Inner and Over Approximated Reachability Analysis for the Verification of Control Systems

Sylvie Putot, Eric Goubault

Cosynus, LIX, Ecole Polytechnique - CNRS

Modeliscale, 20th March 2019

Reachability-based verification

Safety verification, temporal properties

- Compute enveloppes of all possible trajectories
- If these enveloppes do not intersect with unsafe sets of states, then the system is safe
- We may then want to prove some additional temporal properties

This talk: focus on reachability analysis for uncertain non-linear ODEs

- Depending on whether parameters and inputs are controllable (or seen as non controllable disturbances), we discuss maximal and minimal reachability
- We generalize when mixing control and disturbances: robust reachability and approximations : what can we prove beyond safety?
- Not possible to compute exact envelopes : how to compute inner and outer approximations?
- Applications: using these envelopes for the verification of control systems

(to be presented at HSCC 2019, "Inner and Outer Reachability for the Verification of Control Systems")

Reachable sets of continuous uncertain non-linear dynamics

Consider

$$(S)\begin{cases}\dot{x}(t) = f(x(t), u(t)) \\ x(0) \in \boldsymbol{Z}_0, u(t) \in U \subseteq \mathbb{R}^p\end{cases}$$

Under classical hypotheses, solutions (flows) $\phi^f(s; x_0, u)$

Maximal reachability

[I. M. Mitchell, HSCC 2007] Comparing Forward and Backward Reachability as Tools for Safety Analysis

- State x_f is reachable at time s if
$$\exists x_0 \in \boldsymbol{Z}_0,\ \exists u : [0, s] \to U, \text{ s.t. } \varphi^f(s; x_0, u) = x_f$$
- The reachable set of system (S) is
$$R^f_{\mathcal{E}}(\boldsymbol{Z}_0, \mathbb{U}) = \{x_f | x_f \text{ is reachable}\}$$
(but not often computed over infinite time)
- The reachable tube or flowpipe over $[0, T]$ is
$$R^f_{\mathcal{E}}(t; \boldsymbol{Z}_0, \mathbb{U}) = \{x_f | x_f \text{ is reachable at time } s \leq t\}$$

Reachable sets of continuous uncertain non-linear dynamics

Also in [I. M. Mitchell, HSCC 2007] Comparing Forward and Backward Reachability as Tools for Safety Analysis

Minimal reachability

Minimal reachable set : states that trajectories will reach whatever the input signal is

$$R^f_{\mathcal{A}}(t; \boldsymbol{Z}_0, \mathbb{U}) = \{z \in \mathcal{D} \,|\, \forall u \in \mathbb{U}, \exists z_0 \in \boldsymbol{Z}_0,\ z = \varphi^f(t; z_0, u)\}$$

Our generalization, in this talk

Robust reachability : states that trajectories will reach whatever some components u_A of the input signal is, and for some other components u_E of the input signal

$$R^f_{\mathcal{AE}}(t; \boldsymbol{Z}_0, \mathbb{U}) = \{z \in \mathcal{D} \,|\, \forall u_A \in \mathbb{U}_{\mathbb{A}}, \exists u_E \in \mathbb{U}_{\mathbb{E}}, \exists z_0 \in \boldsymbol{Z}_0,\ z = \varphi^f(t; z_0, u_A, u_E)\}$$

Think of non controllable perturbations for u_A, and controls for u_E
(maybe time-dependent inputs - control - and perturbations ; note that some other notion of robustness is $\forall u_E,\ \exists u_A$ but is more difficult to [inner-]approximate!)

First classical application : reachability and safety analysis

Given L a set of unsafe states

Safety verification (definition) : safe if empty intersection of the outer-approximation and the unsafe region :

- The flow φ^f is safe over time horizon $[0, t]$ for all possible inputs
  if for all $z_0 \in \boldsymbol{Z}_0$, for all $u \in \mathbb{U}$, trajectories $\varphi^f([0, t]; z_0, u)$ do not intersect L.
- Similarly, φ^f is safe over time horizon $[0, t]$ for some inputs $u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}$ depending on other arbitrary inputs $u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}$.

Reachability for safety analysis

At least (theorem) :

- If $R^f_{\mathcal{E}}(t; \boldsymbol{Z}_0, \mathbb{U}) \cap L = \emptyset$ then φ^f is safe over horizon $[0, t]$ for all possible inputs $u \in \mathbb{U}$

Unfortunately, reachable sets are in general not computable

Approximations of robust reachability

Inner and outer approximations

Let two sets $\mathcal{I}_{\mathcal{AE}}$ and $\mathcal{O}_{\mathcal{AE}}$ such that

$$\mathcal{I}_{\mathcal{AE}} \subseteq R^f_{\mathcal{AE}}(t; \boldsymbol{Z}_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}}) \subseteq \mathcal{O}_{\mathcal{AE}}.$$

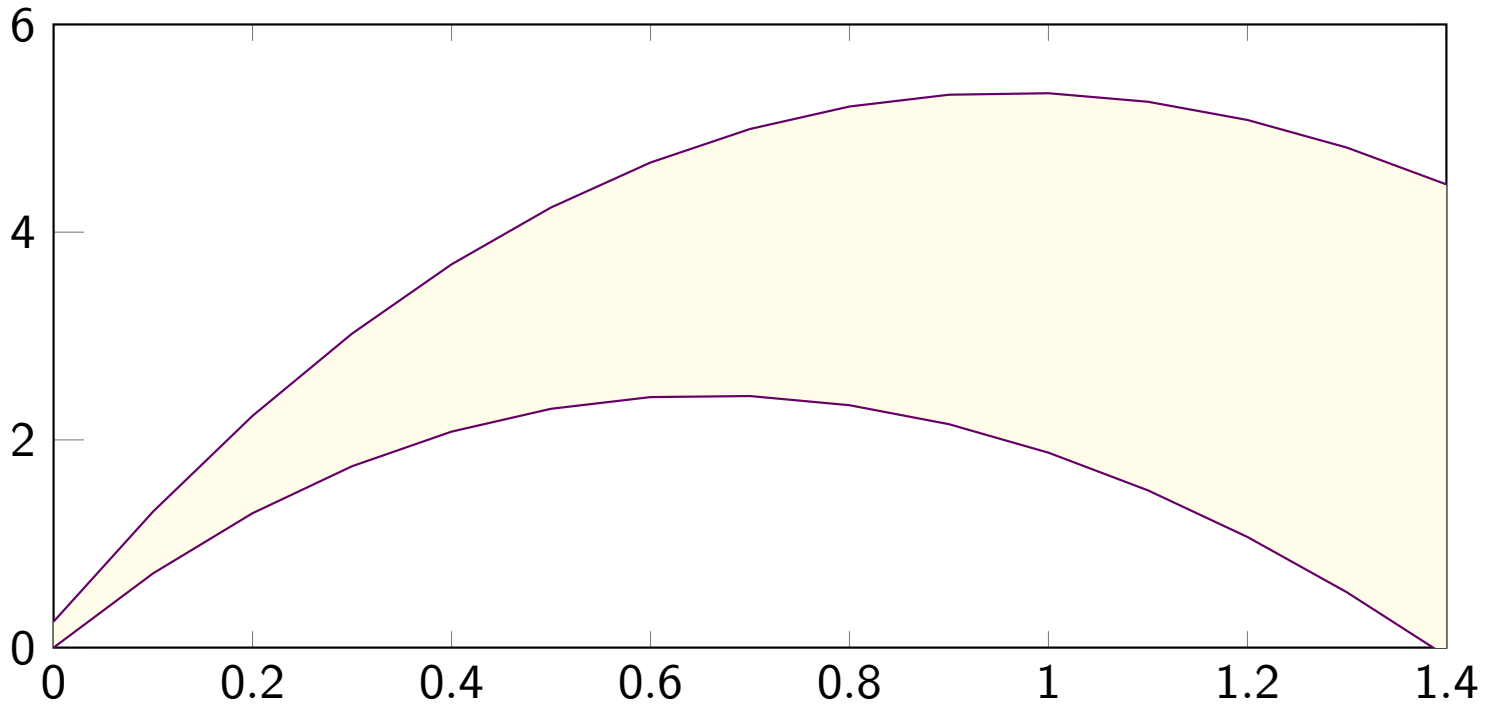
- $\mathcal{I}_{\mathcal{AE}}$ a *robust inner-approximation*, and $\mathcal{O}_{\mathcal{AE}}$ a *robust outer-approximation*. (with respect to disturbance $u_{\mathcal{A}}$).
- When $I_{\mathcal{E}} = \emptyset$, $\mathcal{I}_{\mathcal{AE}} = \mathcal{I}_{\mathcal{A}}$ a *minimal inner-approximation* and $\mathcal{O}_{\mathcal{AE}} = \mathcal{O}_{\mathcal{A}}$ a *minimal outer-approximation*.
- When $I_{\mathcal{A}} = \emptyset$, $\mathcal{I}_{\mathcal{AE}} = \mathcal{I}_{\mathcal{E}}$ a *maximal inner-approximation* and $\mathcal{O}_{\mathcal{AE}} = \mathcal{O}_{\mathcal{E}}$ a *maximal outer-approximation*.

The problem at hand

- Relate inner and outer approximations to safety verification, and other properties of interest (careful with quantified uncertainties!)
- Find computable such inner and outer approximations

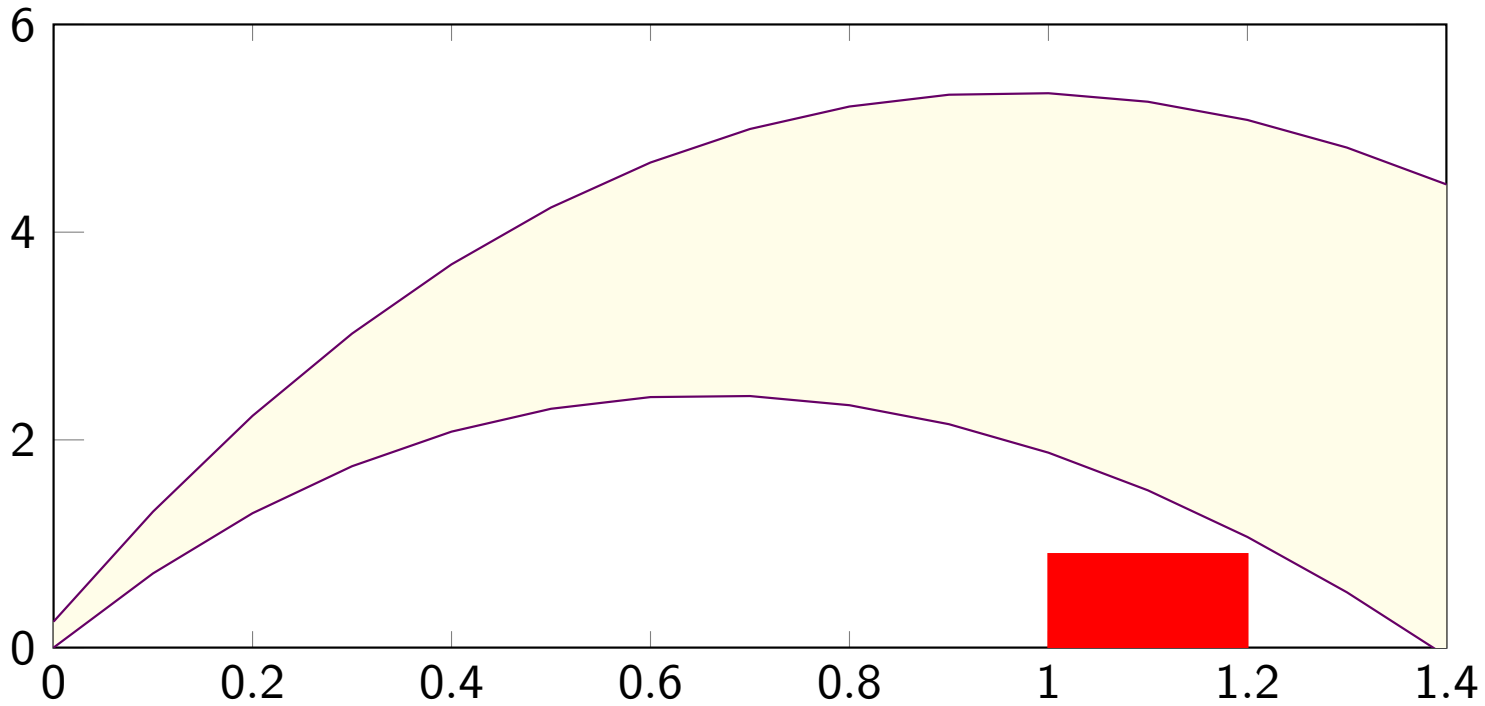
Inner and outer approximations of reachable sets for uncertain dynamical systems

