ANR TickTac 2019-2023

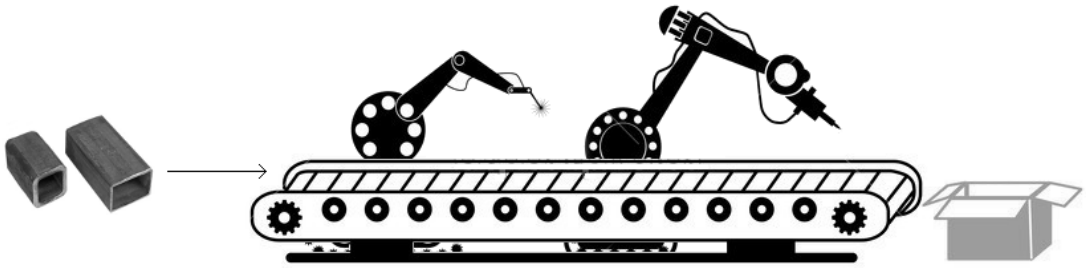
Efficient Techniques and Tools for the Verification and Synthesis of Real-Time Systems

http://www.irisa.fr/sumo/ticktac/

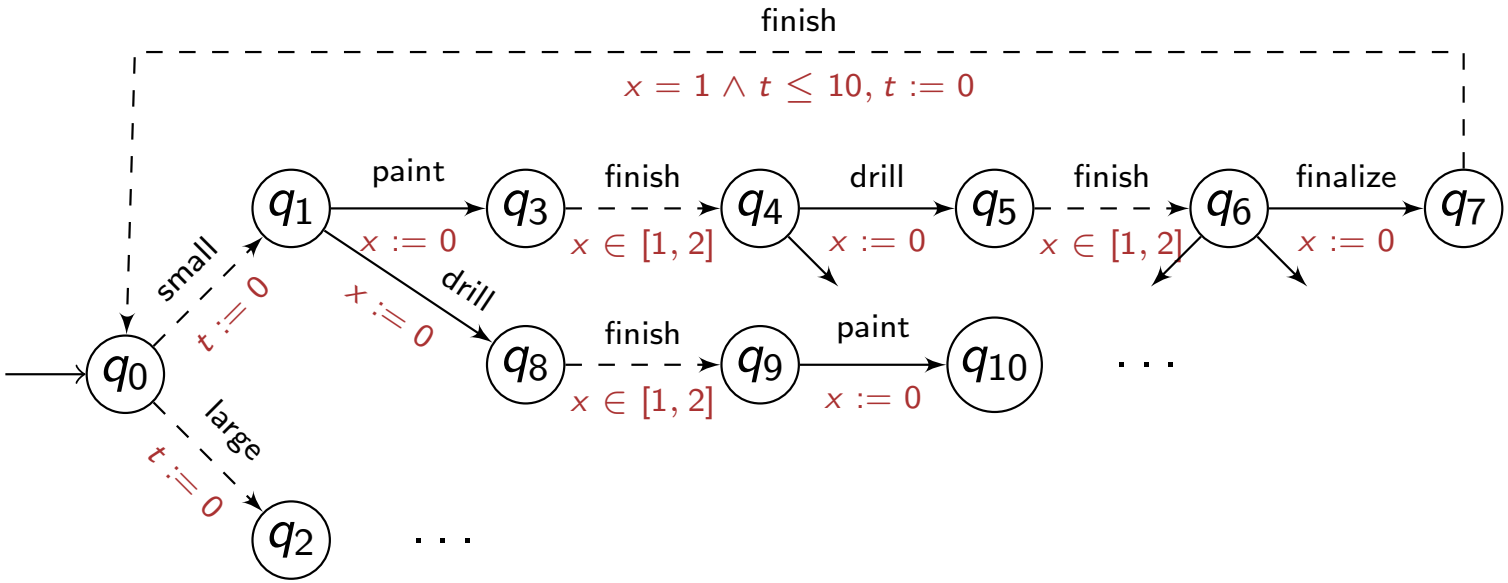
Ocan Sankur

Formal Methods for Real-Time Systems

Real-time System:



Timed automata:



State Of The Art on Timed Automata

Some Problems

- **Model checking**: check all behaviors w.r.t. spec
- **Synthesis**: compute a controller to control the system to satisfy spec
- **Testing**: non-exhaustive verification, coverage criteria
- **Optimization**: compute optimal/worst-case execution

State Of The Art on Timed Automata

Some Problems

- **Model checking**: check all behaviors w.r.t. spec
- **Synthesis**: compute a controller to control the system to satisfy spec
- **Testing**: non-exhaustive verification, coverage criteria
- **Optimization**: compute optimal/worst-case execution

