Reachability Analysis with Measurable Time-Varying Uncertainties*

François Bidet, Éric Goubault, Sylvie Putot

LIX, École polytechnique, Institut Polytechnique de Paris

fbidet@lix.polytechnique.fr, goubault@lix.polytechnique.fr, putot@lix.polytechnique.fr

Introduction

- Safety properties can be proved knowing the set of reachable states
- Computing exact sets of reachable states is often impossible
- We compute an over-approximation: a set guaranteed to contain all reachable states
- Our method is able to handle a broader class of uncertainties than most of state-of-the-art tools

Problem formulation

- We want to compute over-approximations of the set of reachable states of the initial value problem

$$\begin{cases} \dot{x}(t) = g(u(t)) \cdot h(t, x(t)) \\ x(0) = x_0 \in \mathcal{X}_0 \subset \mathbb{R}^n \end{cases} \tag{1}$$

  with $u : [0,T] \to \mathcal{U}$ a Lebesgue-measurable bounded function, where $\mathcal{U}$ is a compact set, $g : \mathcal{U} \to \mathbb{R}^{n\times m}$ and $h : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^m$ two continuous functions.
- Right-hand side not Riemann-integrable $\implies$ most tools produce non guaranteed approximations

Theory

Let h^+ and h^- be continuous functions such that $h = h^+ - h^-$. An over-approximation of the initial value problem

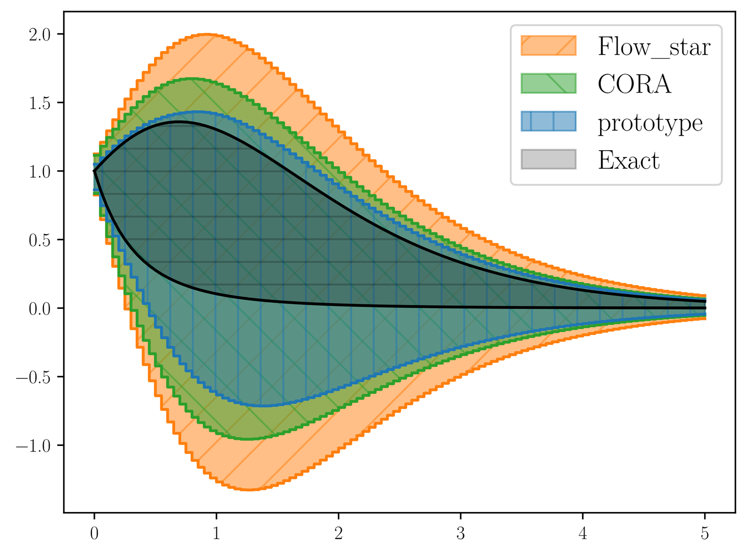
$$\begin{cases} \dot{x}(t) = Ah^+(t, x(t)) - Bh^-(t, x(t)) \\ x(0) = x_0 \in \mathcal{X}_0 \\ A, B \text{ such that } \exists u_A, u_B \in \mathcal{U} : \ g(u_A) = A \text{ and } g(u_B) = B \end{cases}$$

for all x_0, A, and B, is an over-approximation of the problem 1.
The right-hand side is continuous, so we can apply the Picard iteration to guarantee the over-approximation of the set of reachable states, parametrized by t, x_0, A and B.

Example: Nonlinear

Simple example with nonlinear dynamics:

$$\begin{cases} \dot{x}(t) = -x(t) - x(t)y(t)u(t) \\ \dot{y}(t) = -y(t) \\ t \in [0, 20] \\ u(t) \in [0, 1] \\ x(0) = 3 \end{cases}$$