- Outer or over-approximating flowpipes = guaranteed to include all reachable states



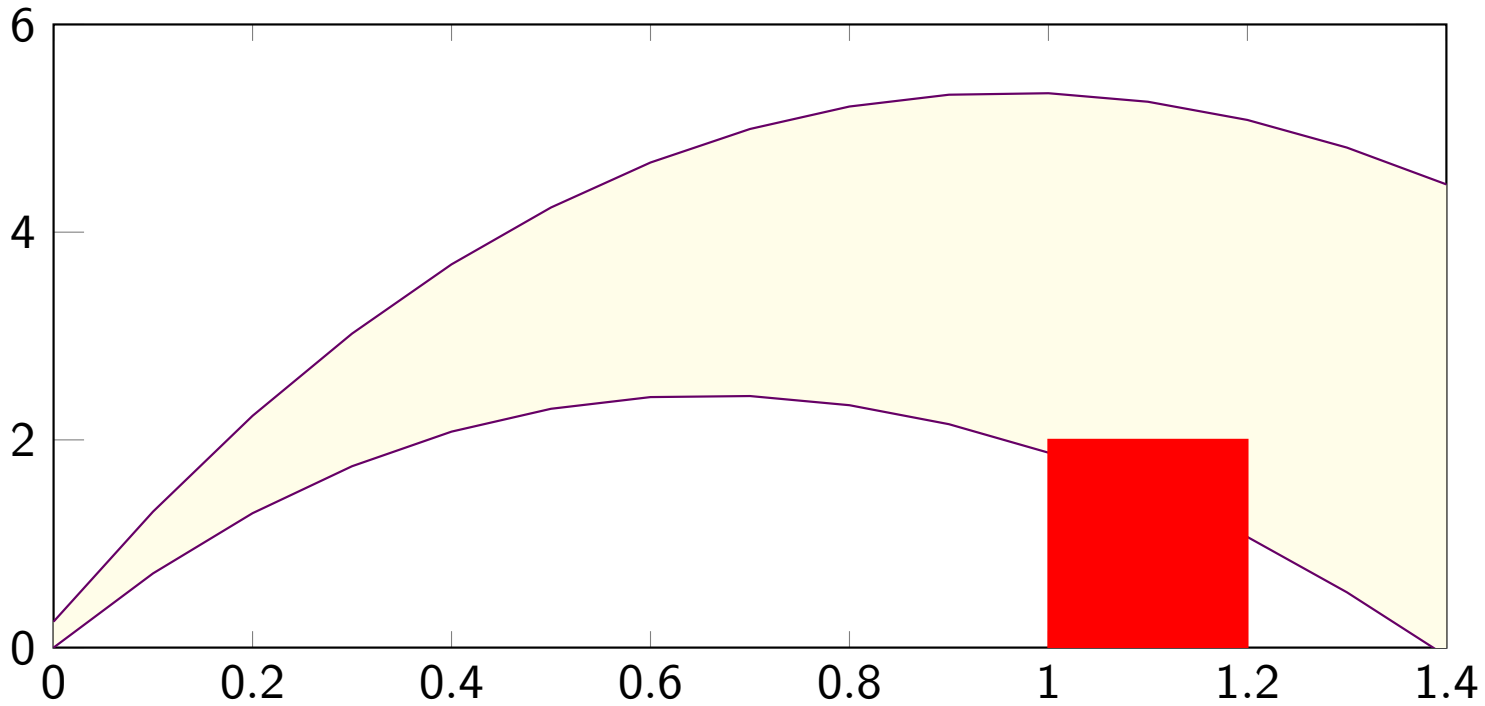
Inner and outer approximations of reachable sets for uncertain dynamical systems

- Outer or over-approximating flowpipes = guaranteed to include all reachable states
  - provide safety proof (we saw that already)



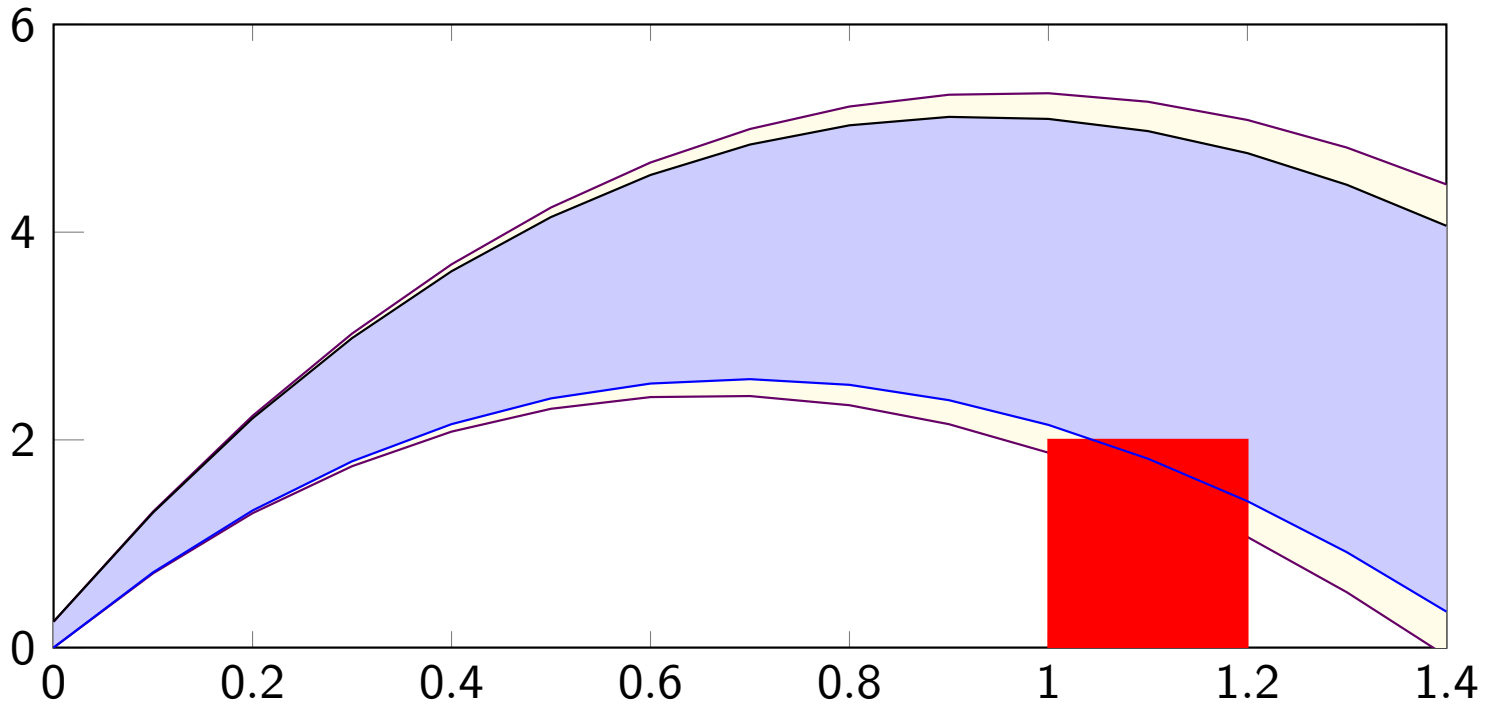
Inner and outer approximations of reachable sets for uncertain dynamical systems

- Outer or over-approximating flowpipes = guaranteed to include all reachable states
  - provide safety proof but conservative ("false alarms")



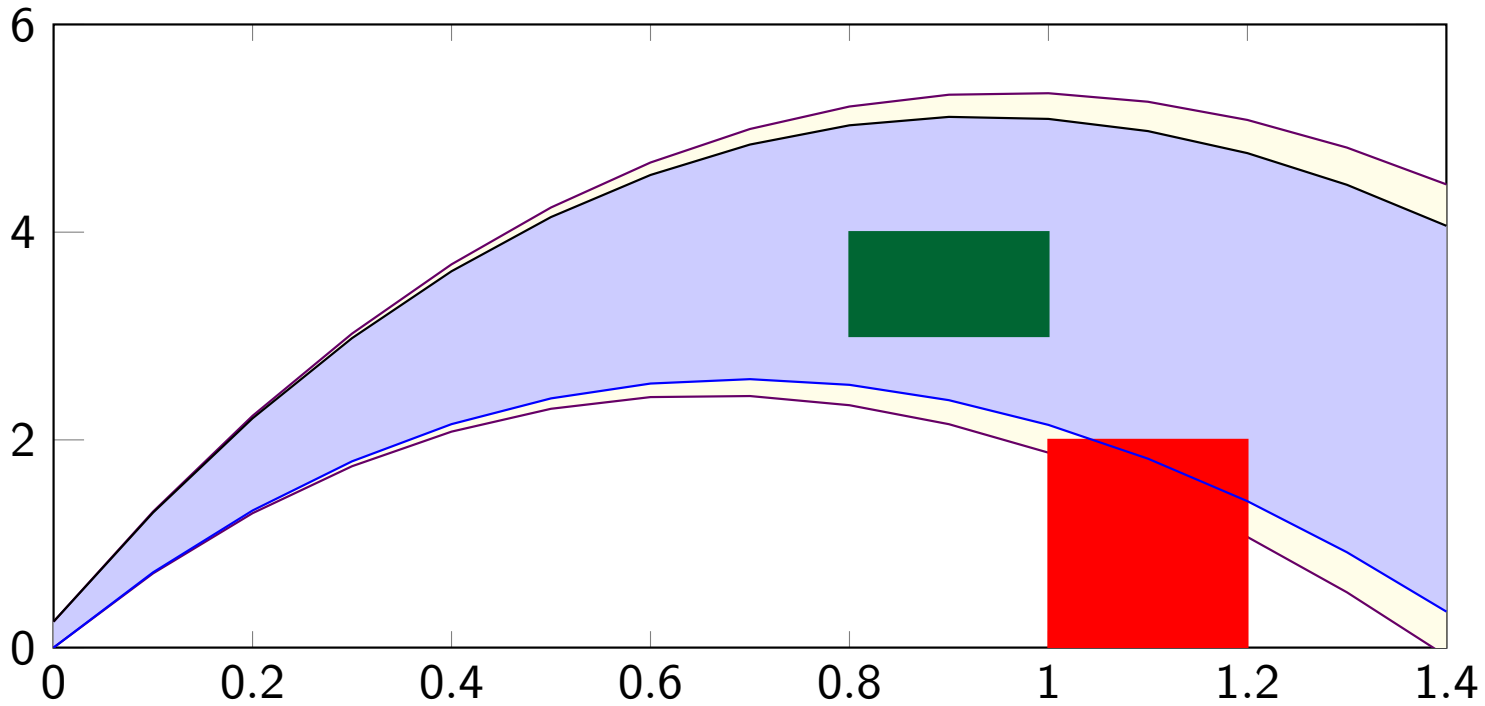
Inner and outer approximations of reachable sets for uncertain dynamical systems

