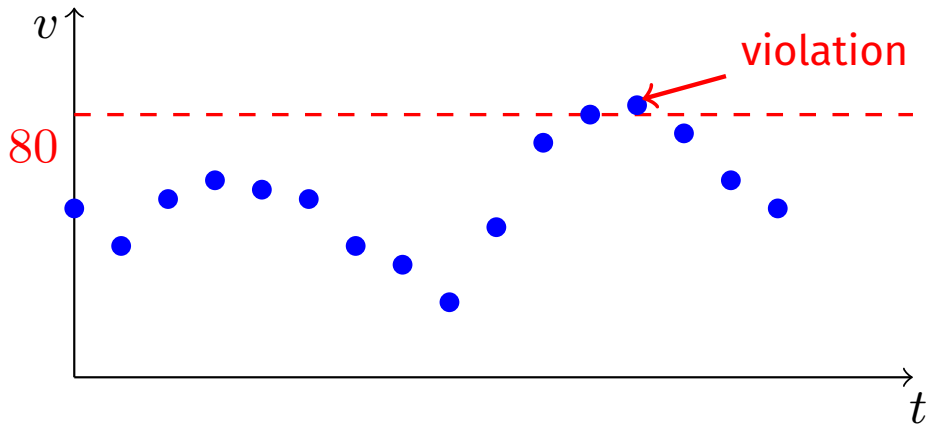
Monitoring cyber-physical systems with sampling

Specification : $\neg(v > 80)$



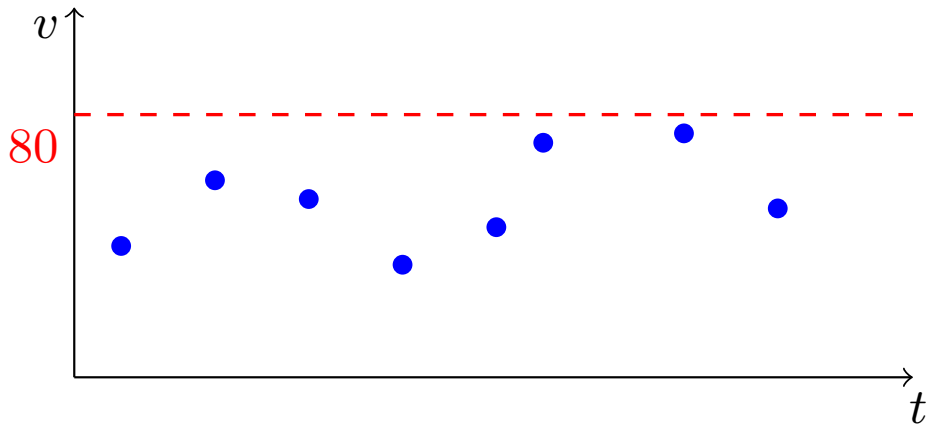
Monitoring cyber-physical systems with sampling

Specification : $\neg(v > 80)$



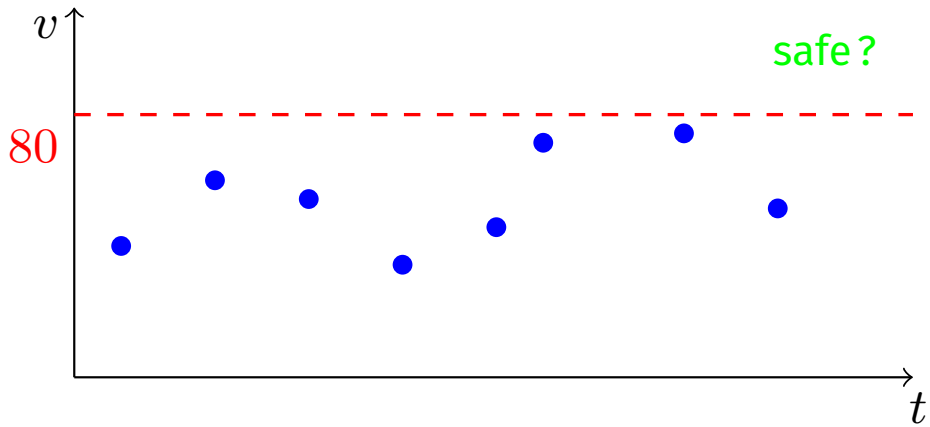
Monitoring cyber-physical systems with sampling

Specification : $\neg(v > 80)$



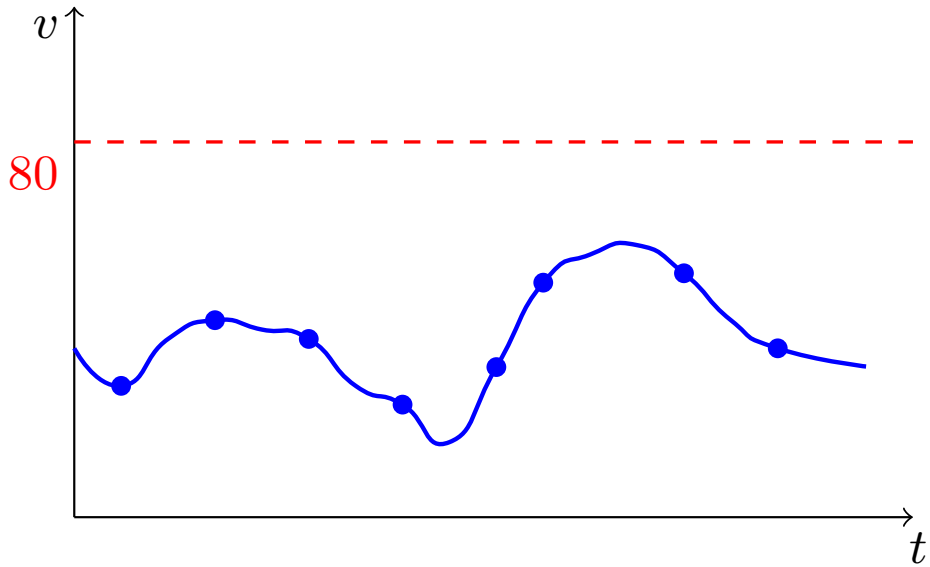
Monitoring cyber-physical systems with sampling

