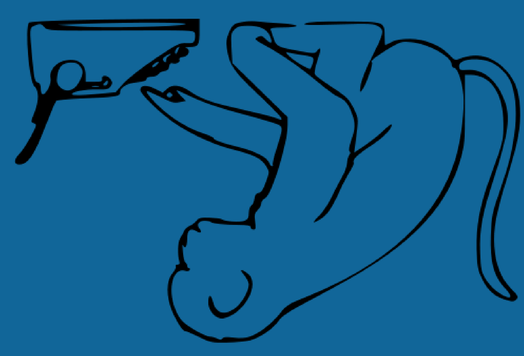
IMITATOR: Parametric verification of real-time systems



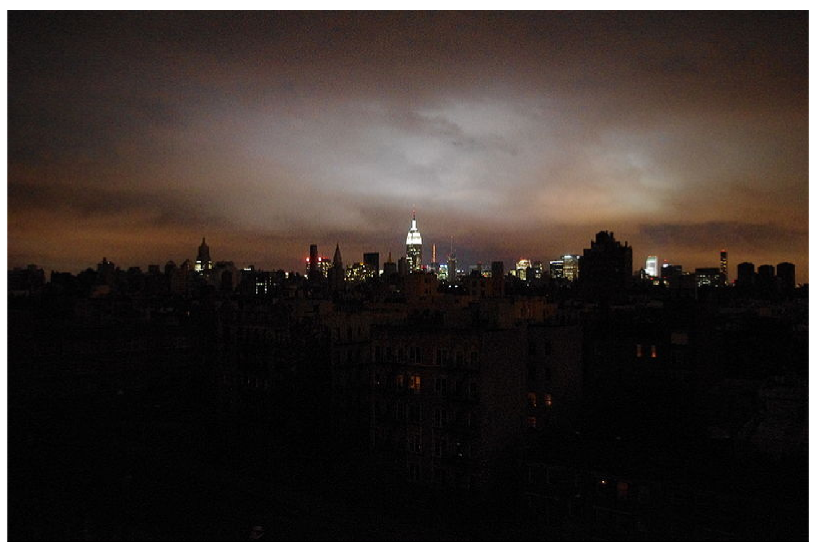
Étienne André

Université Paris 13, France | JFLI, CNRS, Tokyo, Japan | National Institute of Informatics, Japan

Context: Formal verification of real-time systems

Critical systems involve timing constraints and concurrency

Bugs can be **dramatic** (risk of loss of lives or huge financial loss)



$\Rightarrow$ need for **formal verification**

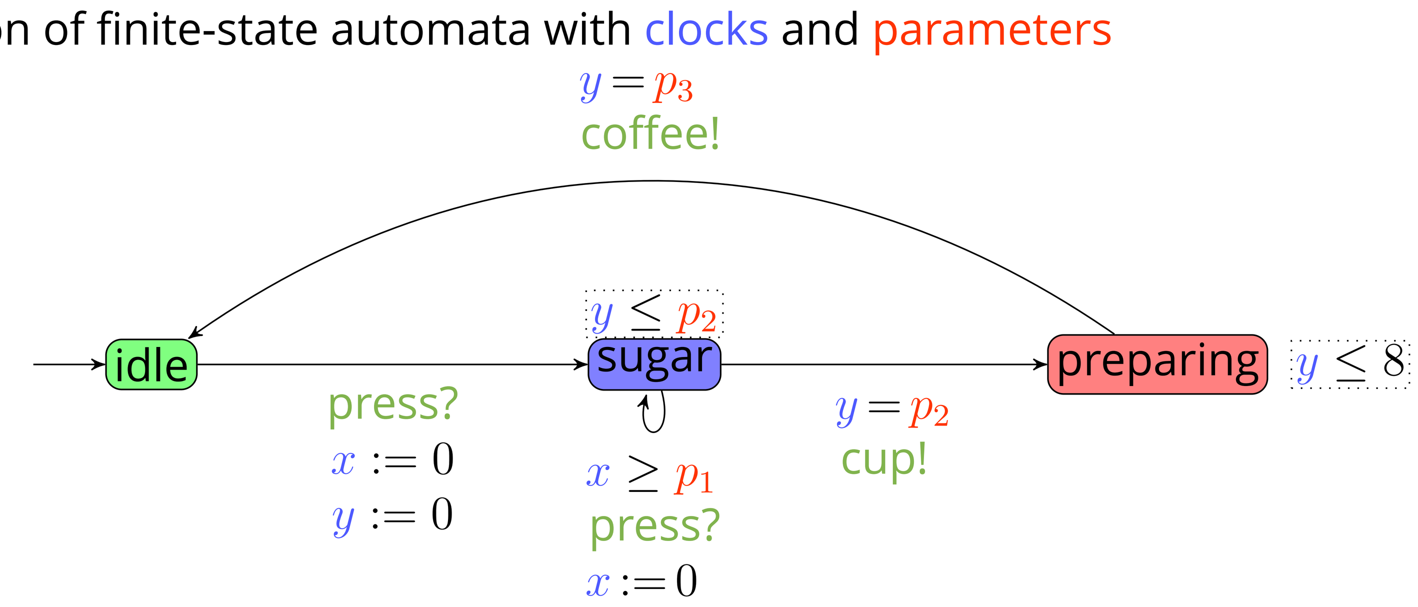
Objective

"Given a model (mathematical representation) of a system and a specification, synthesize timing constraints (parameters) guaranteeing that the system meets its specification"