- Outer or over-approximating flowpipes = guaranteed to include all reachable states
  - provide safety proof but conservative ("false alarms")
- Inner or under-approximating flowpipes = states guaranteed to be reached
  - falsification of safety properties, precision estimates



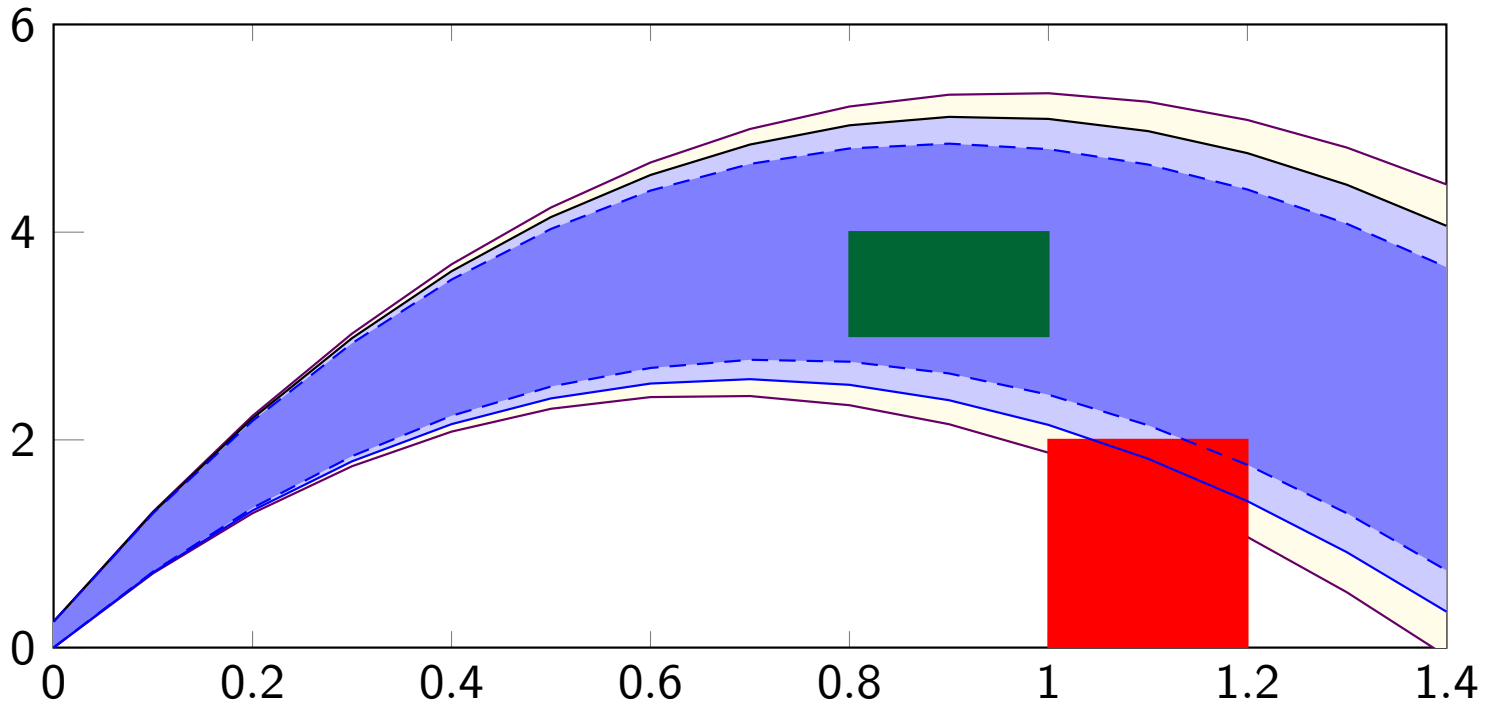
Inner and outer approximations of reachable sets for uncertain dynamical systems

- Outer or over-approximating flowpipes = guaranteed to include all reachable states
  - provide safety proof but conservative ("false alarms")
- Inner or under-approximating flowpipes = states guaranteed to be reached
  - falsification of safety properties, precision estimates
  - verification of new properties (sweep-avoid ?)



Inner and outer approximations of reachable sets for uncertain dynamical systems

- Outer or over-approximating flowpipes = guaranteed to include all reachable states
  - provide safety proof but conservative ("false alarms")
- Inner or under-approximating flowpipes = states guaranteed to be reached
  - falsification of safety properties, precision estimates
  - verification of new properties (sweep-avoid ?)
  - falsification in presence of disturbances or uncertain parameters (robust outer- and inner-approximation)



This can be made precise : safety and falsification analysis

Forward inner and outer-approximations provide semi-decision procedures for safety over a finite time horizon.

Inner and outer approximations for safety

Any inner-approximation $\mathcal{I}_s$ (resp. outer-approximation $\mathcal{O}_s$) for $s \in [0, t]$ or any flowpipe inner-approximation $\mathcal{I}$ (resp. outer-approximation $\mathcal{O}$) of the robust reachable set allows to prove the following:

- If $\mathcal{O}_s \cap L = \emptyset$ for all $s \in [0, t]$ (resp. $\mathcal{O} \cap L = \emptyset$) then φ^f is safe over horizon $[0, t]$ for all possible inputs $u \in \mathbb{U}$
- If $\mathcal{I}_s \cap L \neq \emptyset$ for some $s \in [0, t]$ (resp. $\mathcal{I} \cap L \neq \emptyset$) then φ^f is unsafe over horizon $[0, t]$, for some possible inputs $u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}$ (possibly depending on disturbances $u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}$)

We can also interpret other properties of interest

Given a target set K and a set L to be avoided, what is the set of initial states such that there exists a control going from these initial states to K, while avoiding L?

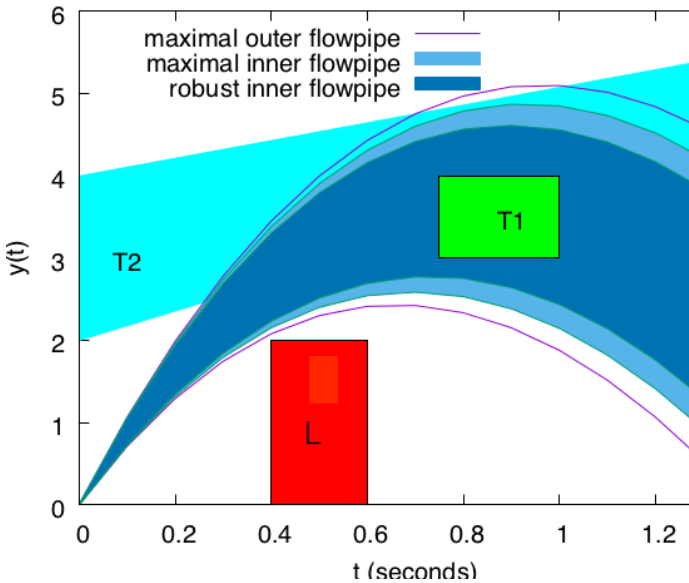
Reach-avoid/Sweep-avoid properties

- If an outer-approximation $\mathcal{O}$ at some time instant is fully included in K, and if the intersection of the outer-approximation tube with the unsafe set L is empty then $\boldsymbol{Z}_0$ is the set of initial states that ensures the reach-avoid property
- If moreover, $K \subseteq \mathcal{I}$, then we proved that the whole target set K is covered, we solved the (robust) sweep-avoid problem.

In brief : "classical" properties for the verification of control systems

Example of a shooting cannon

- Safety verification: if empty intersection of the outer-approximation and the unsafe region - here L
- Safety falsification: if non-empty intersection of the inner-approximation and the unsafe region
- Robust falsification: if non-empty intersection of the robust inner-approximation and the unsafe states (cannot be proved by testing)
- Reach-avoid: some point of region T2 (a moving target) is reachable (while avoiding L), whatever the mass of the bullet: T2 intersects with the robust inner-approximation
- Sweep-avoid: the whole region T1 is covered (while avoiding L) whatever the mass of the bullet, for some initialization: T1 is included in the robust inner-approximation



Height $y(t)$

Also inner and outer-approximations of the viability kernel (but indirectly - not in this paper)

Backward reachable sets

- (Robust) Backward reachable set :

$$B^f_{\mathcal{AE}}(K, [0,t]; \boldsymbol{Z}_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}}) = \{z_0 \in \boldsymbol{Z}_0 \mid \forall u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}, \\ \exists u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}, \exists s \in [0,t], \exists z \in K,\ z = \varphi^f(s; z_0, u)\}$$

- This is just in our case

$$B^f_{\mathcal{AE}}(K, [0,t]; \boldsymbol{Z}_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}}) = R^{-f}_{\mathcal{AE}}([0,t]; K, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}}) \cap \boldsymbol{Z}_0 \quad (1)$$

- Hence inner and outer-approximations of the backward reachable sets, similarly.

Semi-decision for backward reachability

Let L be a set of unsafe states, $\mathcal{I}_{\mathcal{AE}}$ an inner-approximation of the robust reachable set $R^{-f}_{\mathcal{AE}}([0,t]; L, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$, and $\mathcal{O}_{\mathcal{E}}$ a maximal outer-approximation, we have:

- If $\mathcal{O}_{\mathcal{E}} \cap \boldsymbol{Z}_0 = \emptyset$ then $\forall u \in \mathbb{U}$, φ^f is safe over time $[0,t]$
- If $\mathcal{I}_{\mathcal{AE}} \cap \boldsymbol{Z}_0 \neq \emptyset$ then $\exists u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}$ which makes φ^f unsafe

(also, backward reach-avoid properties, see the article)

Taylor models outer-approximated flowpipes (Berz & Makino, Nedialkov, Chen & Abraham & Sankaranarayanan.)

For $\dot{z}(t) = f(z),\ z(t_0) \in [z_0]$ with $f : \mathbb{R}^n \to \mathbb{R}^n$, given a time grid $t_0 < t_1 < \ldots < t_N$, we use Taylor models at order k to outer-approximate the solution $(t, z_0) \mapsto z(t, z_0)$ on each time interval $[t_j, t_{j+1}]$:

$$[z](t, t_j, [z_j]) = [z_j] + \sum_{i=1}^{k-1} \frac{(t-t_j)^i}{i!} f^{[i]}([z_j]) + \frac{(t-t_j)^k}{k!} f^{[k]}([r_{j+1}]),$$

- the Taylor coefficients $f^{[i]}$ are defined inductively and can be computed by automatic differentiation:

$$\begin{aligned} f_k^{[1]} &= f_k \\ f_k^{[i+1]} &= \sum_{j=1}^{n} \frac{\partial f_k^{[i]}}{\partial z_j} f_j \end{aligned}$$

- bounding the remainder supposes to first compute a (rough) enclosure $[r_{j+1}]$ of solution $z(t, z_0)$ on $[t_j, t_{j+1}]$, classical by Picard iteration: find h_{j+1}, $[r_{j+1}]$ such that

$$[z_j] + [0, h_{j+1}] f([r_{j+1}]) \subseteq [r_{j+1}]$$

- initialization of next iterate $[z_{j+1}] = [z](t_{j+1}, t_j, [z_j])$

Taylor models are efficiently and precisely estimated in affine arithmetic / zonotopes

Computing inner-approximations? An outline

Inner approximation of the range of $f : \mathbb{R}^n \to \mathbb{R}^p$ on a set $[x]$

- modal intervals and Kaucher arithmetic ($f : \mathbb{R}^n \to \mathbb{R}$)
- generalized mean value theorem: relies on outer-approximation of f and its *Jacobian* on $[x]$

Inner approximation of the solution of an uncertain dynamical system $\dot{z}(t) = f(z),\ z(t_0) \in [z_0]$

- solution $z_0 \mapsto z(t, z_0)$ of this system is a function $z : \mathbb{R}^n \to \mathbb{R}^n$
- we want to compute inner-approximated flowpipe on this function
- we need an outer-approximated flowpipe for z and its Jacobian with respect to z_0 (and parameters) : "classical" Taylor model based outer-approximated flowpipes
- then we can apply generalized mean value theorem on z

Intervals, outer and inner approximations

Intervals: closed connected subsets of $\mathbb{R}$, noted $[x] \in \boldsymbol{I}$; by extension $[x] \in \boldsymbol{I}^n$ n-dim boxes

For $f : \mathbb{R}^n \to \mathbb{R}^p$, we would like to compute $\text{range}(f, [x]) = \{f(x), x \in [x]\}$.