Specification : $\neg(v > 80)$



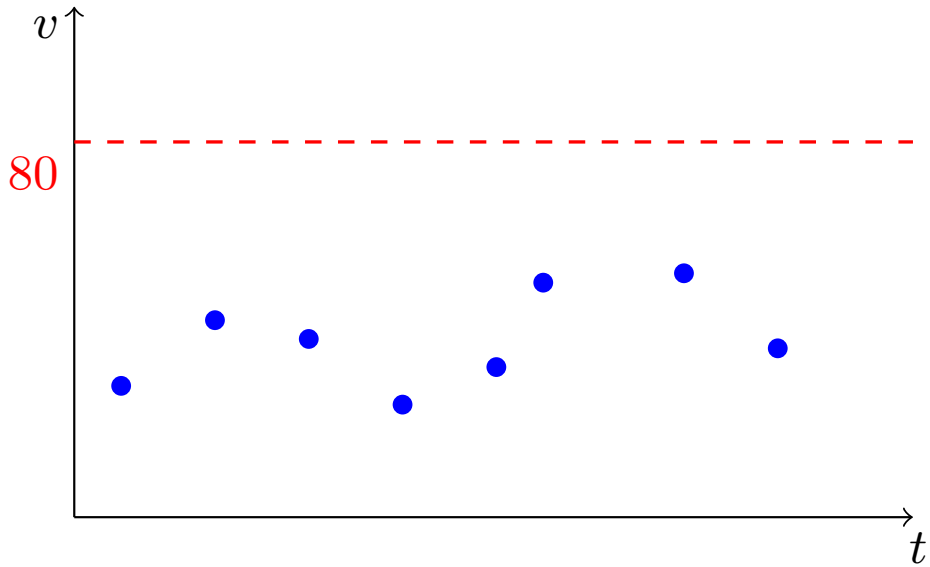
Signal interpolation

Specification : $\neg(v > 80)$



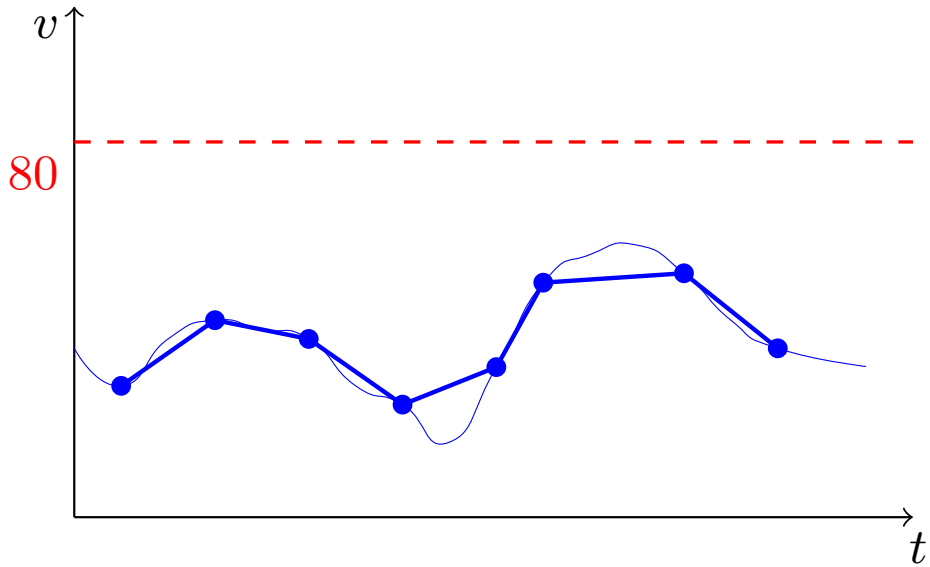
Signal interpolation

Specification : $\neg(v > 80)$



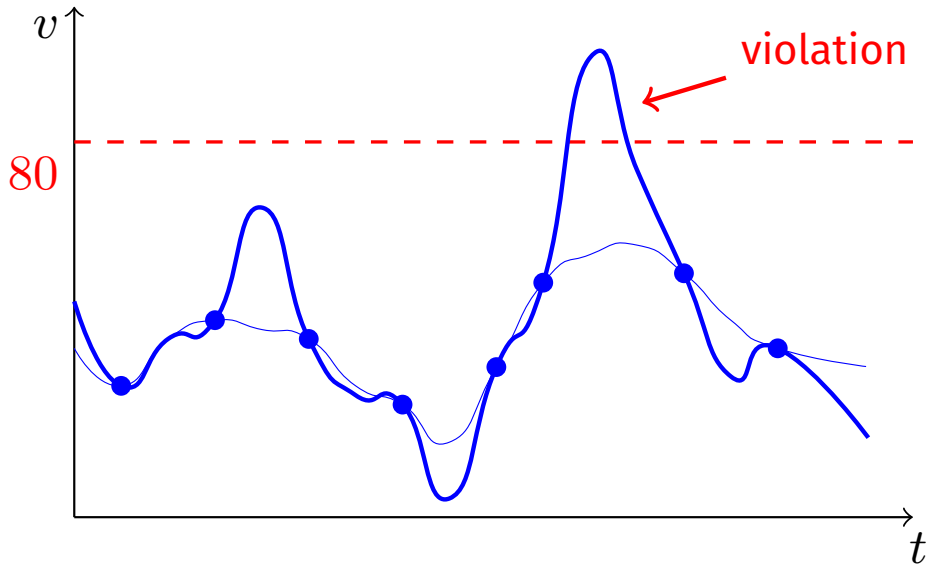
Signal interpolation

Specification : $\neg(v > 80)$



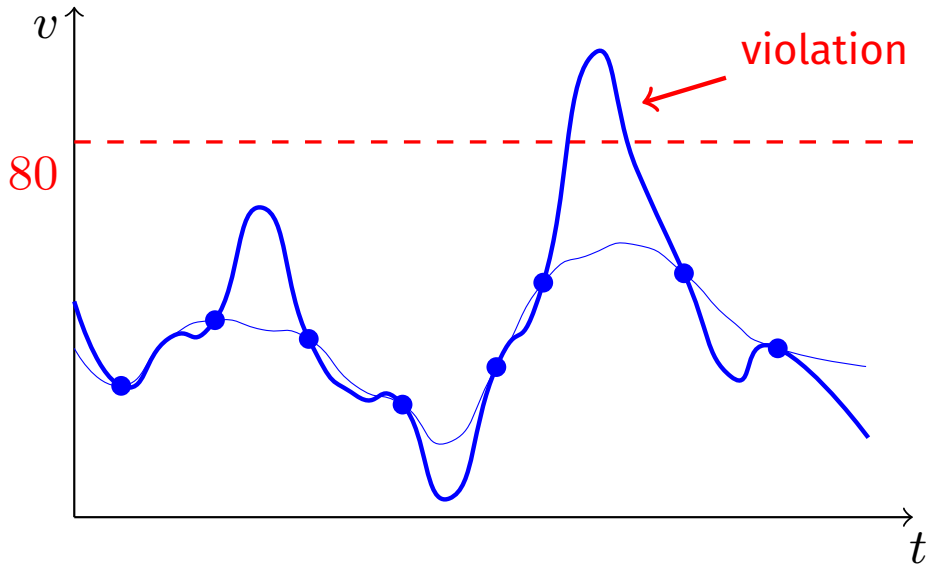
Signal interpolation

Specification : $\neg(v > 80)$



Signal interpolation with prior knowledge

Specification : $\neg(v > 80)$



Impossible violation because we know that $\frac{dv}{dt} < K$ (for some known K)

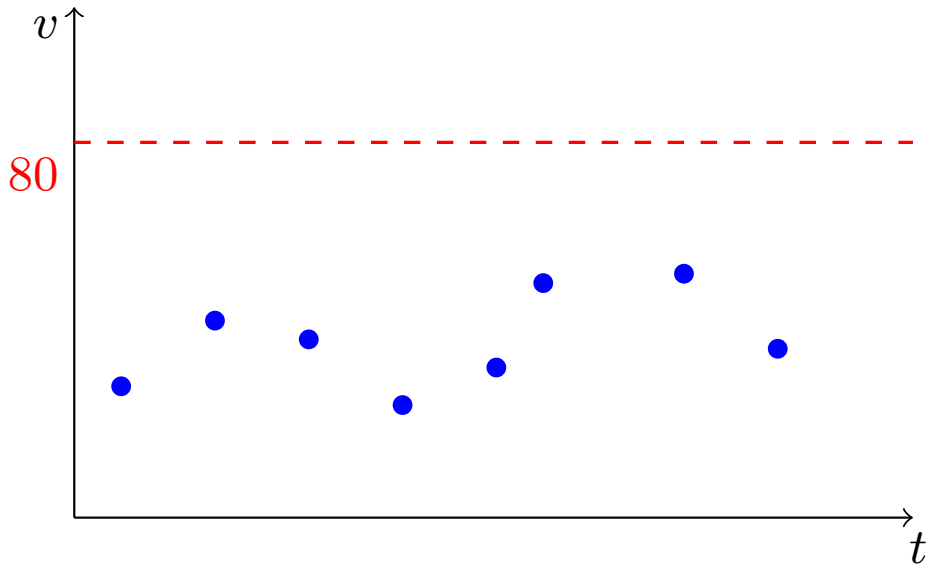
Example : a car cannot accelerate arbitrarily fast

Outline

Model-bounded monitoring [WAH21]

Specification : $\neg(v > 80)$

System log

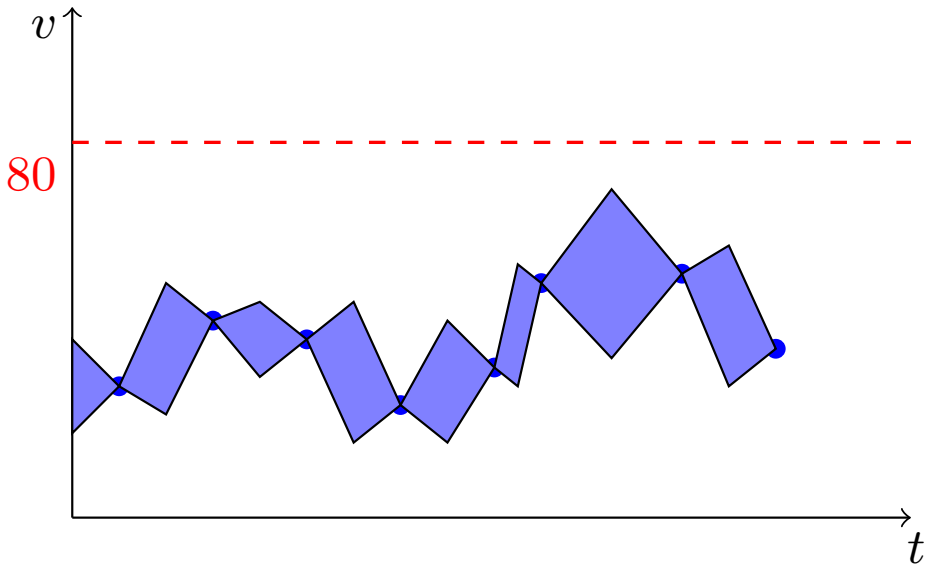


. [WAH21] Masaki Waga, Étienne André et Ichiro Hasuo. « Model-bounded monitoring of hybrid systems ». In : *ICCPS*. ACM, 2021, p. 21-32

Model-bounded monitoring [WAH21]

Specification : $\neg(v > 80)$

System log + knowledge (bounded model) ($\frac{dv}{dt} < K$)