- Reference model checker: **Uppaal** + extensions
  - Uppaal: model checking
  - Uppaal TIGA: synthesis
  - Uppaal TRON: test generation
  - Uppaal CORA: optimization

Format: networks of communicating timed automata + discrete variables

stable, well-known, nice GUI, closed-source, not up-to-date

State Of The Art on Timed Automata - 2

Overview of current algorithms:

1. [Semi-symbolic] **Explicit enumeration** of the discrete state space + **symbolic** treatment of the clock space with zones (e.g. Uppaal)
   some symmetry reduction, some results on PO reduction
2. [Symbolic] (Often) discrete time, uses BDDs or their variants (Red, ITS-tools, etc.). Very sensitive to variable ordering and size of the constants

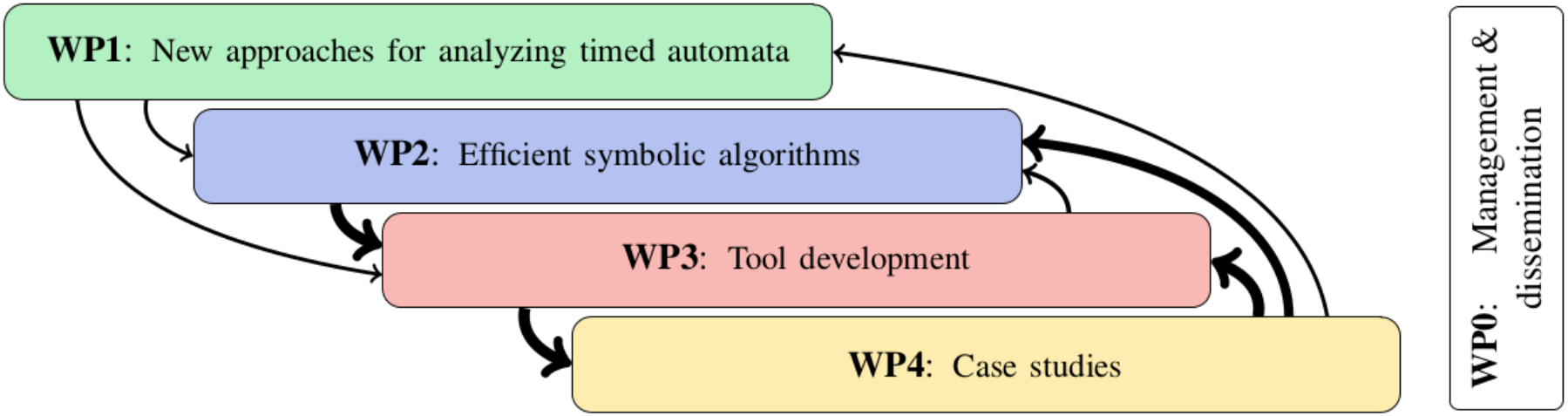
What is missing:

- Scalability w.r.t. discrete states *and* clocks
- Same zone-based algorithms for *all* applications?
- No support for liveness or LTL
- Cost optimization, approximation
- Not enough work for concurrent systems (PO reduction)
- Robustness
- ...

Consortium

- **IRISA**, Rennes + 1 year post-doc
  Thierry Jéron, Nicolas Markey, *Ocan Sankur*
  Emily Clement, Léo Henry, Victor Roussanaly
- **ISIR**, Paris + 1 year post-doc
  Nicolas Perrin, Philipp Schlehuber-Caissier
- **LaBRI**, Bordeaux
  Hugo Gimbert, *Frédéric Herbreteau*, Gérald Point, Igor Walukiewicz
- **LIS**, Marseille
  Benjamin Monmege, Pierre-Alain Reynier, Damien Busatto-Gaston
- **LRDE**, Paris + 1 PhD student
  Alexandre Duret-Lutz, Adrien Pommellet
- **LSV**, "Paris"
  Patirica Bouyer, Paul Gastin

Workpackages



WP1: New Approaches for Analyzing Timed Systems

- **alternative techniques**
  - tree-automata techniques for model checking
  - multiple-player timed games
  - testing, runtime verification, enforcement
- **quantitative verification**
  - approximation algorithms
  - stochastic timed games
- **robustness**
  - synthesis of robust controllers
  - quasi-synchronous abstraction

see Damien's talk

Leader of WP1: Benjamin Monmege

WP2: Efficient Algorithms

- **Dynamic Abstractions**
  - Coarse abstractions dynamically refined on demand — see Victor's talk
  - Mixed abstractions discrete states **and** clock space
  - Abstractions for approximation
- **Small Invariants**
  - Liveness
  - Strategies for Controller synthesis
  - Partial-order reduction techniques — see Igor's talk
- **Fully Symbolic Approaches**
  - Combine abstractions with BDD / SAT
  - Verification of real-time software