Outer approximation

- An outer approximating extension of $f : \mathbb{R}^n \to \mathbb{R}$ over intervals is $[f] : \boldsymbol{I}^n \to \boldsymbol{I}$ such that
$$\forall [x] \in \boldsymbol{I}^n, \text{range}(f, [x]) \subseteq [z] = [f]([x])$$
- Natural interval extension: replacing real by interval operations in function f.

Example: the extension of $f(x) = x^2 - x$ on $[2, 3]$ is $[f]([2, 3]) = [2, 3]^2 - [2, 3] = [1, 7]$, and can be interpreted as

$$(\forall x \in [2, 3])\,(\exists z \in [1, 7])\,(f(x) = z).$$

Inner approximation

An interval inner approximation $[z] \in \boldsymbol{I}$ satisfies $[z] \subseteq \text{range}(f, [x])$ of the range of f over $[x]$, and can be interpreted as

$$(\forall z \in [z])\,(\exists x \in [x])\,(f(x) = z).$$

Generalized intervals for outer and inner approximations

Generalized intervals

- Intervals whose bounds are not ordered $\boldsymbol{K} = \{[a, b],\ a \in \mathbb{R}, b \in \mathbb{R}\}$
- Called proper if $a \leq b$, else improper

Definition (Following Goldsztejn et al. 2005)

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a continuous function and $[x] \in \boldsymbol{K}^n$, decomposed in $[x]_{\mathcal{A}} \in \boldsymbol{I}^p$ and $[x]_{\mathcal{E}} \in (\text{dual } \boldsymbol{I})^q$ with $p + q = n$. A generalized interval $[z] \in \boldsymbol{K}$ is $(f, [x])$-interpretable if

$$(\forall x_{\mathcal{A}} \in [x]_{\mathcal{A}})\,(Q_z z \in \text{pro } [z])\,(\exists x_{\mathcal{E}} \in \text{pro } [x]_{\mathcal{E}}), (f(x) = z)$$

where $Q_z = \exists$ if $[z]$ is proper, and $Q_z = \forall$ if $[z]$ is improper.

- When all intervals are proper, we get an outer approximation of range$(f, [x])$

$$(\forall x \in [x])\,(\exists z \in [z])\,(f(x) = z).$$

- When all intervals are improper, we get an inner approximation of range$(f, [x])$

$$(\forall z \in \text{pro } [z])\,(\exists x \in \text{pro } [x])\,(f(x) = z).$$

Kaucher arithmetic [Kaucher 1980] on generalized intervals

Kaucher addition extends addition on classical intervals:
$[x] + [y] = [\underline{x} + \underline{y}, \overline{x} + \overline{y}]$ and $[x] - [y] = [\underline{x} - \overline{y}, \overline{x} - \underline{y}]$.

Kaucher multiplication

Let $\mathcal{P} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \geqslant 0 \wedge \overline{x} \geqslant 0\}$, $-\mathcal{P} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \leqslant 0 \wedge \overline{x} \leqslant 0\}$,
$\mathcal{Z} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \leqslant 0 \leqslant \overline{x}\}$, and dual $\mathcal{Z} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \geqslant 0 \geqslant \overline{x}\}$.

$[x] \times [y]$	$[y] \in \mathcal{P}$	$\mathcal{Z}$	$-\mathcal{P}$	dual$\mathcal{Z}$
$[x] \in \mathcal{P}$	$[\underline{x}\underline{y}, \overline{x}\overline{y}]$	$[\overline{x}\underline{y}, \overline{x}\overline{y}]$	$[\overline{x}\underline{y}, \underline{x}\overline{y}]$	$[\underline{x}\underline{y}, \underline{x}\overline{y}]$
$\mathcal{Z}$	$[\underline{x}\overline{y}, \overline{x}\overline{y}]$	$[\min(\underline{x}\overline{y}, \overline{x}\underline{y}),$ $\max(\underline{x}\underline{y}, \overline{x}\overline{y})]$	$[\overline{x}\underline{y}, \underline{x}\underline{y}]$	0
$-\mathcal{P}$	$[\underline{x}\overline{y}, \overline{x}\underline{y}]$	$[\underline{x}\overline{y}, \underline{x}\underline{y}]$	$[\overline{x}\overline{y}, \underline{x}\underline{y}]$	$[\overline{x}\overline{y}, \overline{x}\underline{y}]$
dual$\mathcal{Z}$	$[\underline{x}\underline{y}, \overline{x}\underline{y}]$	0	$[\overline{x}\overline{y}, \underline{x}\overline{y}]$	$[\max(\underline{x}\underline{y}, \overline{x}\overline{y}),$ $\min(\underline{x}\overline{y}, \overline{x}\underline{y})]$

Interpretation of Kaucher arithmetic, Goldsztejn et al. 2005

Let $f : \mathbb{R}^n \to \mathbb{R}$ be given by an arithmetic expression with single occurrences of variables.
Then for $[x] \in \boldsymbol{K}^n$, $f([x])$, computed using Kaucher arithmetic, is $(f, [x])$-interpretable.

Kaucher arithmetic [Kaucher 1980] on generalized intervals

Kaucher addition extends addition on classical intervals:
$[x] + [y] = [\underline{x} + \underline{y}, \overline{x} + \overline{y}]$ and $[x] - [y] = [\underline{x} - \overline{y}, \overline{x} - \underline{y}]$.

Kaucher multiplication

Let $\mathcal{P} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \geqslant 0 \wedge \overline{x} \geqslant 0\}$, $-\mathcal{P} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \leqslant 0 \wedge \overline{x} \leqslant 0\}$,
$\mathcal{Z} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \leqslant 0 \leqslant \overline{x}\}$, and dual $\mathcal{Z} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \geqslant 0 \geqslant \overline{x}\}$.

$[x] \times [y]$	$[y] \in \mathcal{P}$	$\mathcal{Z}$	$-\mathcal{P}$	dual$\mathcal{Z}$
$[x] \in \mathcal{P}$	$[\underline{x}\underline{y}, \overline{x}\overline{y}]$	$[\overline{x}\underline{y}, \overline{x}\overline{y}]$	$[\overline{x}\underline{y}, \underline{x}\overline{y}]$	$[\underline{x}\underline{y}, \underline{x}\overline{y}]$
$\mathcal{Z}$	$[\underline{x}\overline{y}, \overline{x}\overline{y}]$	$[\min(\underline{x}\overline{y}, \overline{x}\underline{y}),$ $\max(\underline{x}\underline{y}, \overline{x}\overline{y})]$	$[\overline{x}\underline{y}, \underline{x}\underline{y}]$	0
$-\mathcal{P}$	$[\underline{x}\overline{y}, \overline{x}\underline{y}]$	$[\underline{x}\overline{y}, \underline{x}\underline{y}]$	$[\overline{x}\overline{y}, \underline{x}\underline{y}]$	$[\overline{x}\overline{y}, \overline{x}\underline{y}]$
dual$\mathcal{Z}$	$[\underline{x}\underline{y}, \overline{x}\underline{y}]$	0	$[\overline{x}\overline{y}, \underline{x}\overline{y}]$	$[\max(\underline{x}\underline{y}, \overline{x}\overline{y}),$ $\min(\underline{x}\overline{y}, \overline{x}\underline{y})]$

Interpretation of Kaucher arithmetic, Goldsztejn et al. 2005

Let $f : \mathbb{R}^n \to \mathbb{R}$ be given by an arithmetic expression with single occurrences of variables.
Then for $[x] \in \boldsymbol{K}^n$, $f([x])$, computed using Kaucher arithmetic, is $(f, [x])$-interpretable.

Example: $[z] = [x] \times [y] = 0$ when $[x] \in \mathcal{Z}$ and $[y] \in$ dual $\mathcal{Z}$

Example: Kaucher multiplication

Example (Interpretation of the Kaucher multiplication in the case $\mathcal{Z} \times$ dual $\mathcal{Z}$)

$[z] = [x] \times [y] = 0$ when $[x] \in \mathcal{Z} = \{[x],\ \underline{x} \leqslant 0 \leqslant \overline{x}\}$ (e.g. [-5,4]) and $[y] \in$ dual $\mathcal{Z} = \{[x],\ \underline{x} \geqslant 0 \geqslant \overline{x}\}$ (e.g. [1,-1]).

Definition (reminder)

Let $f : \mathbb{R}^n \to \mathbb{R}$ and $[x] \in \boldsymbol{K}^n$, which we can decompose in $[x]_{\mathcal{A}} \in \boldsymbol{I}^p$ and $[x]_{\mathcal{E}} \in (\text{dual } \boldsymbol{I})^q$ with $p + q = n$. A generalized interval $[z] \in \boldsymbol{K}$ is $(f, [x])$-interpretable if

$$(\forall x_{\mathcal{A}} \in [x]_{\mathcal{A}})\,(Q_z z \in \text{pro } [z])\,(\exists x_{\mathcal{E}} \in \text{pro } [x]_{\mathcal{E}}), (f(x) = z)$$

where $Q_z = \exists$ if $[z]$ is proper, and $Q_z = \forall$ otherwise.

Example: Kaucher multiplication

Example (Interpretation of the Kaucher multiplication in the case $\mathcal{Z} \times$ dual $\mathcal{Z}$)

$[z] = [x] \times [y] = 0$ when $[x] \in \mathcal{Z} = \{[x],\ \underline{x} \leqslant 0 \leqslant \overline{x}\}$ (e.g. [-5,4]) and $[y] \in$ dual $\mathcal{Z} = \{[x],\ \underline{x} \geqslant 0 \geqslant \overline{x}\}$ (e.g. [1,-1]).

Definition (reminder)

Let $f : \mathbb{R}^2 \to \mathbb{R}$ and $[x] \in \boldsymbol{I}$ and $[y] \in$ (dual $\boldsymbol{I}$). A generalized interval $[z] \in \boldsymbol{K}$ is $(f, [x] \times [y])$-interpretable if

$$(\forall x \in [x])\,(Q_z z \in \text{pro}\ [z])\,(\exists y \in [y]), (f(x, y) = x \times y = z)$$

where $Q_z = \exists$ if $[z]$ is proper, and $Q_z = \forall$ otherwise.

Example: Kaucher multiplication

Example (Interpretation of the Kaucher multiplication in the case $\mathcal{Z} \times$ dual $\mathcal{Z}$)

$[z] = [x] \times [y] = 0$ when $[x] \in \mathcal{Z} = \{[x],\ \underline{x} \leqslant 0 \leqslant \overline{x}\}$ (e.g. [-5,4]) and $[y] \in$ dual $\mathcal{Z} = \{[x],\ \underline{x} \geqslant 0 \geqslant \overline{x}\}$ (e.g. [1,-1]).

Definition (reminder)

Let $f : \mathbb{R}^2 \to \mathbb{R}$ and $[x] \in \boldsymbol{I}$ and $[y] \in$ (dual $\boldsymbol{I}$). A generalized interval $[z] \in \boldsymbol{K}$ is $(f, [x] \times [y])$-interpretable if

$$(\forall x \in [x])\,(\forall z \in \text{pro } [z])\,(\exists y \in [y]), (f(x, y) = x \times y = z)$$

where $Q_z = \exists$ if $[z]$ is proper, and $Q_z = \forall$ otherwise.