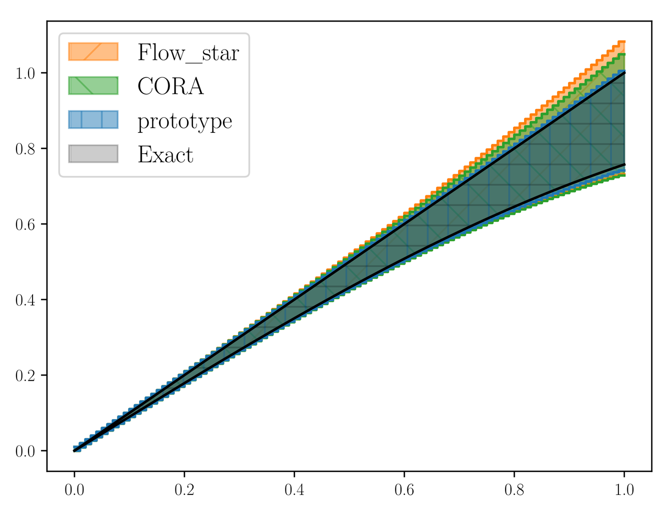


Over-approximations of $x(t)$

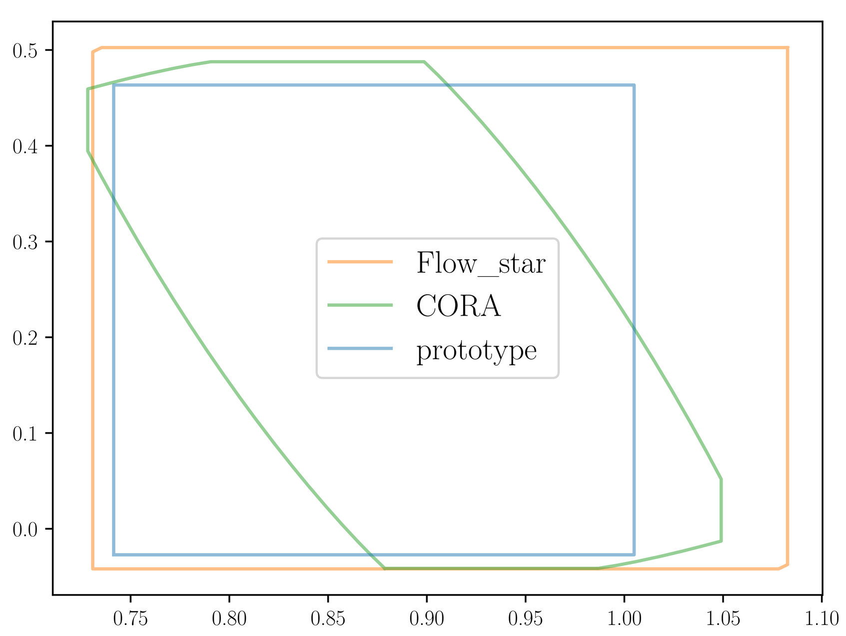
Example: Dubins car

Variation of the Dubins car model:

$$\begin{cases} \dot{x}(t) = u_1(t)\cos(z(t)) \\ \dot{y}(t) = u_1(t)\sin(z(t)) \\ \dot{z}(t) = u_2(t) \end{cases} \quad \text{with} \quad \begin{cases} t \in [0, 1] \\ u_1(t) \in [0.9, 1]; \ u_2(t) \in [0, 1] \\ x(0) = y(0) = z(0) = 0 \end{cases}$$



Over-approximations of $x(t)$



Over-approximations of $y(1)$ wrt. $x(1)$

Picard iteration

Let $\dot{x}(t) = f(t, x(t))$ be an ordinary differential equation with f a continuous function and $x(0) = x_0$ be an initial state.
Given a set-valued function $\overline{\varphi}(t)$, whose all images are closed, convex and bounded, such that

$$x_0 + \int_0^t f(s, \overline{\varphi}(s))\, ds \subset \overline{\varphi}(t)$$

then $\overline{\varphi}(t)$ is an over-approximation of the set of reachable states of the system at time t: for all solution x, $x(t) \in \overline{\varphi}(t)$.