The formalism: parametric timed automata

[AHV93]

Extension of finite-state automata with clocks and parameters



Exemple: a coffee machine modeled using a parametric timed automaton

IMITATOR in a nutshell

A **parametric timed model checker**

Input

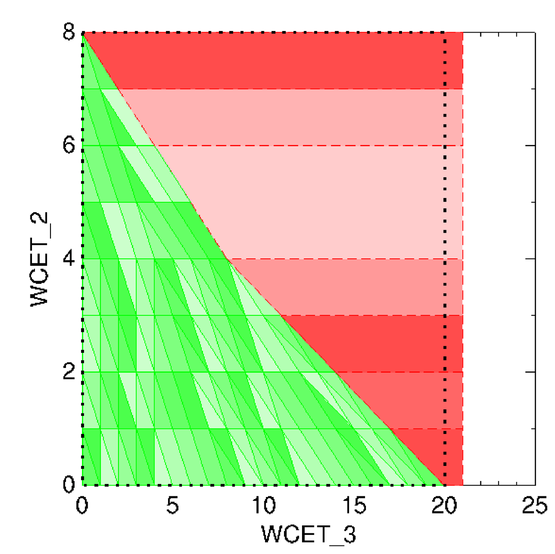
- a **real-time system** modeled using parametric timed automata
- a **specification**

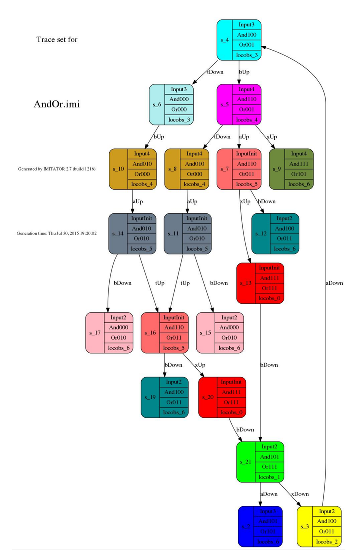
Output

- Conditions on the parameters formally guaranteeing the system correctness

```
Constraint for which the system meets its specification:
p1 + p2 > 2 p3 & p3 > 0
```

- Graphical visualization





What's inside?

Implemented in **OCaml**

Relying on the **Parma Polyhedra Library** [BHZ08]

Large repository of **benchmarks** [And18]

Distributed under the **GNU-GPL license**

Try it!

`www.imitator.fr`

Notable applications of IMITATOR

- **Hardware verification** [CEFX09]
  - Collaboration with ST-Microelectronics
- **Scheduling for aerospace** [FLMS12]
  - Collaboration with ArianeGroup
- **Scheduling under uncertainty** [SAL15]
  - Solved an industrial challenge by Thales
- **Testing software product lines** [LSBL17]
- Analysis of **music scores** [FJ13]
  - IRCAM, Paris, France
- **Monitoring** real-time systems [AHW18]
  - applications to automotive industry
  - best paper award @ ICECCS 2018

What's next?

- Integration to real-time systems formalisms
  - E.g. Thales' "Time4sys"
- Beyond timed automata
  - Linear hybrid automata
    - Can represent more subtle variations of speed, temperature, energy...
    - Potential: bring (more) formal methods to automotive industry

Bibliography

[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. Springer, 2012.

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

[AHW18] Étienne André, Ichiro Hasuo, and Masaki Waga. Offline timed pattern matching under uncertainty. In *ICECCS*, pages 10–20. IEEE CPS, 2018.

[And18] Étienne André. A benchmark library for parametric timed model checking. In *FTSCS*, Lecture Notes in Computer Science. Springer, 2018.

[BHZ08] Roberto Bagnara, Patricia M. Hill, and Enea Zaffanella. The Parma Polyhedra Library: Toward a complete set of numerical abstractions for the analysis and verification of hardware and software systems. *Science of Computer Programming*, 72(1–2):3–21, 2008.

[CEFX09] Rémy Chevallier, Emmanuelle Encrenaz-Tiphène, Laurent Fribourg, and Weiwen Xu. Timed verification of the generic architecture of a memory circuit using parametric timed automata. *Formal Methods in System Design*, 34(1):59–81, 2009.

[FJ13] Léa Fanchon and Florent Jacquemard. Formal timing analysis of mixed music scores. In *ICMC*. Michigan Publishing, 2013.

[FLMS12] Laurent Fribourg, David Lesens, Pierre Moro, and Romain Soulat. Robustness analysis for scheduling problems using the inverse method. In *TIME*, pages 73–80. IEEE Computer Society Press, 2012.

[LSBL17] Lars Luthmann, Andreas Stephan, Johannes Bürdek, and Malte Lochau. Modeling and testing product lines with unbounded parametric real-time constraints. In *SPLC, Volume A*, pages 104–113. ACM, 2017.

[SAL15] Youcheng Sun, Étienne André, and Giuseppe Lipari. Verification of two real-time systems using parametric timed automata. In *WATERS*, 2015.

Version: December 27, 2018

Credit: Deepwater Horizon Offshore Drilling Platform on Fire (ideum, cc by-sa) | Hurricane Sandy Blackout New York Skyline (David Shankbone, cc by) | Typing monkey (KaterBegemot, cc by-sa)

LaTeX TikZposter