Let us suppose $[z]$ improper:

- computing $[z] = [x] \times [y]$ consists in finding $[z]$ such that $\forall x \in [x]$, $\forall z \in$ pro $[z]$, $\exists y \in$ pro $[y]$, $z = x \times y$;
- instanciating the property for $0 \in [x]$, we get $\forall z \in$ pro $[z]$, $(\exists y \in$ pro $[y])$ $z = 0$. Thus $[z]$ is necessarily 0.

Limitations of Kaucher and interval arithmetic

Kaucher arithmetic defines a generalized interval natural extension :

- Interpretable as outer approximation when all intervals are proper (interval arithmetic), but may be insufficiently accurate because of dependency problem
- Interpretable as inner approximation when all intervals are improper and f is given by an arithmetic expression with single occurences of variables

Example

Let $f(x) = x^2 - x$ that we want to evaluate on $[2, 3]$. Exact range is $\text{range}(f, [2, 3]) = [2, 6]$.

- dependency problem in outer-approximation: accuracy loss
  $[f]([2, 3]) = [2, 3] * [2, 3] - [2, 3] = [1, 7]$
- single-occurence limitation in inner-approximation: not interpretable
  $[f]([3, 2])$ computed with Kaucher arithmetic is $[7, 1]$, not an inner-approximation.

A solution: mean-value theorem (and inductive construction of a zonotopic outer-approximation)

Solving the single-occurence limitation

Generalized mean-value theorem (Goldsztejn 2005)

Let $f : \mathbb{R}^n \to \mathbb{R}$ be differentiable, $[x] \in \boldsymbol{K}^n$, and suppose that for each $i \in \{1, \ldots, n\}$, we can compute $[\boldsymbol{\Delta}_i] \in \boldsymbol{I}$ such that $\left\{ \frac{\partial f}{\partial x_i}(x),\ x \in \text{pro } [x] \right\} \subseteq [\boldsymbol{\Delta}_i]$. Then, for any $\tilde{x} \in \text{pro } [x]$,

$$\tilde{f}([x]) = f(\tilde{x}) + \sum_{i=1}^{n} [\boldsymbol{\Delta}_i]([x_i] - \tilde{x}_i),$$

evaluated with Kaucher interval arithmetic, is $(f, [x])$-interpretable. In particular,

- if $\tilde{f}(\text{dual pro } [x])$, computed with Kaucher arithmetic, is improper, then pro $\tilde{f}(\text{dual pro } [x])$ is an inner approximation of $\{f(x),\ x \in \text{pro } [x]\} = \text{range}(f, [x])$.
- $\tilde{f}(\text{pro } [x])$ is proper and it is an outer approximation of $\text{range}(f, [x])$.

Example (Mean-value theorem for same example $f(x) = x^2 - x$ for $2 \leq x \leq 3$)

$\tilde{f}([x]) = f(2.5) + [f'([2, 3])]([x] - 2.5) = 3.75 + [3, 5]([x] - 2.5)$ is $(f, [x])$-interpretable:

Solving the single-occurence limitation

Generalized mean-value theorem (Goldsztejn 2005)

Let $f : \mathbb{R}^n \to \mathbb{R}$ be differentiable, $[x] \in \boldsymbol{K}^n$, and suppose that for each $i \in \{1, \ldots, n\}$, we can compute $[\boldsymbol{\Delta}_i] \in \boldsymbol{I}$ such that $\left\{ \frac{\partial f}{\partial x_i}(x),\ x \in \text{pro } [x] \right\} \subseteq [\boldsymbol{\Delta}_i]$. Then, for any $\tilde{x} \in \text{pro } [x]$,

$$\tilde{f}([x]) = f(\tilde{x}) + \sum_{i=1}^{n} [\boldsymbol{\Delta}_i]([x_i] - \tilde{x}_i),$$

evaluated with Kaucher interval arithmetic, is $(f, [x])$-interpretable. In particular,

- if $\tilde{f}(\text{dual pro } [x])$, computed with Kaucher arithmetic, is improper, then pro $\tilde{f}(\text{dual pro } [x])$ is an inner approximation of $\{f(x),\ x \in \text{pro } [x]\} = \text{range}(f, [x])$.
- $\tilde{f}(\text{pro } [x])$ is proper and it is an outer approximation of $\text{range}(f, [x])$.

Example (Mean-value theorem for same example $f(x) = x^2 - x$ for $2 \leq x \leq 3$)

$\tilde{f}([x]) = f(2.5) + [f'([2,3])]([x] - 2.5) = 3.75 + [3,5]([x] - 2.5)$ is $(f, [x])$-interpretable:

$$pro(3.75 + [3,5]([3,2] - 2.5) \subseteq \text{range}(f, [2,3]) \subseteq 3.75 + [3,5]([2,3] - 2.5)$$

Solving the single-occurence limitation

Generalized mean-value theorem (Goldsztejn 2005)

Let $f : \mathbb{R}^n \to \mathbb{R}$ be differentiable, $[x] \in \boldsymbol{K}^n$, and suppose that for each $i \in \{1, \ldots, n\}$, we can compute $[\boldsymbol{\Delta}_i] \in \boldsymbol{I}$ such that $\left\{ \frac{\partial f}{\partial x_i}(x),\ x \in \text{pro } [x] \right\} \subseteq [\boldsymbol{\Delta}_i]$. Then, for any $\tilde{x} \in \text{pro } [x]$,

$$\tilde{f}([x]) = f(\tilde{x}) + \sum_{i=1}^{n} [\boldsymbol{\Delta}_i]([x_i] - \tilde{x}_i),$$

evaluated with Kaucher interval arithmetic, is $(f, [x])$-interpretable. In particular,

- if $\tilde{f}(\text{dual pro } [x])$, computed with Kaucher arithmetic, is improper, then pro $\tilde{f}(\text{dual pro } [x])$ is an inner approximation of $\{f(x),\ x \in \text{pro } [x]\} = \text{range}(f, [x])$.
- $\tilde{f}(\text{pro } [x])$ is proper and it is an outer approximation of $\text{range}(f, [x])$.

Example (Mean-value theorem for same example $f(x) = x^2 - x$ for $2 \leq x \leq 3$)

$\tilde{f}([x]) = f(2.5) + [f'([2,3])]([x] - 2.5) = 3.75 + [3,5]([x] - 2.5)$ is $(f, [x])$-interpretable:

$$pro(3.75 + [3,5]([0.5, -0.5]) \subseteq \text{range}(f, [2,3]) \subseteq 3.75 + [3,5]([-0.5, 0.5])$$

Solving the single-occurence limitation

Generalized mean-value theorem (Goldsztejn 2005)

Let $f : \mathbb{R}^n \to \mathbb{R}$ be differentiable, $[x] \in \boldsymbol{K}^n$, and suppose that for each $i \in \{1, \ldots, n\}$, we can compute $[\boldsymbol{\Delta}_i] \in \boldsymbol{I}$ such that $\left\{ \frac{\partial f}{\partial x_i}(x),\ x \in \text{pro } [x] \right\} \subseteq [\boldsymbol{\Delta}_i]$. Then, for any $\tilde{x} \in \text{pro } [x]$,

$$\tilde{f}([x]) = f(\tilde{x}) + \sum_{i=1}^{n} [\boldsymbol{\Delta}_i]([x_i] - \tilde{x}_i),$$

evaluated with Kaucher interval arithmetic, is $(f, [x])$-interpretable. In particular,

- if $\tilde{f}(\text{dual pro } [x])$, computed with Kaucher arithmetic, is improper, then pro $\tilde{f}(\text{dual pro } [x])$ is an inner approximation of $\{f(x),\ x \in \text{pro } [x]\} = \text{range}(f, [x])$.
- $\tilde{f}(\text{pro } [x])$ is proper and it is an outer approximation of $\text{range}(f, [x])$.

Example (Mean-value theorem for same example $f(x) = x^2 - x$ for $2 \leq x \leq 3$)

$\tilde{f}([x]) = f(2.5) + [f'([2,3])]([x] - 2.5) = 3.75 + [3,5]([x] - 2.5)$ is $(f, [x])$-interpretable:

$$pro(3.75 + [1.5, -1.5]) \subseteq \text{range}(f, [2,3]) \subseteq 3.75 + [-2.5, 2.5]$$

Solving the single-occurence limitation

Generalized mean-value theorem (Goldsztejn 2005)

Let $f : \mathbb{R}^n \to \mathbb{R}$ be differentiable, $[x] \in \boldsymbol{K}^n$, and suppose that for each $i \in \{1, \ldots, n\}$, we can compute $[\boldsymbol{\Delta}_i] \in \boldsymbol{I}$ such that $\left\{ \frac{\partial f}{\partial x_i}(x),\ x \in \text{pro } [x] \right\} \subseteq [\boldsymbol{\Delta}_i]$. Then, for any $\tilde{x} \in \text{pro } [x]$,

$$\tilde{f}([x]) = f(\tilde{x}) + \sum_{i=1}^{n} [\boldsymbol{\Delta}_i]([x_i] - \tilde{x}_i),$$

evaluated with Kaucher interval arithmetic, is $(f, [x])$-interpretable. In particular,

- if $\tilde{f}(\text{dual pro } [x])$, computed with Kaucher arithmetic, is improper, then pro $\tilde{f}(\text{dual pro } [x])$ is an inner approximation of $\{f(x),\ x \in \text{pro } [x]\} = \text{range}(f, [x])$.
- $\tilde{f}(\text{pro } [x])$ is proper and it is an outer approximation of $\text{range}(f, [x])$.

Example (Mean-value theorem for same example $f(x) = x^2 - x$ for $2 \leq x \leq 3$)

$\tilde{f}([x]) = f(2.5) + [f'([2, 3])]([x] - 2.5) = 3.75 + [3, 5]([x] - 2.5)$ is $(f, [x])$-interpretable:

$$pro([5.25, 2.25]) \subseteq \text{range}(f, [2, 3]) \subseteq [1.25, 6.25]$$

Solving the single-occurence limitation

Generalized mean-value theorem (Goldsztejn 2005)

Let $f : \mathbb{R}^n \to \mathbb{R}$ be differentiable, $[x] \in \boldsymbol{K}^n$, and suppose that for each $i \in \{1, \ldots, n\}$, we can compute $[\boldsymbol{\Delta}_i] \in \boldsymbol{I}$ such that $\left\{ \frac{\partial f}{\partial x_i}(x),\ x \in \text{pro } [x] \right\} \subseteq [\boldsymbol{\Delta}_i]$. Then, for any $\tilde{x} \in \text{pro } [x]$,

$$\tilde{f}([x]) = f(\tilde{x}) + \sum_{i=1}^{n} [\boldsymbol{\Delta}_i]([x_i] - \tilde{x}_i),$$

evaluated with Kaucher interval arithmetic, is $(f, [x])$-interpretable. In particular,

- if $\tilde{f}(\text{dual pro } [x])$, computed with Kaucher arithmetic, is improper, then pro $\tilde{f}(\text{dual pro } [x])$ is an inner approximation of $\{f(x),\ x \in \text{pro } [x]\} = \text{range}(f, [x])$.
- $\tilde{f}(\text{pro } [x])$ is proper and it is an outer approximation of $\text{range}(f, [x])$.