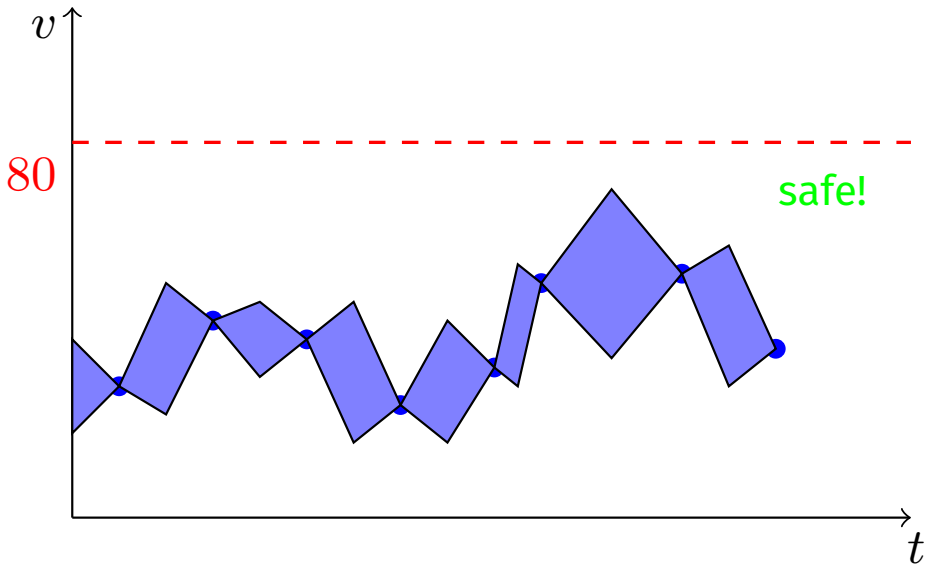


. [WAH21] Masaki Waga, Étienne André et Ichiro Hasuo. « Model-bounded monitoring of hybrid systems ». In : *ICCPS*. ACM, 2021, p. 21-32

Model-bounded monitoring [WAH21]

Specification : $\neg(v > 80)$

System log + knowledge (bounded model) ($\frac{dv}{dt} < K$)



. [WAH21] Masaki Waga, Étienne André et Ichiro Hasuo. « Model-bounded monitoring of hybrid systems ». In : *ICCPS*. ACM, 2021, p. 21-32

The bounding model : a linear hybrid automaton

A bounding model should :

- ☺ be expressive
- ☺ yet allow for efficient computation

. [Hen96] Thomas A. Henzinger. « The Theory of Hybrid Automata ». In : *LiCS*. IEEE Computer Society, 1996, p. 278-292

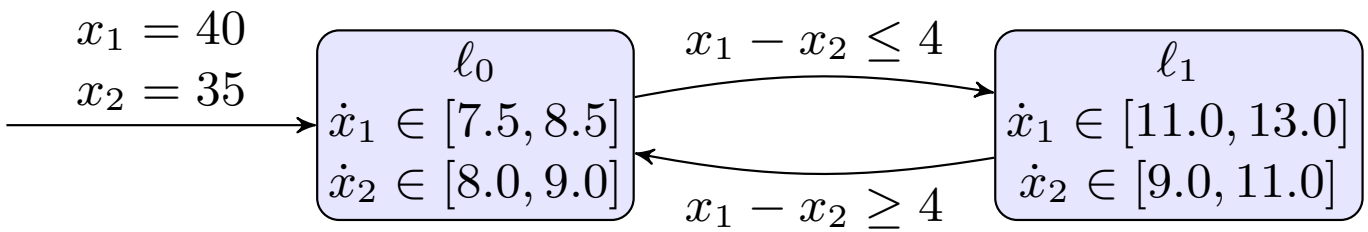
The bounding model : a linear hybrid automaton

A bounding model should :

- ☺ be expressive
- ☺ yet allow for efficient computation

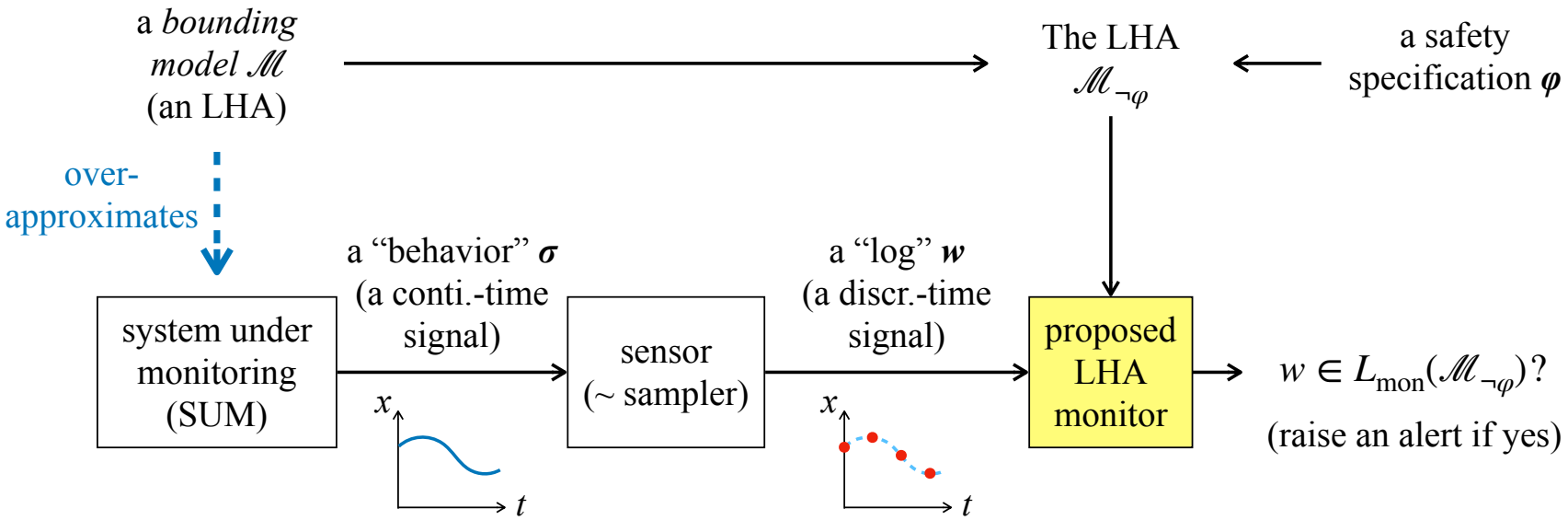
Our formalism : linear hybrid automata [Hen96]

- discrete modes
- invariants, guards, derivatives expressed by polyhedra

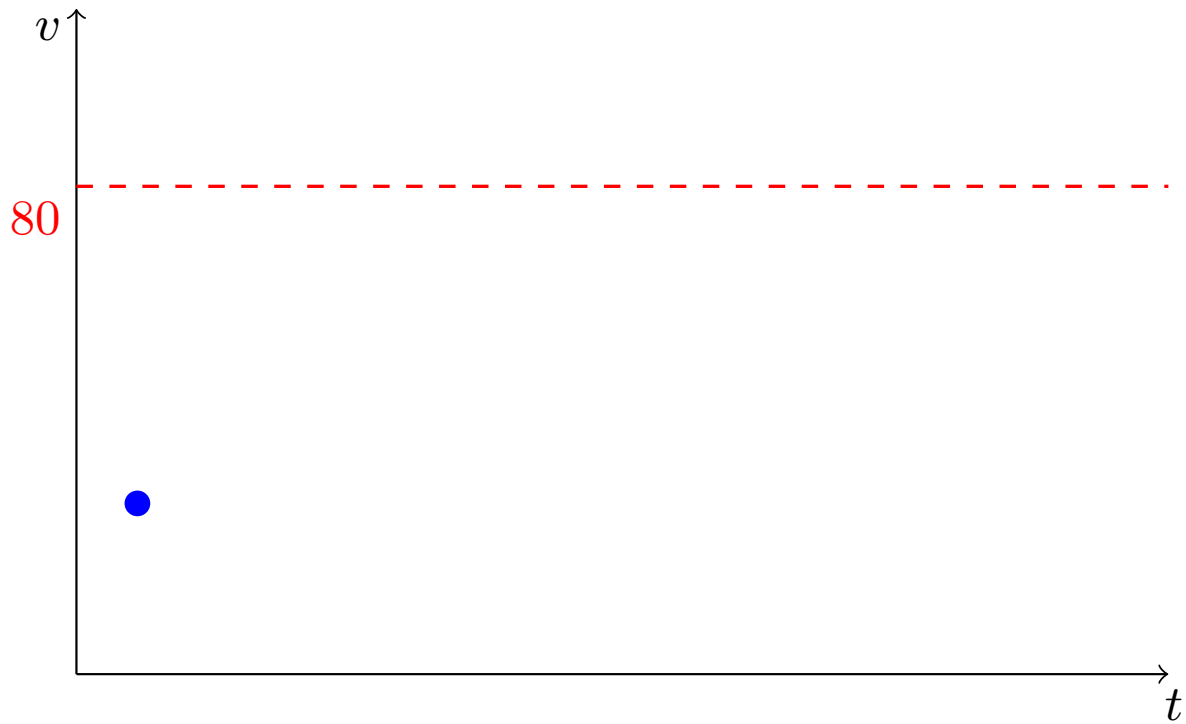


. [Hen96] Thomas A. Henzinger. « The Theory of Hybrid Automata ». In : *LiCS*. IEEE Computer Society, 1996, p. 278-292

