Beyond Model Checking:
Parameters Everywhere

Étienne André¹, Benoît Delahaye², Peter Habermehl³, Claude Jard², Didier Lime⁴, Laure Petrucci¹, Olivier H. Roux⁴, Tayssir Touili³

¹ Université Paris 13, Sorbonne Paris Cité, LIPN, CNRS, France
² LINA/Université de Nantes, France
³ LIAFA, Université Paris Diderot – Paris7, France
⁴ IRCCyN, École Centrale de Nantes, France
Beyond Model Checking

😊 Model checking guarantees the absence of bugs
Beyond Model Checking

😊 Model checking guarantees the absence of bugs

😊 …but its use in the industry is rather disappointing
Beyond Model Checking... are Parameters

Two possible reasons for the lack of interest:

😊 the binary response to properties satisfaction, which is not informative enough

😢 the insufficient abstraction to cater for tuning and scalability of systems
Beyond Model Checking... are Parameters

Two possible reasons for the lack of interest:

😊 the binary response to properties satisfaction, which is not informative enough

😢 the insufficient abstraction to cater for tuning and scalability of systems

Challenge

Overcome these limitations by providing parametric formal methods for the verification and automated analysis of systems behaviour
Beyond Model Checking... are Parameters

Two possible reasons for the lack of interest:

😊 the binary response to properties satisfaction, which is not informative enough

❤️ the insufficient abstraction to cater for tuning and scalability of systems

Challenge

Overcome these limitations by providing \textit{parametric formal methods} for the verification and automated analysis of systems behaviour

Instead of “yes” or “no”, \textit{parameter synthesis} answers “yes if...”

■ \( \rightsquigarrow \) Derivation of \textit{correctness conditions}
Parameter Synthesis: Interesting but Hard

Interesting applications:

- **Infinite** systems
- **Partially defined** systems (timing constants or number of processes not known with certainty)
- **Robustness** issues (variation of timing delays, clock drifts)

---

É. André, O.H. Roux et al.

Beyond Model Checking

12 juin 2014 4 / 5
Parameter Synthesis: Interesting but Hard

Interesting applications:

- **Infinite** systems
- **Partially defined** systems (timing constants or number of processes not known with certainty)
- **Robustness** issues (variation of timing delays, clock drifts)

Mostly undecidable problems (e.g., [Alur et al., 1993, Bozzelli and La Torre, 2009, Jovanović et al., 2013]), with few exceptions:

- Regular model checking
  [Bouajjani et al., 2000, Bouajjani et al., 2008, Bouajjani et al., 2012]
- L/U automata (partially disappointing)
  [Hune et al., 2002, Bozzelli and La Torre, 2009, Jovanović et al., 2013]
- Interrupt automata [Bérard et al., 2012]
- Bounded integer parametric timed automata [Jovanović et al., 2013]
Agenda

1. Exhibit interesting **decidable subclasses** and write efficient algorithms

2. Design efficient **semi-algorithms** for undecidable problems

3. Mix **different types of parameters** together: discrete (processes), timed (delays), probabilistic (uncertainly), costs (energy)
References I


Additional explanation
Explanation for the 4 pictures in the beginning

Allusion to the Northeast blackout (USA, 2003)
Computer bug
Consequences: 11 fatalities, huge cost
(Picture actually from the Sandy Hurricane, 2012)

Allusion to any plane crash
(Picture actually from the happy-ending US Airways Flight 1549, 2009)

Allusion to the sinking of the Sleipner A offshore platform (Norway, 1991)
No fatalities
Computer bug: inaccurate finite element analysis modeling
(Picture actually from the Deepwater Horizon Offshore Drilling Platform)

Allusion to the MIM-104 Patriot Missile Failure (Iraq, 1991)
28 fatalities, hundreds of injured
Computer bug: software error (clock drift)
(Picture of an actual MIM-104 Patriot Missile, though not the one of 1991)
Licensing
Source of the graphics used

Title: Hurricane Sandy Blackout New York Skyline
Author: David Shankbone
Source: https://commons.wikimedia.org/wiki/File:Hurricane_Sandy_Blackout_New_York_Skyline.JPG
License: CC BY 3.0

Title: Miracle on the Hudson
Author: Janis Krums (cropped by Étienne André)
Source: https://secure.flickr.com/photos/davidwatts1978/3199405401/
License: CC BY 2.0

Title: Deepwater Horizon Offshore Drilling Platform on Fire
Author: ideum
Source: https://secure.flickr.com/photos/ideum/4711481781/
License: CC BY-SA 2.0

Title: DA-SC-88-01663
Author: imcomkorea
Source: https://secure.flickr.com/photos/imcomkorea/3017886760/
License: CC BY-NC-ND 2.0
License of this document

This presentation can be published, reused and modified under the terms of the license Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0)

(LATEX source available on demand)

Author: Étienne André

https://creativecommons.org/licenses/by-sa/3.0/