Example (Mean-value theorem for same example $f(x) = x^2 - x$ for $2 \leq x \leq 3$)

$\tilde{f}([x]) = f(2.5) + [f'([2, 3])]([x] - 2.5) = 3.75 + [3, 5]([x] - 2.5)$ is $(f, [x])$-interpretable:

$$[2.25, 5.25] \subseteq \text{range}(f, [2, 3]) \subseteq [1.25, 6.25]$$

Solving the single-occurence limitation

Generalized mean-value theorem (Goldsztejn 2005)

Let $f : \mathbb{R}^n \to \mathbb{R}$ be differentiable, $[x] \in \boldsymbol{K}^n$, and suppose that for each $i \in \{1, \ldots, n\}$, we can compute $[\boldsymbol{\Delta}_i] \in \boldsymbol{I}$ such that $\left\{ \frac{\partial f}{\partial x_i}(x),\ x \in \text{pro } [x] \right\} \subseteq [\boldsymbol{\Delta}_i]$. Then, for any $\tilde{x} \in \text{pro } [x]$,

$$\tilde{f}([x]) = f(\tilde{x}) + \sum_{i=1}^{n} [\boldsymbol{\Delta}_i]([x_i] - \tilde{x}_i),$$

evaluated with Kaucher interval arithmetic, is $(f, [x])$-interpretable. In particular,

- if $\tilde{f}(\text{dual pro } [x])$, computed with Kaucher arithmetic, is improper, then pro $\tilde{f}(\text{dual pro } [x])$ is an inner approximation of $\{f(x),\ x \in \text{pro } [x]\} = \text{range}(f, [x])$.
- $\tilde{f}(\text{pro } [x])$ is proper and it is an outer approximation of $\text{range}(f, [x])$.

Example (Mean-value theorem for same example $f(x) = x^2 - x$ for $2 \leq x \leq 3$)

$\tilde{f}([x]) = f(2.5) + [f'([2, 3])]([x] - 2.5) = 3.75 + [3, 5]([x] - 2.5)$ is $(f, [x])$-interpretable:

$$[2.25, 5.25] \subseteq \text{range}(f, [2, 3]) \subseteq [1.25, 6.25]$$

solves the single-occurence limitation

Inner-approximated flowpipes for uncertain ODEs

Generalized mean-value theorem on the solution $z_0 \mapsto z(t, z_0)$ of the ODE:

we need a guaranteed enclosure of $z(t, \tilde{z}_0)$ for some $\tilde{z}_0 \in$ pro $[z_0]$ and $\left\{ \frac{\partial z}{\partial z_{0,i}}(t, z_0),\ z_0 \in \text{pro } [z_0] \right\} \subseteq [\boldsymbol{J}_i]$: Taylor models

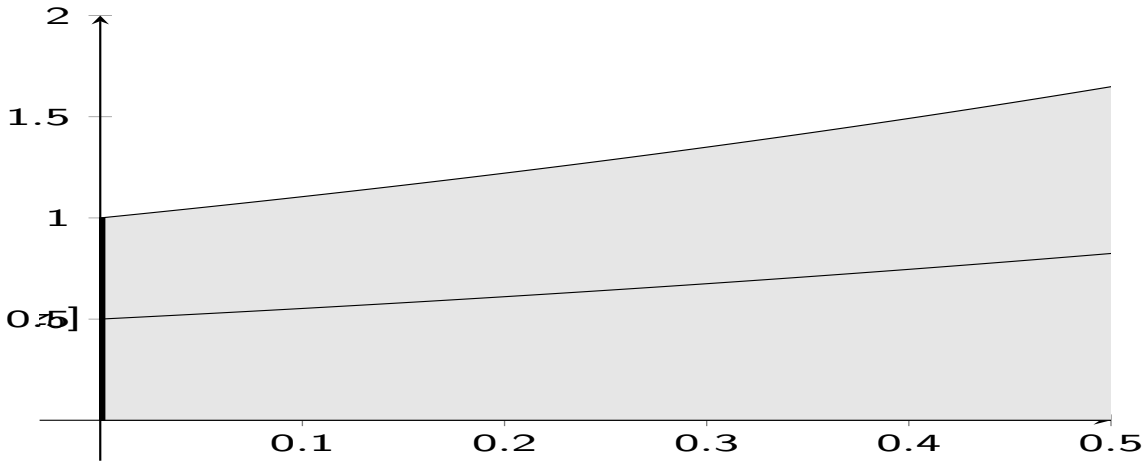
Algorithm (Init: $j = 0$, $t_j = t_0$, $[\boldsymbol{z}_j] = [\boldsymbol{z}_0]$, $[\tilde{z}_j] = \tilde{z}_0 \in [\boldsymbol{z}_0]$, $[\boldsymbol{J}_j] = Id$)

- For each time interval $[t_j, t_{j+1}]$, build Taylor models for:
  - $[\tilde{z}](t, t_j, [\tilde{z}_j])$ outer enclosure of $z(t, \tilde{z}_0)$ valid on $[t_j, t_{j+1}]$
  - $[z](t, t_j, [z_j])$ outer enclosure of $z(t, [z_0])$
  - $[J](t, t_j, [z_j], [J_j])$ outer enclosure of Jacobian $\frac{\partial z}{\partial z_0}(t, [z_0])$ (can be derived from $[z]$)
- Deduce an inner-approximation valid for t in $[t_j, t_{j+1}]$: if

$$]\boldsymbol{z}[(t, t_j) = [\tilde{\boldsymbol{z}}](t, t_j, [\tilde{\boldsymbol{z}}_j]) + [\boldsymbol{J}](t, t_j, [\boldsymbol{z}_j]) * ([\overline{z_0}, \underline{z_0}] - \tilde{z}_0)$$

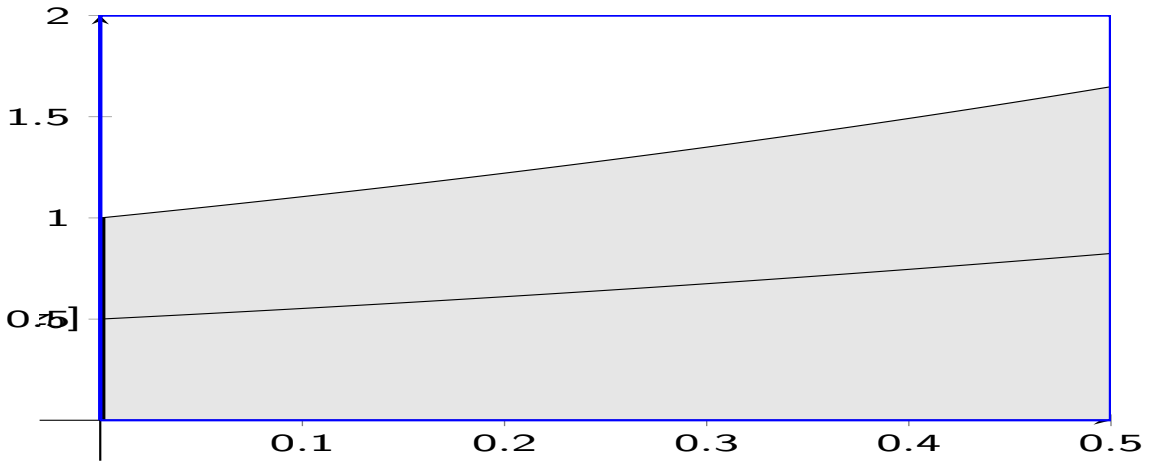
  is an improper interval, then pro $]\boldsymbol{z}[(t, t_j)$ is an inner-approximation of the set of solutions $\{z(t, z_0),\ z_0(t_0) \in \boldsymbol{z}_0\}$, otherwise the inner-approximation is empty.
- $[\boldsymbol{z}_{j+1}] = [\boldsymbol{z}](t_{j+1}, t_j, [\boldsymbol{z}_j])$, $[\tilde{\boldsymbol{z}}_{j+1}] = [\tilde{\boldsymbol{z}}](t_{j+1}, t_j, [\tilde{\boldsymbol{z}}_j])$, $[\boldsymbol{J}_{j+1}] = [\boldsymbol{J}](t, t_j, [\boldsymbol{z}_j], [J_j])$

Example: simple ODE $\dot{z} = z$ with $z_0 \in [z_0] = [0, 1]$, on $t \in [0, 0.5]$



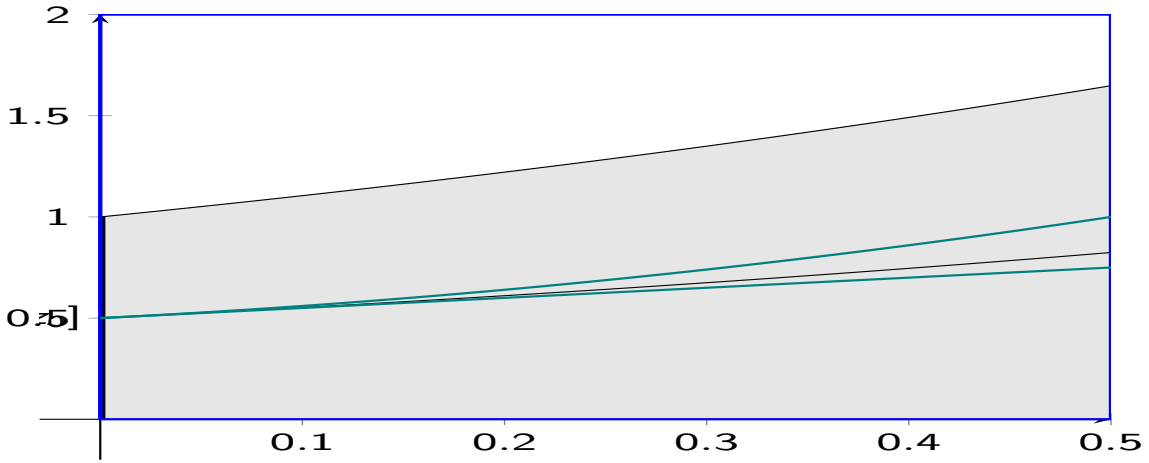
- Init: $[z_0] = [0, 1]$, $\tilde{z}_0 = 0.5$, $[J_0] = 1$

Example: simple ODE $\dot{z} = z$ with $z_0 \in [z_0] = [0, 1]$, on $t \in [0, 0.5]$



- Init: $[z_0] = [0, 1]$, $\tilde{z}_0 = 0.5$, $[J_0] = 1$
- A priori enclosures: $\forall t \in [0, 0.5], \forall z_0 \in [0, 1]$, $z(t, z_0) \in [0, 2]$ and $J(t, z_0) \in [1, 2]$

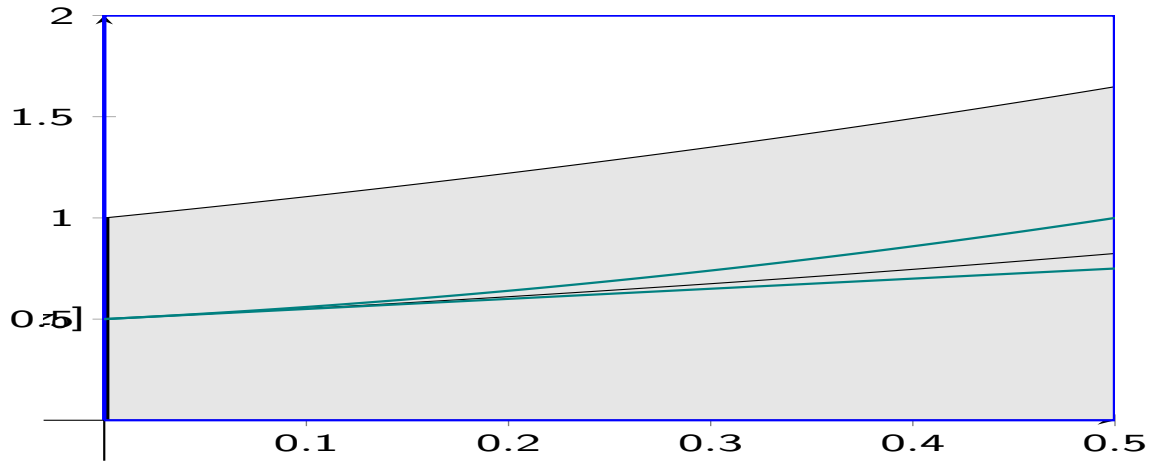
Example: simple ODE $\dot{z} = z$ with $z_0 \in [z_0] = [0, 1]$, on $t \in [0, 0.5]$