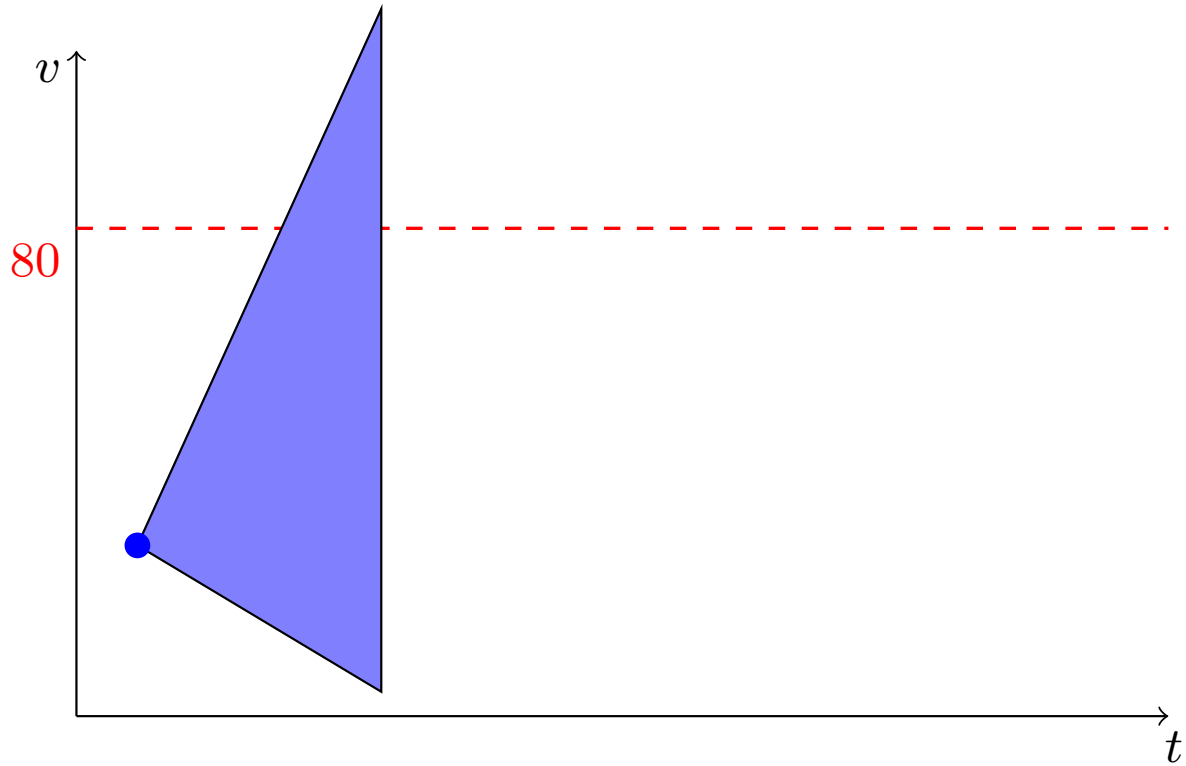
Model-bounded monitoring in a nutshell



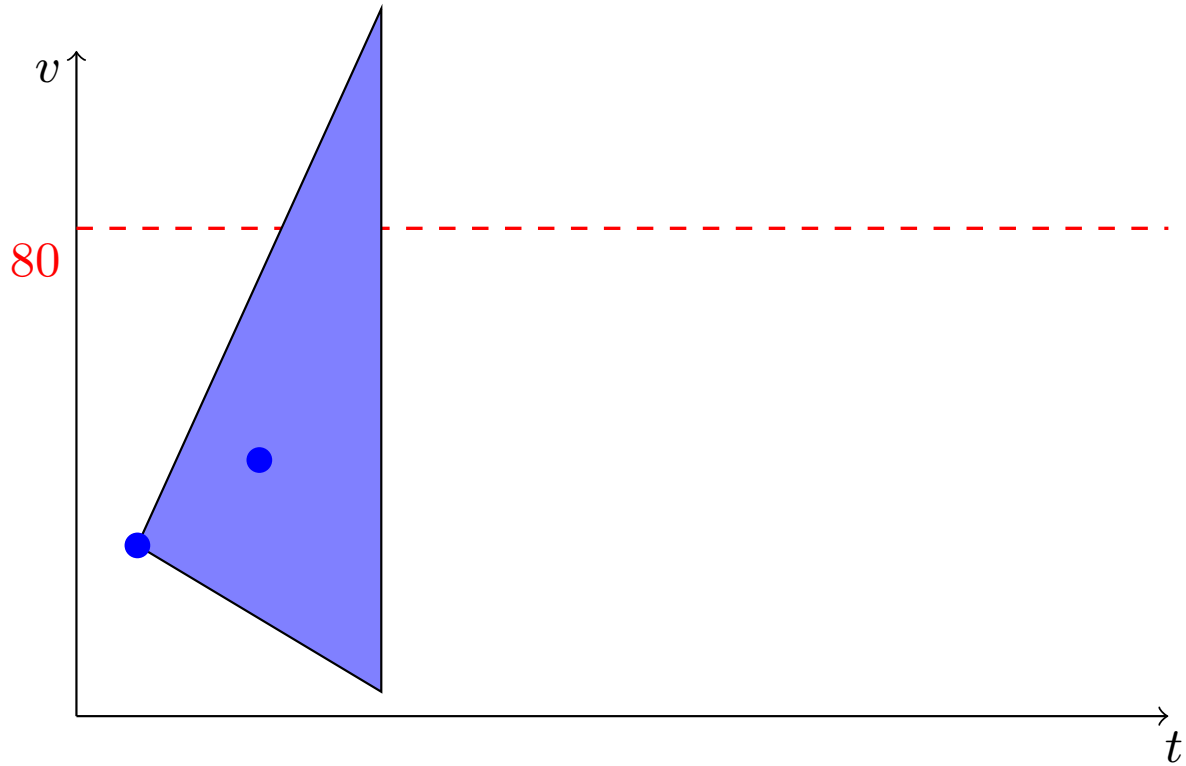
Algorithm : bounded-time reachability



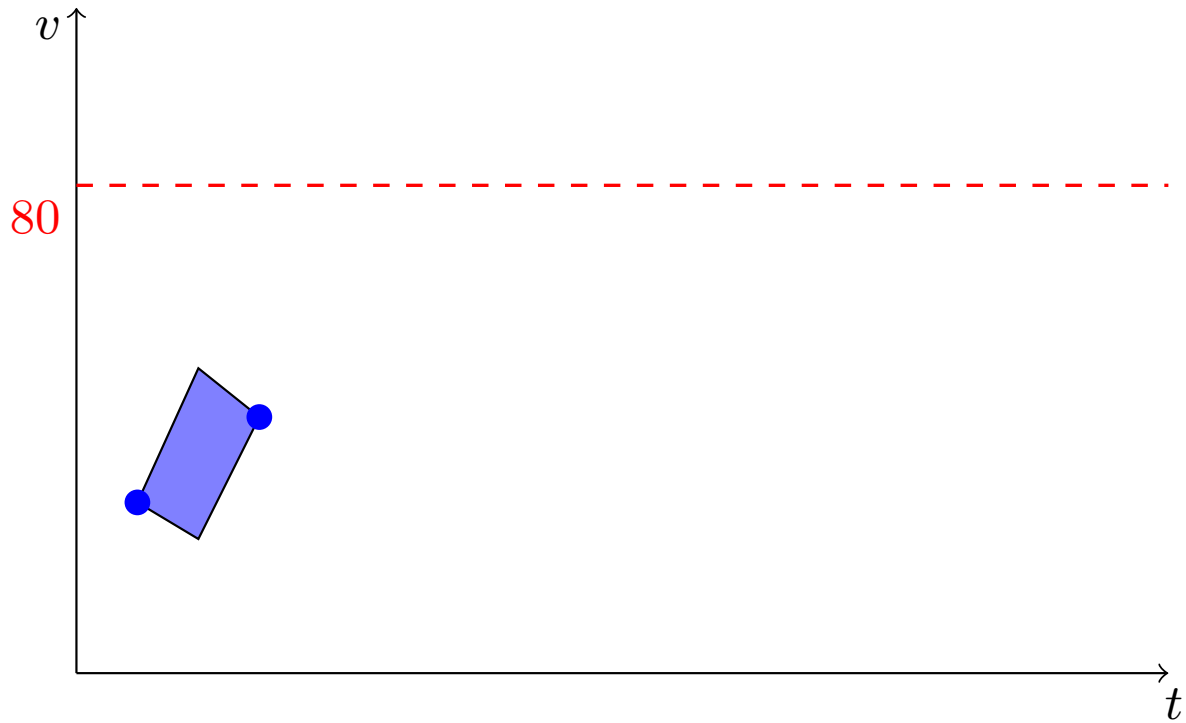
Algorithm : bounded-time reachability



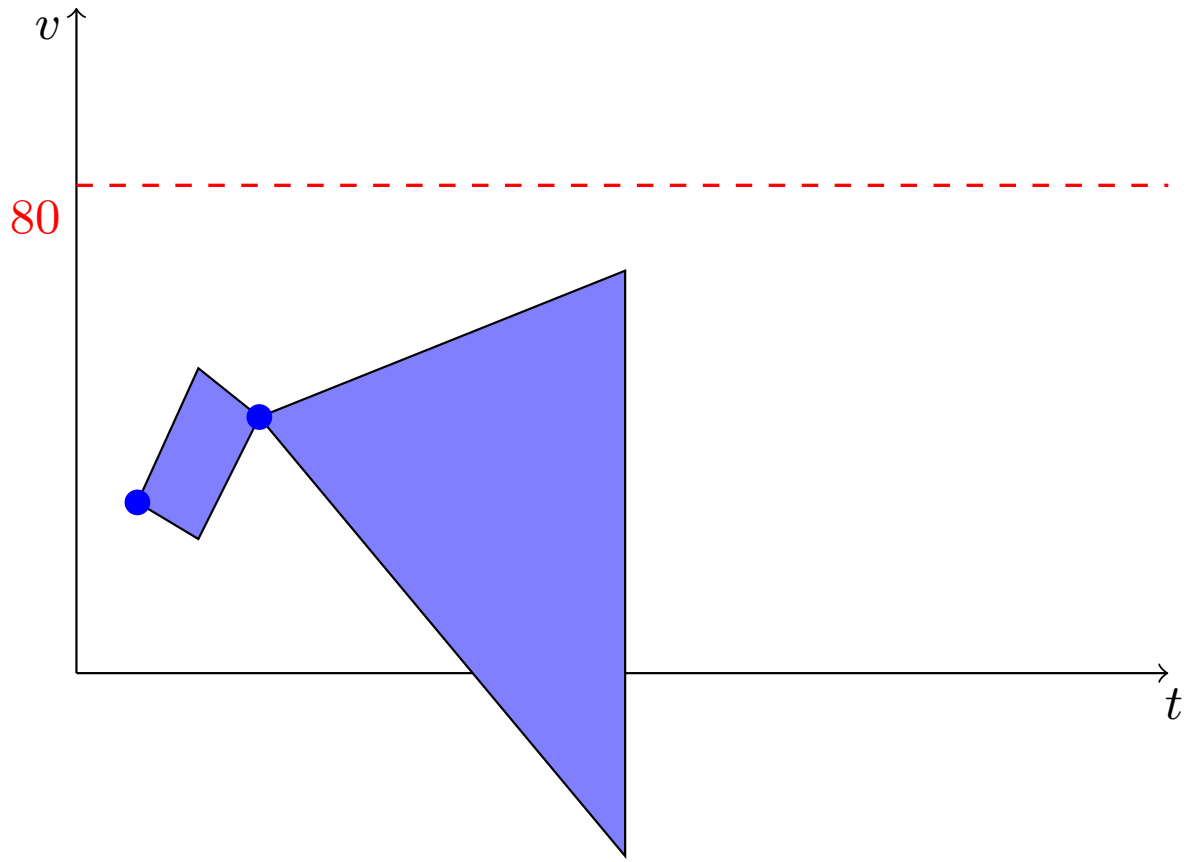