Leader of WP2: IRISA

WP3: Tool Development

Existing tools and prototypes

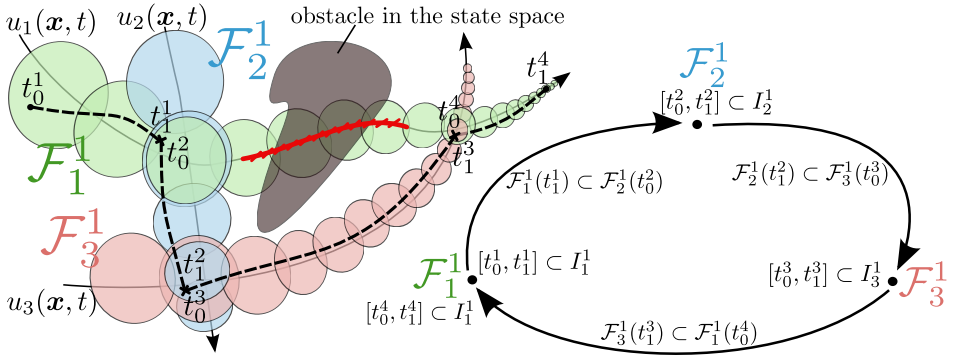
- **TChecker** (Frédéric Herbreteau). C++.
  - State-of-the-art semi-symbolic algorithms for safety and liveness verification.
- **Tiamo, Symrob** (Maximilien Colange, Ocan Sankur). OCaml.
  - Best weighted timed automata algorithms
  - Robustness analysis and parameter synthesis

- The new tool will be built on TChecker
- Build a large set of benchmarks to allow researchers to compare their algorithms and tools

More on this workpackage by Frédéric today
See also Alexandre's talk on Spot 2.0

WP3 Leader: Frédéric Hebreteau

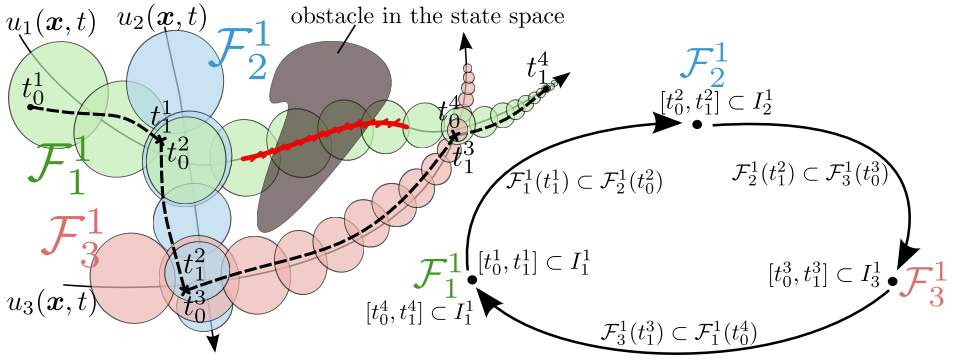
WP4: Case Studies



- **applications to robotics**: see Nicolas & Philipp's talk
  - Motion planning
  - large models
  - robustness
  - synthesis

WP4 Leader: Nicolas Perrin

WP4: Case Studies



- **applications to robotics**: see Nicolas & Philipp's talk
  - Motion planning
  - large models
  - robustness
  - synthesis

- **collaborations outside the project**:
  - Mitsubishi Electric Research Center Europe (Irisa)
  - Tata Consultancy Services (LaBRI, CMI Chennai)

WP4 Leader: Nicolas Perrin

Schedule

Today

- **14h30** Damien Busatto-Gaston. Robust controller synthesis in timed Büchi automata: a symbolic approach
- **15h15** Igor Walukiewicz. Partial-order reduction for real-time systems
- **16h** Break
- **16h30** Frederic Herbreteau. TChecker and the tool development WP
- **17h15** Alexandre Duret-Lutz. Development of the model checker Spot 2.0

20h Dinner: Crêperie Sainte Anne. 6 place Sainte Anne

Tomorrow

- **9h30** Victor Roussanaly. Abstraction refinement algorithms for timed automata
- **10h15** Paul Gastin. TBA
- **11h** Nicolas Perrin. Motion planning using timed automata and the case study work package
- **12h** Lunch Buffet
- **14h** Free time for discussions