- Init: $[z_0] = [0, 1]$, $\tilde{z}_0 = 0.5$, $[J_0] = 1$
- A priori enclosures: $\forall t \in [0, 0.5], \forall z_0 \in [0, 1]$, $z(t, z_0) \in [0, 2]$ and $J(t, z_0) \in [1, 2]$
  - Taylor Model for the center $z(t, \tilde{z}_0)$, $\tilde{z}_0 \in [z_0] = [0, 1]$:

$$\begin{aligned} z(t, z_0) &= z(0, z_0) + z(0, z_0)t + \frac{z(\xi, z_0)}{2} t^2, \quad \xi \in [0, 0.5] \\ [z](t, \tilde{z}_0) &= \tilde{z}_0 + \tilde{z}_0 t + [0, 1] t^2 \end{aligned}$$

Example: simple ODE $\dot{z} = z$ with $z_0 \in [z_0] = [0, 1]$, on $t \in [0, 0.5]$



- Init: $[z_0] = [0, 1]$, $\tilde{z}_0 = 0.5$, $[J_0] = 1$
- A priori enclosures: $\forall t \in [0, 0.5], \forall z_0 \in [0, 1]$, $z(t, z_0) \in [0, 2]$ and $J(t, z_0) \in [1, 2]$
  - Taylor Model for the center $z(t, \tilde{z}_0)$, $\tilde{z}_0 \in [z_0] = [0, 1]$:

$$\begin{aligned} z(t, z_0) &= z(0, z_0) + z(0, z_0)t + \frac{z(\xi, z_0)}{2} t^2, \quad \xi \in [0, 0.5] \\ [z](t, \tilde{z}_0) &= \tilde{z}_0 + \tilde{z}_0 t + [0, 1] t^2 \end{aligned}$$

  - Taylor model for the Jacobian for all $z_0 \in [z_0] = [0, 1]$

$$\begin{aligned} J(t, z_0) &= 1 + J(0, z_0)t + \frac{J(\xi, z_0)}{2} t^2, \quad \xi \in [0, 0.5] \\ [J]\,(t, [z_0]) &= = 1 + t + [0.5, 1]\, t^2 \end{aligned}$$

Mean-value theorem, with $\tilde{z_0} = \text{mid}([z_0]) = 0.5$ for inner tube:

$$]\boldsymbol{z}[(t,[z_0]) \quad = \quad [\tilde{\boldsymbol{z}}](t,t_j,[\tilde{\boldsymbol{z}}_j]) + [\boldsymbol{J}](t,t_j,[\boldsymbol{z}_j]) \times ([\overline{z_0},\underline{z_0}] - \tilde{z_0})$$

Mean-value theorem, with $\tilde{z_0} = \text{mid}([z_0]) = 0.5$ for inner tube:

$$
\begin{aligned}
]z[(t,[z_0]) &= [\tilde{z}](t,t_j,[\tilde{z}_j]) + [\boldsymbol{J}](t,t_j,[z_j]) \times ([\overline{z_0},\underline{z_0}] - \tilde{z_0}) \\
&= [\tilde{z}](t,0.5) + [\boldsymbol{J}](t,[z_0]) * ([1,0] - 0.5)
\end{aligned}
$$

Mean-value theorem, with $\tilde{z_0} = \text{mid}([z_0]) = 0.5$ for inner tube:

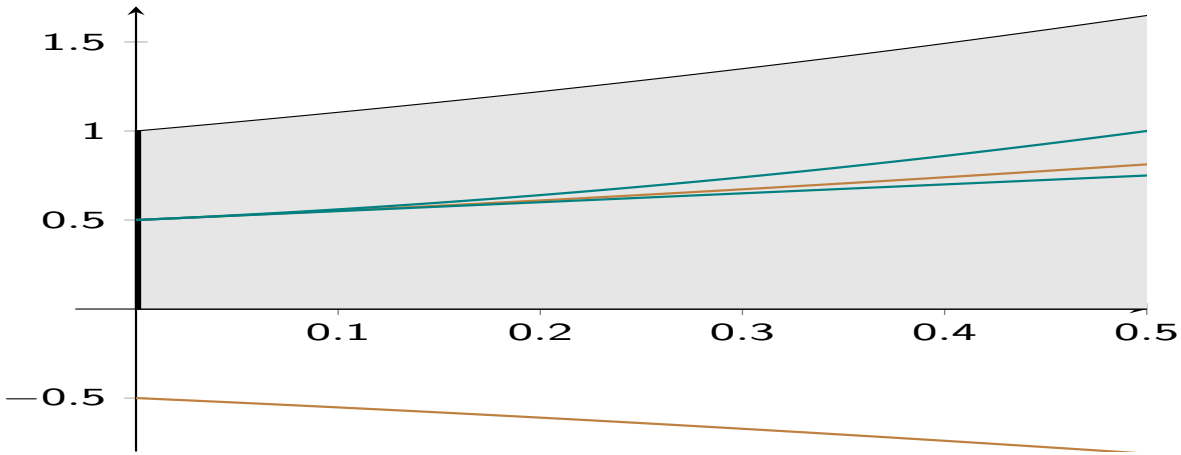
$$
\begin{aligned}
]z[(t,[z_0]) &= [\tilde{z}](t,t_j,[\tilde{z}_j]) + [J](t,t_j,[z_j]) \times ([\overline{z_0},\underline{z_0}] - \tilde{z_0}) \\
&= [\tilde{z}](t,0.5) + [J](t,[z_0]) * ([1,0] - 0.5) \\
&= \underbrace{0.5 + 0.5t + [0,1]t^2}_{\text{proper}} + \underbrace{[(1 + t + [0.5,1]t^2) \times [0.5,-0.5]}_{\text{improper}} = \text{improper?}
\end{aligned}
$$

Mean-value theorem, with $\tilde{z_0} = \text{mid}([z_0]) = 0.5$ for inner tube:

$$
\begin{aligned}
]z[([t],[z_0]) &= [\tilde{z}]([t],[t_j],[\tilde{z}_j]) + [J]([t],[t_j],[z_j]) \times ([\overline{z_0},\underline{z_0}] - \tilde{z_0}) \\
&= [\tilde{z}]([t],0.5) + [J]([t],[z_0]) * ([1,0] - 0.5) \\
&= \underbrace{0.5 + 0.5[t] + [0,1][t]^2}_{\text{proper}} + \underbrace{[(1 + [t] + [0.5,1][t]^2) \times [0.5,-0.5]}_{\text{improper}} = \text{improper?} \\
&= [0.5 + 0.5[t], 0.5 + 0.5[t] + [t]^2] + \underbrace{[1 + [t] + 0.5[t]^2, 1 + [t] + [t]^2]}_{\in \mathcal{P}} \times \underbrace{[0.5,-0.5]}_{\in \text{dual } \mathcal{Z}}
\end{aligned}
$$

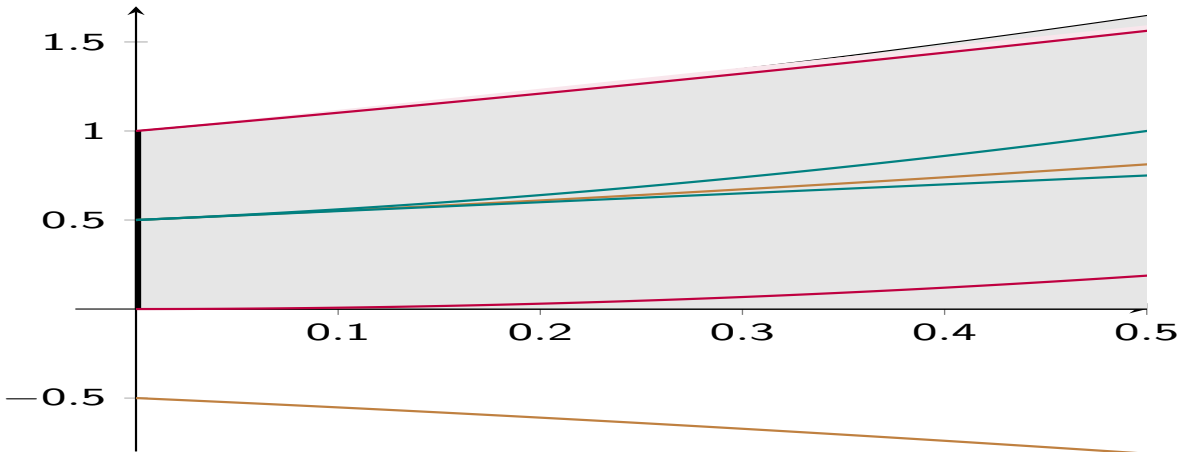
Mean-value theorem, with $\tilde{z_0} = \text{mid}([z_0]) = 0.5$ for inner tube:

$$
\begin{aligned}
]z[(t,[z_0]) &= [\tilde{z}](t,t_j,[\tilde{z}_j]) + [J](t,t_j,[z_j]) \times ([\overline{z_0},\underline{z_0}] - \tilde{z_0}) \\
&= [\tilde{z}](t,0.5) + [J](t,[z_0]) * ([1,0] - 0.5) \\
&= \underbrace{0.5 + 0.5t + [0,1]t^2}_{\text{proper}} + \underbrace{[(1 + t + [0.5,1]t^2) \times [0.5,-0.5]}_{\text{improper}} = \text{improper?} \\
&= [0.5 + 0.5t, 0.5 + 0.5t + t^2] + \underbrace{[1 + t + 0.5t^2, 1 + t + t^2]}_{\in \mathcal{P}} \times \underbrace{[0.5,-0.5]}_{\in \text{dual } \mathcal{Z}} \\
&= \underbrace{[0.5 + 0.5t, 0.5 + 0.5t + t^2]}_{\text{proper x1}} + \underbrace{[0.5 + 0.5t + 0.25t^2, -0.5 - 0.5t - 0.25t^2]}_{\text{x2 improper (iff } 0 \notin [J])}
\end{aligned}
$$



Mean-value theorem, with $\tilde{z_0} = \text{mid}([z_0]) = 0.5$ for inner tube:

$$
\begin{aligned}
]z[([t],[z_0]) &= [\tilde{z}](t, t_j, [\tilde{z}_j]) + [J](t, t_j, [z_j]) \times ([\overline{z_0}, \underline{z_0}] - \tilde{z_0}) \\
&= [\tilde{z}](t, 0.5) + [J](t, [z_0]) * ([1, 0] - 0.5) \\
&= \underbrace{0.5 + 0.5t + [0,1]t^2}_{\text{proper}} + \underbrace{[(1 + t + [0.5,1]t^2) \times [0.5, -0.5]}_{\text{improper}} = \text{improper?} \\
&= [0.5 + 0.5t, 0.5 + 0.5t + t^2] + \underbrace{[1 + t + 0.5t^2, 1 + t + t^2]}_{\in \mathcal{P}} \times \underbrace{[0.5, -0.5]}_{\in \text{dual } \mathcal{Z}} \\
&= \underbrace{[0.5 + 0.5t, 0.5 + 0.5t + t^2]}_{\text{proper x1}} + \underbrace{[0.5 + 0.5t + 0.25t^2, -0.5 - 0.5t - 0.25t^2]}_{\text{x2 improper (iff } 0 \notin [J])} \\
&= [1 + t + 0.25t^2, 0.75t^2] \text{ is improper! (width }]z[= \text{width x2 - width x1)}
\end{aligned}
$$



The case of time dependent inputs/parameters

Outer-approximations

Suppose u is a function of time, sufficiently smooth on each time interval $[t_j, t_{j+1}]$, and with bounded time derivatives $u^{(i)}$, then $\boldsymbol{f}^{[i+1]}$ has to be computed as:

$$\boldsymbol{f}^{[i+1]} = \frac{1}{i+1}\left(\frac{\partial \boldsymbol{f}^{[i]}}{\partial z}.\boldsymbol{f} + \sum_{l=0}^{i-1} \frac{\partial \boldsymbol{f}^{[i]}}{\partial u^{(l)}}.\boldsymbol{u^{(l+1)}}\right)$$

And the rest of the Taylor method applies

The case of time dependent inputs

Inner-approximations

- Restrict $\mathbb{U}$ to the space of m piecewise polynomials of degree l on each interval $[t_j, t_{j+1}]$ (still an inner-approximation) :

$$p_{(u_j^i)}(t) = \sum_{q=0}^{l} u_j^q \frac{(t - t_j)^q}{q!} \tag{2}$$

  for $t \in [t_j, t_{j+1}]$.
- Extend the original ODE by adding variable z_{n+1}, identified with time, solution of $\dot{z}_{n+1} = 1$, $z_{n+1}(0) = 0$. Replacing each control component by expressions (2), and t with z_{n+1}, gives a new ODE system.
- The rest of the inner- Taylor method applies when we have bounds on values and derivatives of controls up to some degree l (that imply interval values for (u_j^q)).