Algorithm : bounded-time reachability



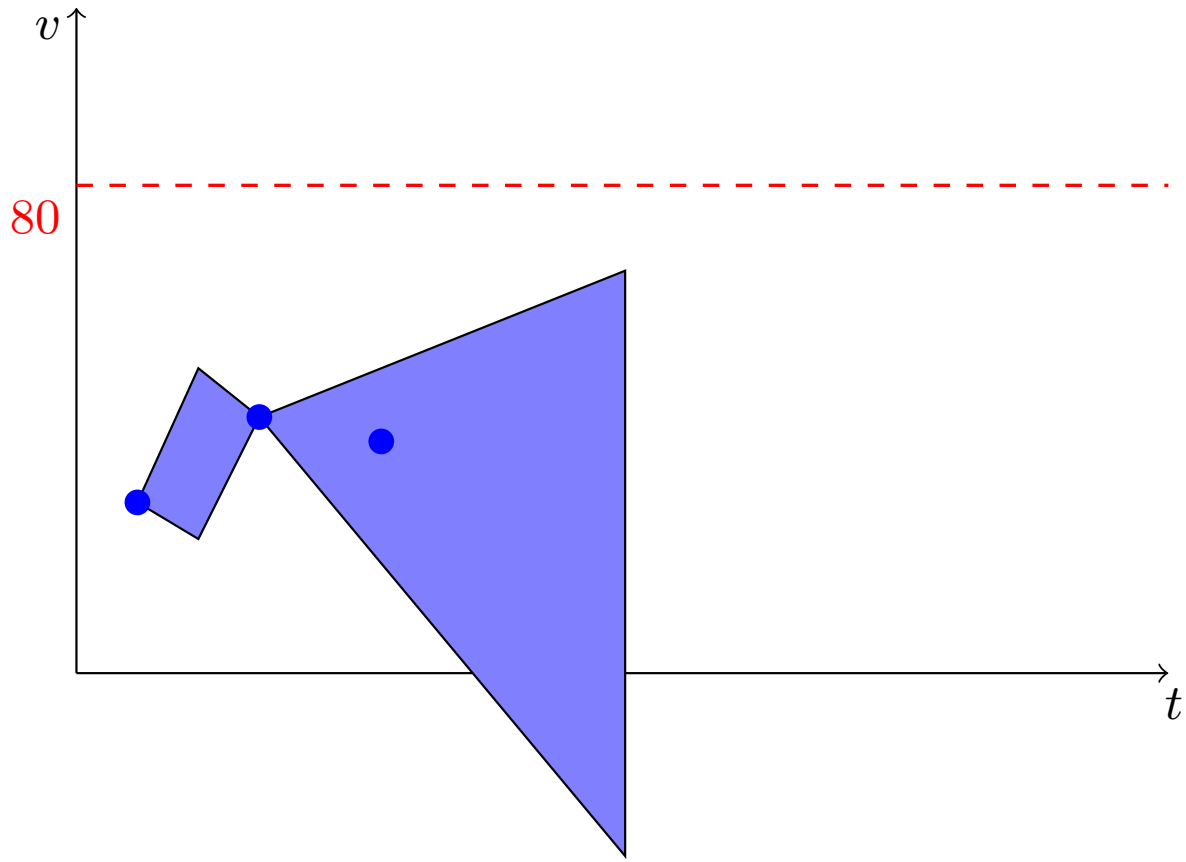
Algorithm : bounded-time reachability



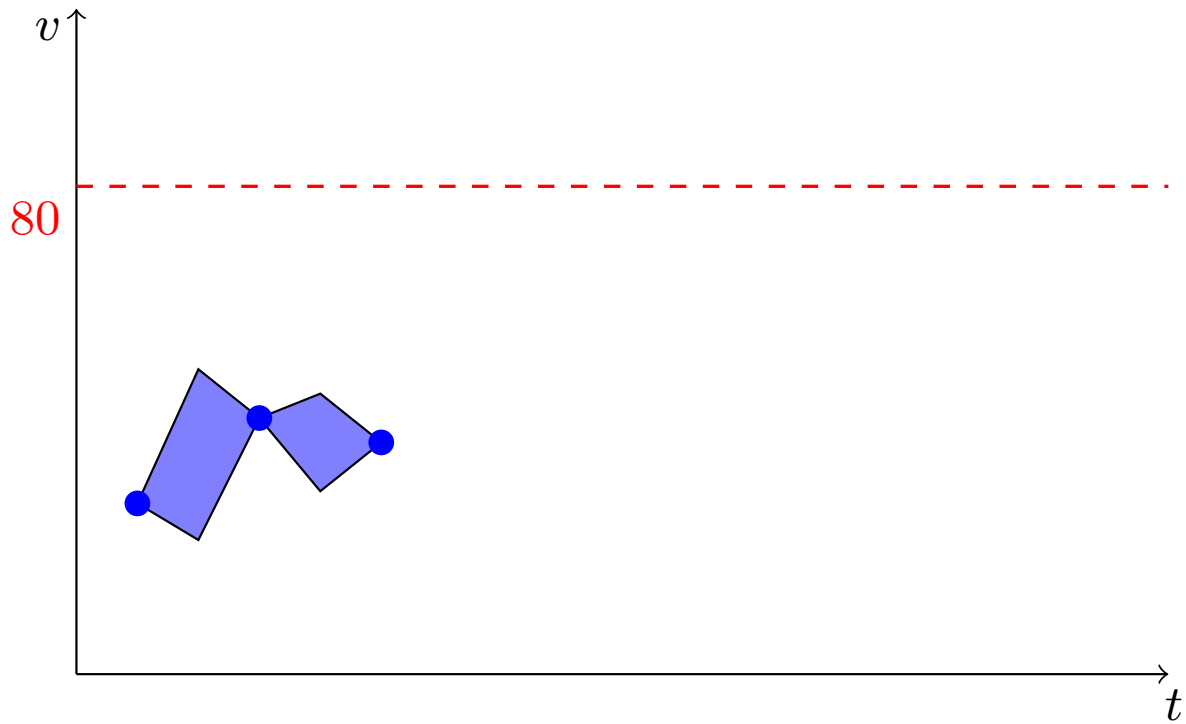
Algorithm : bounded-time reachability



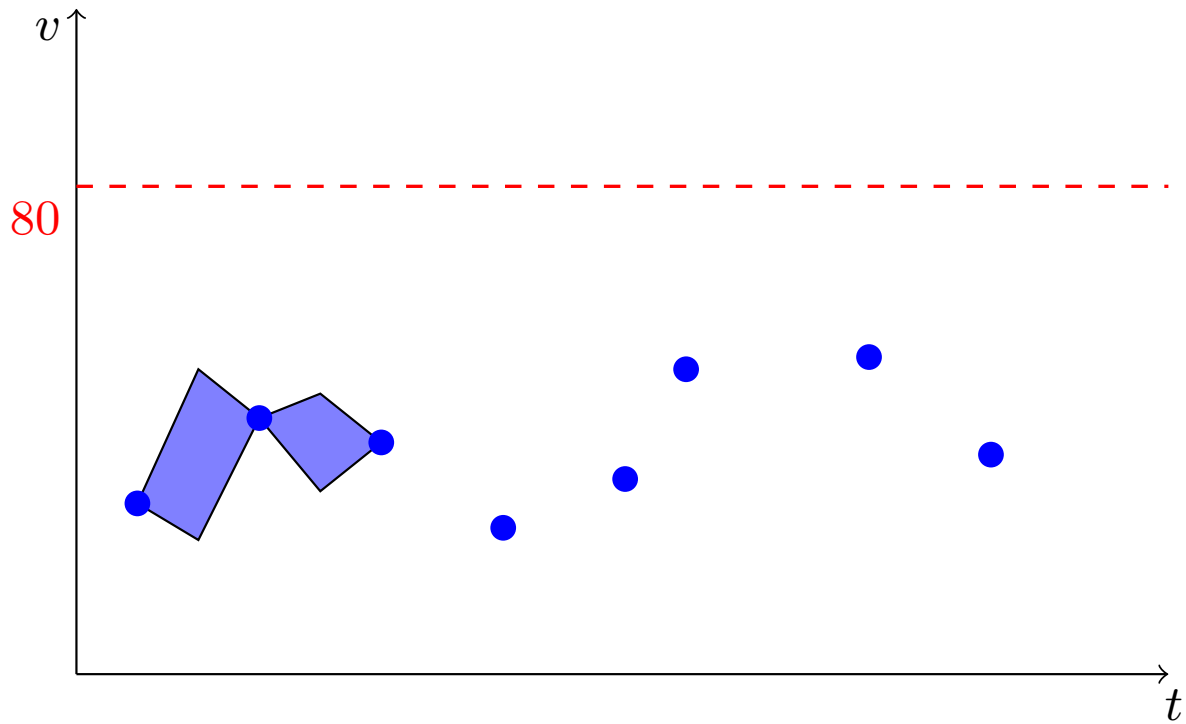
Algorithm : bounded-time reachability