Sets representation: Taylor models (TMs)

- triple $(\mathcal{D}, p, I)$ with $\mathcal{D} \subset \mathbb{R}^k$ be a domain, $p : \mathcal{D} \to \mathbb{R}$ be a polynomial, and $I \subset \mathbb{R}$ be an interval called remainder
- a Taylor model $(\mathcal{D}, p, I)$ is an over-approximation of f on $\mathcal{D}$ if $\forall x \in \mathcal{D},\ f(x) \in \{p(x) + v \mid v \in I\}$
- Easy to over-approximate usual operators and easy to implement

Positive decomposition

- Best decompositions of h using TMs minimize $\|h_i^+\|_1 + \|h_i^-\|_1$
- If $h(t, x) \in [a, b]$ with $a < 0 < b$, the best affine decomposition is

$$h_i^+ = \frac{b}{b-a}h - \frac{ab}{b-a} \quad \text{and} \quad h_j^- = \frac{a}{b-a}h - \frac{ab}{b-a}$$

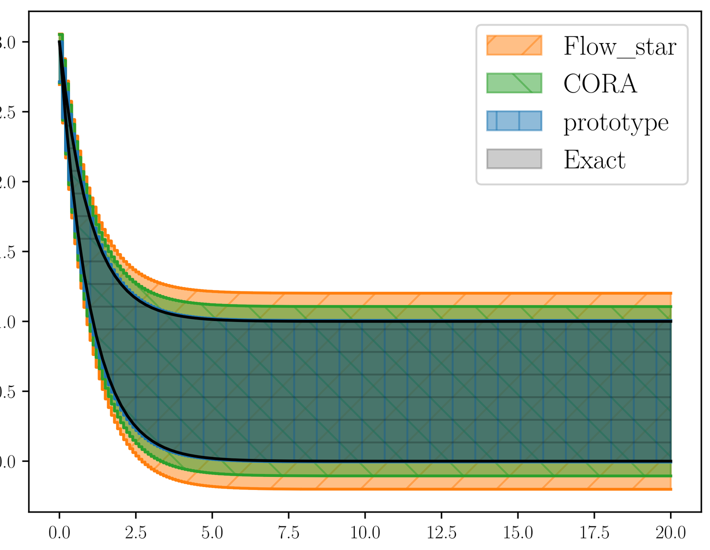
- We tried multiple decompositions on the problem $\dot{x}(t) = (0.1 - t)u(t)$ with $x(0) = 0$ and $u(t) \in [-1, 1]$ and displayed the results below

Decomposition	Over-Approximation
$(h + 0.1) - 0.1$	$[-0.040, 0.040]$
$(0.5h + 0.05) - (0.05 - 0.5h)$	$[-0.020, 0.020]$
$(h + 0.5)^2 - (h^2 + 0.25)$	$[-0.102, 0.102]$
$(h + 0.25)^2 - (h - 0.25)^2$	$[-0.027, 0.027]$

Example: Switching

Simple example with multiple possible fixed-points:

$$\begin{cases} \dot{x}(t) = u(t) - x(t) \\ t \in [0, 20] \\ u(t) \in [0, 1] \\ x(0) = 3 \end{cases}$$



Over-approximations of $x(t)$

Discussion about examples

Areas	CORA	Flow*	proto	exact
Nonlinear	5.956	7.735	4.866	3.576
Switching	23.33	26.81	19.48	19.00
Dubins car	0.114	0.114	0.099	0.086

- Tighter over-approximations of $x(t)$ (cf. table above)
- Loss of dependencies between variables (cf. Dubins car example)
- Handle broader class of uncertainties (Lebesgue-measurable)

Conclusion and future work

- New method to handle Lebesgue-measurable uncertainties
- Could be generalized to stochastic uncertainties (Itô calculus)
- Tight over-approximation on simple examples
  $\implies$ useful for safety properties proofs
- Could be used with transitions' abstractions of hybrid automata

*This work has been accepted for publication as "Reachability Analysis of Generalized Input-Affine Systems with Bounded Measurable Time-varying Uncertainties" in the IEEE Control Systems Letters (L-CSS).