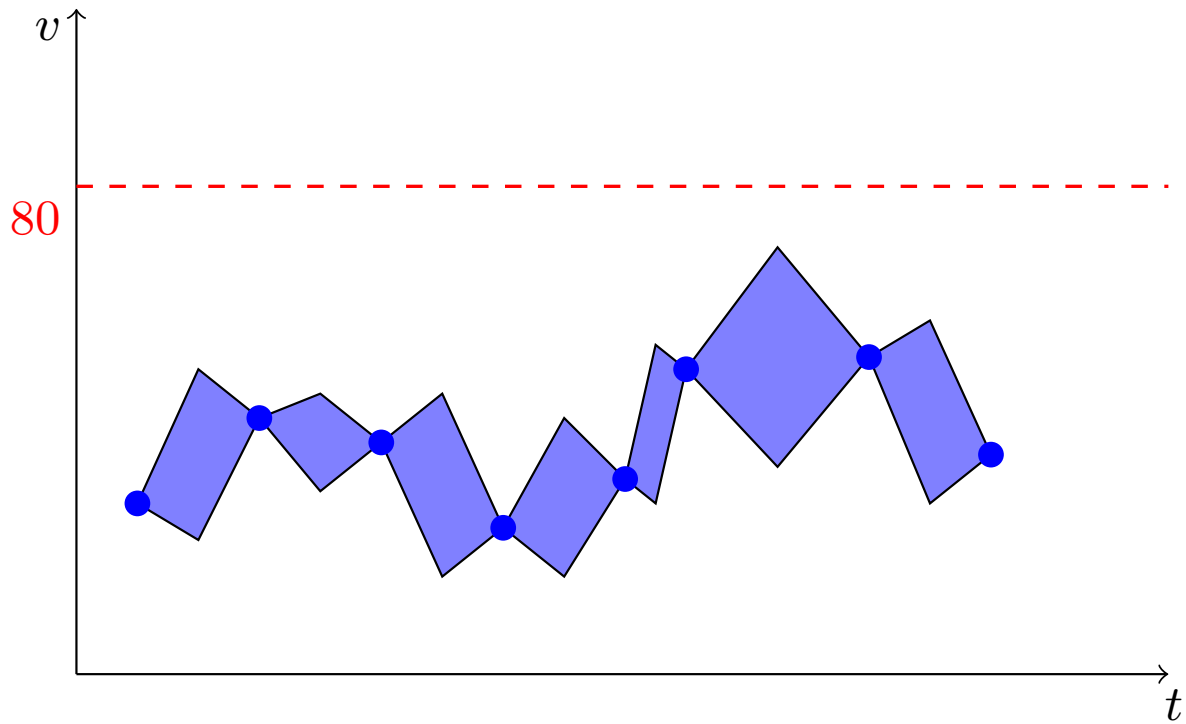
Algorithm : bounded-time reachability



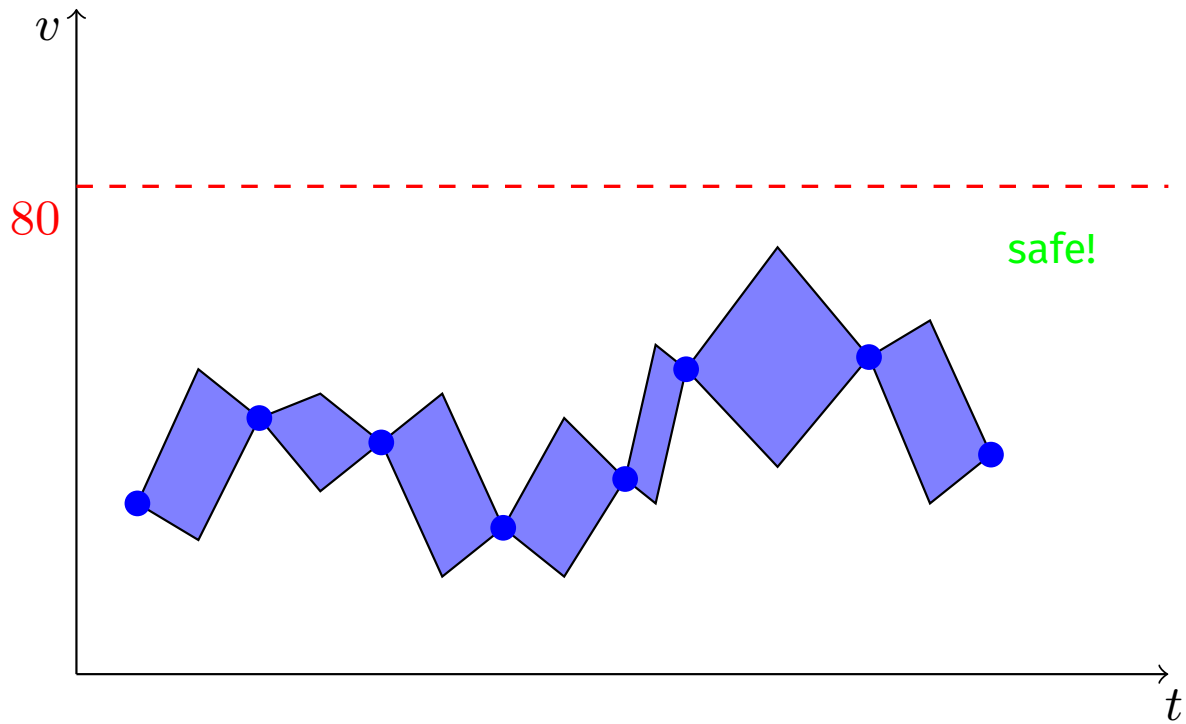
Algorithm : bounded-time reachability



Algorithm : bounded-time reachability



Algorithm : bounded-time reachability



Are linear hybrid automata efficient?

☹ Reachability analysis in (linear) hybrid automata is very hard

- Long line of research (e. g., [Bu+19] [Bog+20])

. [Bu+19] Lei Bu, Jiawan Wang, Yuming Wu et Xuandong Li. « From Bounded Reachability Analysis of Linear Hybrid Automata to Verification of Industrial CPS and IoT ». In : *SETSS*. T. 12154. LNCS. Springer, 2019, p. 10-43

. [Bog+20] Sergiy Bogomolov, Marcelo Forets, Goran Frehse, Kostiantyn Potomkin et Christian Schilling. « Reachability Analysis of Linear Hybrid Systems via Block Decomposition ». In : *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 39.11 (2020), p. 4018-4029

Are linear hybrid automata efficient?

☹ Reachability analysis in (linear) hybrid automata is very hard

- Long line of research (e. g., [Bu+19] [Bog+20])

☺ But in our scheme we "reset" the uncertainty at each new sample

- No error accumulation, no divergence

. [Bu+19] Lei Bu, Jiawan Wang, Yuming Wu et Xuandong Li. « From Bounded Reachability Analysis of Linear Hybrid Automata to Verification of Industrial CPS and IoT ». In : *SETSS*. T. 12154. LNCS. Springer, 2019, p. 10-43

. [Bog+20] Sergiy Bogomolov, Marcelo Forets, Goran Frehse, Kostiantyn Potomkin et Christian Schilling. « Reachability Analysis of Linear Hybrid Systems via Block Decomposition ». In : *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 39.11 (2020), p. 4018-4029

Outline

Two implementations

Approach 1 : existing model-checker PHAVerLite [BZ19]

- Light fork of PHAVerLite [Fre08]
- ☺ Highly optimized reachability analysis

Approach 2 : *ad hoc* dedicated monitor HAMoni (by Masaki Waga)

- ☺ Best performance in theory

. [BZ19] Anna Becchi et Enea Zaffanella. « Revisiting Polyhedral Analysis for Hybrid Systems ». In : *SAS*. T. 11822. LNCS. Springer, 2019, p. 183-202

. [Fre08] Goran Frehse. « PHAVer : Algorithmic Verification of Hybrid Systems Past HyTech ». In : *International Journal on Software Tools for Technology Transfer* 10.3 (mai 2008), p. 263-279. ISSN : 1433-2779

Benchmarks

Three main benchmarks :

1. Adaptive cruise controller [BRS19]
2. Robot navigation benchmark [FI04]
3. Shared Gas-Burner [DHR05]

. [BRS19] Lei Bu, Rajarshi Ray et Stefan Schupp. « ARCH-COMP19 Category Report : Bounded Model Checking of Hybrid Systems with Piecewise Constant Dynamics ». In : *ARCH@CPSIoTWeek*. T. 61. EPiC Series in Computing. EasyChair, 2019, p. 120-128

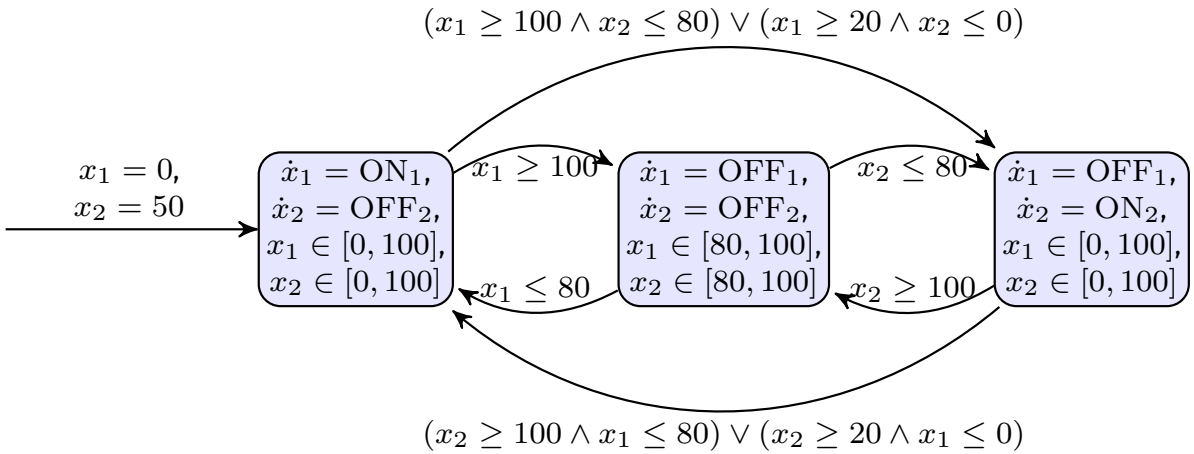
. [FI04] Ansgar Fehnker et Franjo Ivancic. « Benchmarks for Hybrid Systems Verification ». In : *HSCC*. T. 2993. LNCS. Springer, 2004, p. 326-341

. [DHR05] Laurent Doyen, Thomas A. Henzinger et Jean-François Raskin. « Automatic Rectangular Refinement of Affine Hybrid Systems ». In : *FORMATS*. T. 3829. LNCS. Springer, 2005, p. 144-161

Benchmarks : bounding models

Bounding models : mostly taken from the literature

- Example : GasBurner :

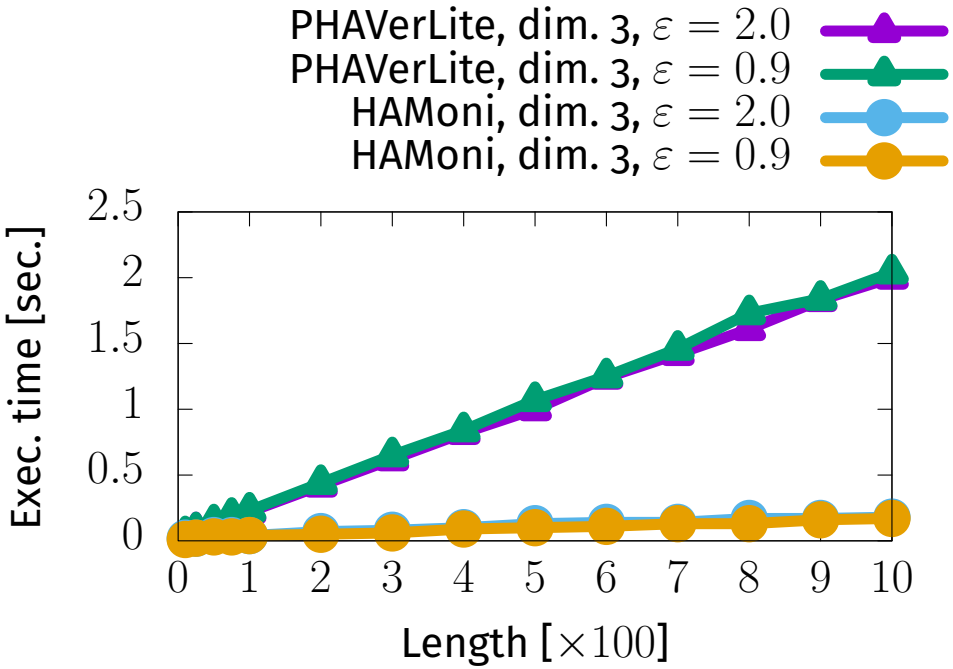


The affine hybrid automaton for the original model in GasBurner, where $h = 2, a = 0.01, b = 0.005, \mathrm{ON}_1 = h - ax_1 + bx_2$, $\mathrm{ON}_2 = h - ax_2 + bx_1, \mathrm{OFF}_1 = -ax_1 + bx_2$, and $\mathrm{OFF}_2 = -ax_2 + bx_1$.

Logs : randomly generated from the bounding models (this coincidence is not mandatory)

- Length of the logs : 150 to 100,000

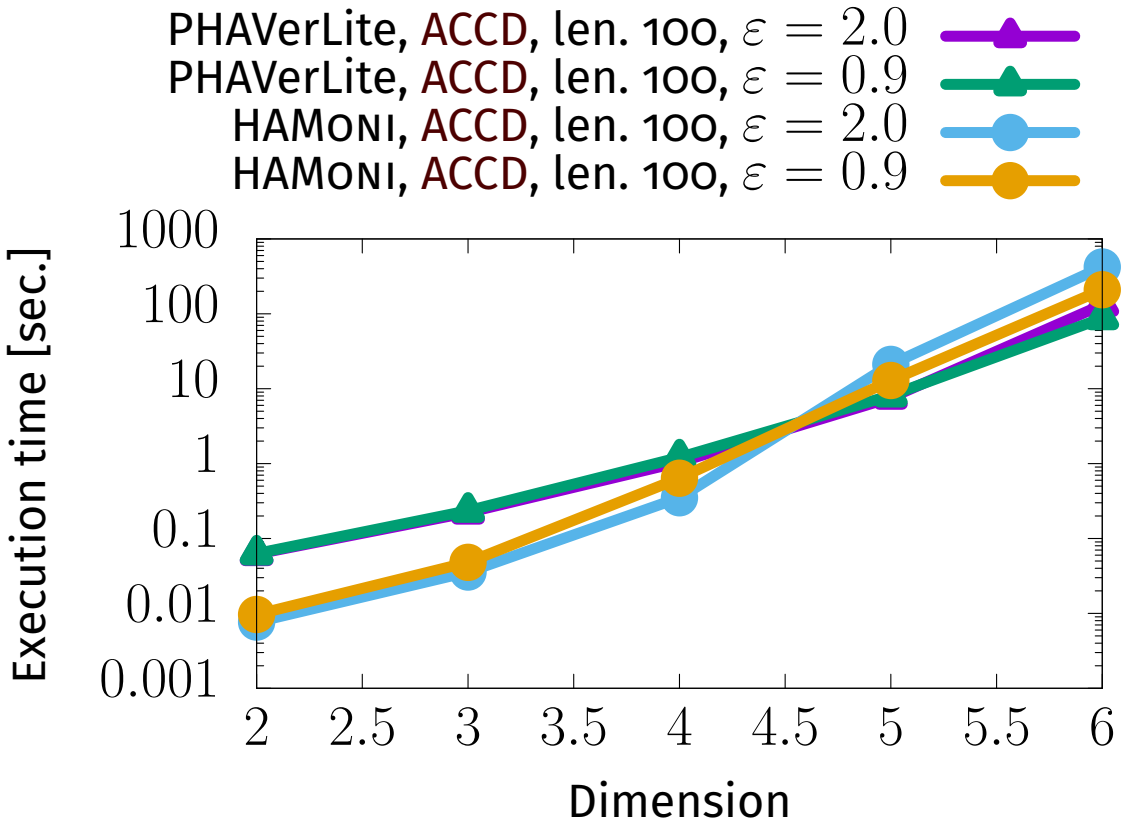
Changing observation length



Conclusions :

- linear
- very scalable : $> 5,000$ samples / second
- Our tool HAMoni is about 10 times faster than the existing PHAVerLite

Changing model dimension



Conclusions :

- Existing model checker PHAVerLite faster for dimensions > 6
- Future work : further optimization of our tool HAMoNi

Outline

Conclusion

Model-bounded monitoring

- Bounding model (prior knowledge) : linear hybrid automaton

Algorithms and implementations

- Idea : bounded-time reachability
- Crux : no error accumulation due to new sampling
- Experiments : effectively monitorable

Conclusion

Model-bounded monitoring

- Bounding model (prior knowledge) : linear hybrid automaton

Algorithms and implementations

- Idea : bounded-time reachability
- Crux : no error accumulation due to new sampling
- Experiments : effectively monitorable

Joint patent : NII (Japan) + Université de Lorraine (France)

Perspectives

- Monitoring beyond safety
  - Monitoring against temporal properties
- Uncertainties in the observation
  - partial logs
  - values known with uncertainties
- Uncertainty in the specification
  - Timing parameters
- Quantitative monitoring
  - “By how much is the specification violated ?”

Bibliography

References I

Étienne André, Ichiro Hasuo et Masaki Waga. « Offline timed pattern matching under uncertainty ». In : *ICECCS* (12-14 déc. 2018). Sous la dir. d'Anthony Widjaja Lin et Jun Sun. Melbourne, Australia : IEEE Computer Society, 2018, p. 10-20. DOI : 10.1109/ICECCS2018.2018.00010.

Sergiy Bogomolov, Marcelo Forets, Goran Frehse, Kostiantyn Potomkin et Christian Schilling. « Reachability Analysis of Linear Hybrid Systems via Block Decomposition ». In : *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 39.11 (2020), p. 4018-4029. DOI : 10.1109/TCAD.2020.3012859.

Lei Bu, Rajarshi Ray et Stefan Schupp. « ARCH-COMP19 Category Report : Bounded Model Checking of Hybrid Systems with Piecewise Constant Dynamics ». In : *ARCH@CPSIoTWeek* (15 avr. 2019). T. 61. EPiC Series in Computing. Montréal, QC, Canada : EasyChair, 2019, p. 120-128.

Lei Bu, Jiawan Wang, Yuming Wu et Xuandong Li. « From Bounded Reachability Analysis of Linear Hybrid Automata to Verification of Industrial CPS and IoT ». In : *SETSS* (21-27 avr. 2019). T. 12154. LNCS. Chongqing, China : Springer, 2019, p. 10-43. DOI : 10.1007/978-3-030-55089-9_2.

Anna Becchi et Enea Zaffanella. « Revisiting Polyhedral Analysis for Hybrid Systems ». In : *SAS* (8-11 oct. 2019). Sous la dir. de Bor-Yuh Evan Chang. T. 11822. LNCS. Porto, Portugal : Springer, 2019, p. 183-202. DOI : 10.1007/978-3-030-32304-2_10.

References II

Laurent Doyen, Thomas A. Henzinger et Jean-François Raskin. « Automatic Rectangular Refinement of Affine Hybrid Systems ». In : *FORMATS* (26-28 sept. 2005). Sous la dir. de Paul Pettersson et Wang Yi. T. 3829. LNCS. Uppsala, Sweden : Springer, 2005, p. 144-161. DOI : 10.1007/11603009_13.

Ansgar Fehnker et Franjo Ivancic. « Benchmarks for Hybrid Systems Verification ». In : *HSCC* (25-27 mar. 2004). Sous la dir. de Rajeev Alur et George J. Pappas. T. 2993. LNCS. Philadelphia, PA, USA : Springer, 2004, p. 326-341. DOI : 10.1007/978-3-540-24743-2_22.

Goran Frehse. « PHAVer : Algorithmic Verification of Hybrid Systems Past HyTech ». In : *International Journal on Software Tools for Technology Transfer* 10.3 (mai 2008), p. 263-279. ISSN : 1433-2779. DOI : 10.1007/s10009-007-0062-x.

Thomas A. Henzinger. « The Theory of Hybrid Automata ». In : *LiCS* (). Sous la dir. de Moshe Y. Vardi et Edmund M. Clarke. New Brunswick, New Jersey, USA : IEEE Computer Society, 1996, p. 278-292. DOI : 10.1109/LICS.1996.561342.

Masaki Waga, Étienne André et Ichiro Hasuo. « Model-bounded monitoring of hybrid systems ». In : *ICCPS* (19-21 mai 2021). Sous la dir. de Martina Maggio, James Weimer, Mohammad Al Farque et Meeko Oishi. Nashville, TN, USA : ACM, 2021, p. 21-32. DOI : 10.1145/3450267.3450531.

Additional information

Benchmarks

ϵ : slow-down parameter

Licensing

Source of the graphics used I

Title : Smiley green alien big eyes (aaah)
Author : LadyofHats
Source : `https://commons.wikimedia.org/wiki/File:Smiley_green_alien_big_eyes.svg`
License : public domain

Title : Smiley green alien big eyes (cry)
Author : LadyofHats
Source : `https://commons.wikimedia.org/wiki/File:Smiley_green_alien_big_eyes.svg`
License : public domain

Title : Tesla Model S
Author : National Transportation Safety Board
Source : `https://commons.wikimedia.org/wiki/File:Tesla_Model_S_(35366284636).jpg`
License : public domain

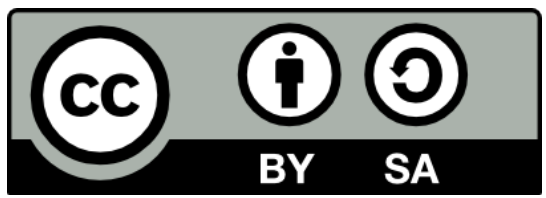
Title : Mtn view tesla scene graphic
Author : National Transportation Safety Board
Source : `https://commons.wikimedia.org/wiki/File:Mtn_view_tesla_scene_graphic_(28773524958).jpg`
License : public domain

License of this document

This presentation can be published, reused and modified under the terms of the license Creative Commons **Attribution-ShareAlike 4.0 Unported (CC BY-SA 4.0)**

(LaTeX source available on demand)

Authors : **Masaki Waga** and **Étienne André**



creativecommons.org/licenses/by-sa/4.0/