Application: analysis of the (nonlinear) dynamics of a small quadrotor (the crazyflie 2.0) and of its attitude controller

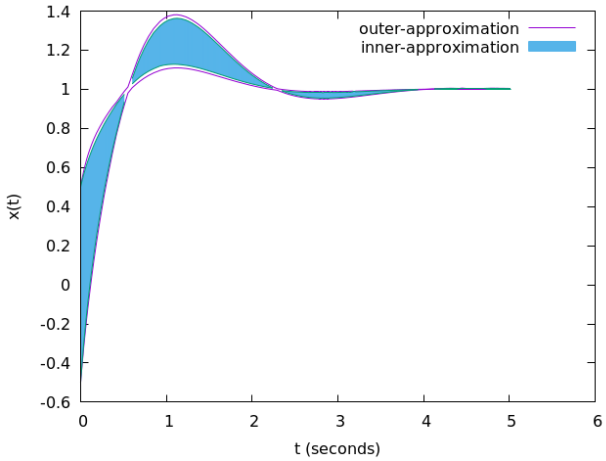
$$
\begin{aligned}
\dot{z} &= -sin(\theta)u + cos(\theta)sin(\phi)v + cos(\theta)cos(\phi)w \\
\dot{u} &= rv - qw + sin(\theta)g \\
\dot{v} &= -ru + pw - cos(\theta)sin(\phi)g \\
\dot{w} &= qu - pv - cos(\theta)cos(\phi)g + \frac{F}{m} \\
\dot{\phi} &= p + cos(\phi)tan(\theta)r + tan(\theta)sin(\phi)q \\
\dot{\theta} &= cos(\phi)q - sin(\phi)r \\
\dot{\psi} &= \frac{cos(\phi)}{cos(\theta)}r + \frac{sin(\phi)}{cos(\theta)}q \\
\dot{p} &= \frac{I_y - I_z}{I_x}qr + \frac{1}{I_x}M_x \\
\dot{q} &= \frac{I_z - I_x}{I_y}pr + \frac{1}{I_y}M_y \\
\dot{r} &= \frac{I_x - I_y}{I_z}pq + \frac{1}{I_z}M_z \\
M_x &= (4C_T C_1^2 d * thrust + 4C_2 C_T d C_1)cmd_\phi - (4C_1^2 C_T d)cmd_\theta cmd_\psi \\
M_y &= (-4C_1^2 C_T d)cmd_\phi * cmd_\psi + (4C_T C_1^2 d * thrust + 4C_2 C_T C_1 d)cmd_\theta \\
M_z &= (-2C_1^2 Cd)cmd_\phi cmd_\theta + (8C_D C_1^2 * thrust + 8C_2 C_D C_1)cmd_\psi \\
F &= C_T C_1^2 cmd_\theta^2 + C_T C_1^2 cmd_\phi^2 + 4C_T C_1^2 cmd_\psi^2 + (4C_T C_1^2) * thrust^2 + (8C_T C_1 C_2) * thrust + 4C_T C_2^2
\end{aligned}
$$

Prove the good behavior of the PID controller which is actually embedded on the crazyflie, with a realistic model, for uncertain parameters.

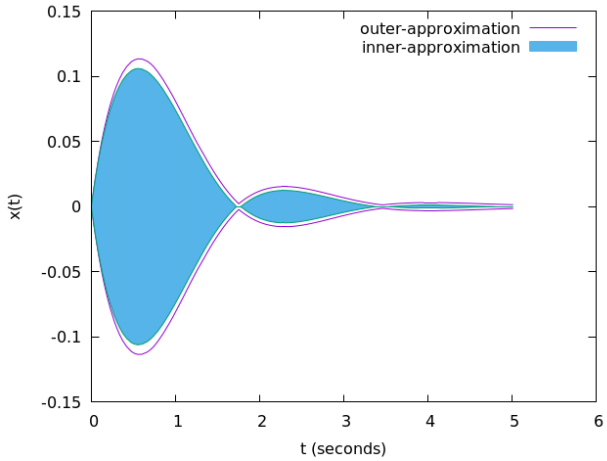
$$
\begin{cases}
thrust &= 1000 * (25(2(z_{sp} - z) - w) + 15\int(2(z_{sp} - z) - w)dt) + 36000 \\
cmd_\phi &= 250(p_{sp} - p) + 500\int(p_{sp} - p)dt \\
cmd_\theta &= 250(q_{sp} - q) + 500\int(q_{sp} - q)dt \\
cmd_\psi &= 120(r_{sp} - r) + 16.7\int(r_{sp} - r)dt
\end{cases}
$$

Reachability results on the crazyflie (with F. Djeumou)

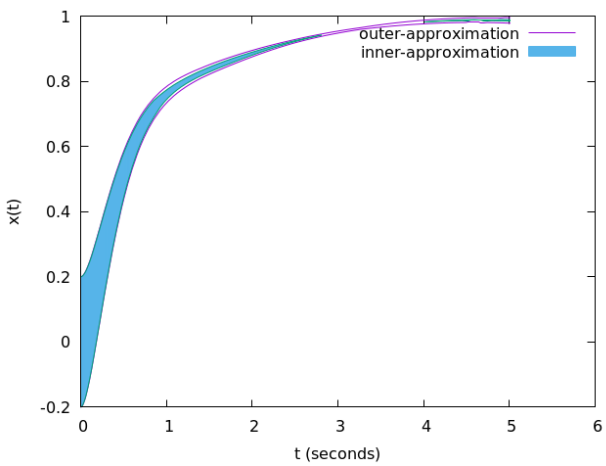
Takes 6.3 seconds with Taylor models of order 5



Roll rate p



Roll ϕ



Altitude z

Robust inner-approximating flowpipes

Let initial set Z_0 and uncertain (constant) parameters $u = (u_{\mathcal{A}}, u_{\mathcal{E}}) \in \mathbb{U}$:

(Maximal) Inner-approximation

An inner-approximation at time t of the reachable set, is $]\boldsymbol{z}[(t; Z_0, \mathbb{U})$ such that $(\forall z \in]\boldsymbol{z}[(t; Z_0, \mathbb{U}))\,(\exists u \in \mathbb{U})\,(\exists z_0 \in Z_0)\,(\varphi(t; z_0, u) = z)$.

Robust (minimal) Inner-approximation

An inner-approximation of the reachable set $\boldsymbol{z}(t; Z_0, \mathbb{U})$ at time t, robust with respect to $u_{\mathcal{A}}$, is a set $]\boldsymbol{z}[_{\mathcal{A}}(t; Z_0, \mathbb{U}_{\mathcal{A}}, \mathbb{U}_{\mathcal{E}})$ such that $(\forall z \in]\boldsymbol{z}[_{\mathcal{A}}(t; Z_0, \mathbb{U}_{\mathcal{A}}, \mathbb{U}_{\mathcal{E}}))\,(\forall u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}})\,(\exists u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}})\,(\exists z_0 \in Z_0)\,(\varphi(t; z_0, u_{\mathcal{A}}, u_{\mathcal{E}}) = z)$.

Theorem (Generalized Mean-Value Theorem again)

If for t in $[t_{ij}, t_{i(j+1)}]$, the following, evaluated with Kaucher arithmetic, is improper

$$
\begin{aligned}
]\boldsymbol{z}[_{\mathcal{A}}(t, t_{ij}, Z_0, \mathbb{U}_{\mathcal{A}}, \mathbb{U}_{\mathcal{E}}) = [\boldsymbol{z}](t, t_{ij}, Z_0, [\tilde{\boldsymbol{z}}_{ij}]) + [\boldsymbol{J}]_{\mathcal{A}}(t, t_{ij}, Z_0, [\boldsymbol{J}_{ij}])(\mathbb{U}_{\mathcal{A}} - \tilde{u}_{\mathcal{A}}) \\
+ [\boldsymbol{J}]_{\mathcal{E}}(t, t_{ij}, Z_0, [\boldsymbol{J}_{ij}])(\mathit{dual}\ \mathbb{U}_{\mathcal{E}} - \tilde{u}_{\mathcal{E}}) + [\boldsymbol{J}]_{Z_0}(t, t_{ij}, Z_0, [\boldsymbol{J}_{ij}])(\mathit{dual}\ Z_0 - \tilde{z}_0)
\end{aligned}
$$

then (pro $]\boldsymbol{z}[_{\mathcal{A}}(t, t_{ij}, Z_0, \mathbb{U}_{\mathcal{A}}, \mathbb{U}_{\mathcal{E}})$) is an inner-approximation of the reachable set $\boldsymbol{z}(t; Z_0, \mathbb{U})$ on $[t_{ij}, t_{i(j+1)}]$, robust to the parameters $u_{\mathcal{A}}$

Robust outer-approximating flowpipes

Remember: the Generalized Mean-value theorem is also suited for outer-approximation!

Theorem (Generalized Mean-Value Theorem again)

If for t in $[t_{ij}, t_{i(j+1)}]$, the following, evaluated with Kaucher arithmetic, is proper

$$[\boldsymbol{z}]_{\mathcal{A}}(t, t_{ij}, Z_0, \mathbb{U}_{\mathcal{A}}, \mathbb{U}_{\mathcal{E}}) = [\boldsymbol{z}](t, t_{ij}, Z_0, [\tilde{\boldsymbol{z}}_{ij}]) + [\boldsymbol{J}]_{\mathcal{A}}(t, t_{ij}, Z_0, [\boldsymbol{J}_{ij}])(\mathbb{U}_{\mathcal{E}} - \tilde{u}_{\mathcal{E}}) + [\boldsymbol{J}]_{Z_0}(t, t_{ij}, Z_0, [\boldsymbol{J}_{ij}])(Z_0 - \tilde{z}_0) + [\boldsymbol{J}]_{\mathcal{E}}(t, t_{ij}, Z_0, [\boldsymbol{J}_{ij}])(\textit{dual}\ \mathbb{U}_{\mathcal{A}} - \tilde{u}_{\mathcal{A}})$$

then $([\boldsymbol{z}]_{\mathcal{A}}(t, t_{ij}, Z_0, \mathbb{U}_{\mathcal{A}}, \mathbb{U}_{\mathcal{E}}))$ is a robust outer-approximation of the reachable set $\boldsymbol{z}(t; Z_0, \mathbb{U})$ on $[t_{ij}, t_{i(j+1)}]$, robust to the parameters $u_{\mathcal{A}}$

Intuitively, the term on $u_{\mathcal{A}}$ is improper, and thus decreases the width of the outer-approximations which may even become empty (more subtle than it looks, see paper!)

An example, a simple self-driving car

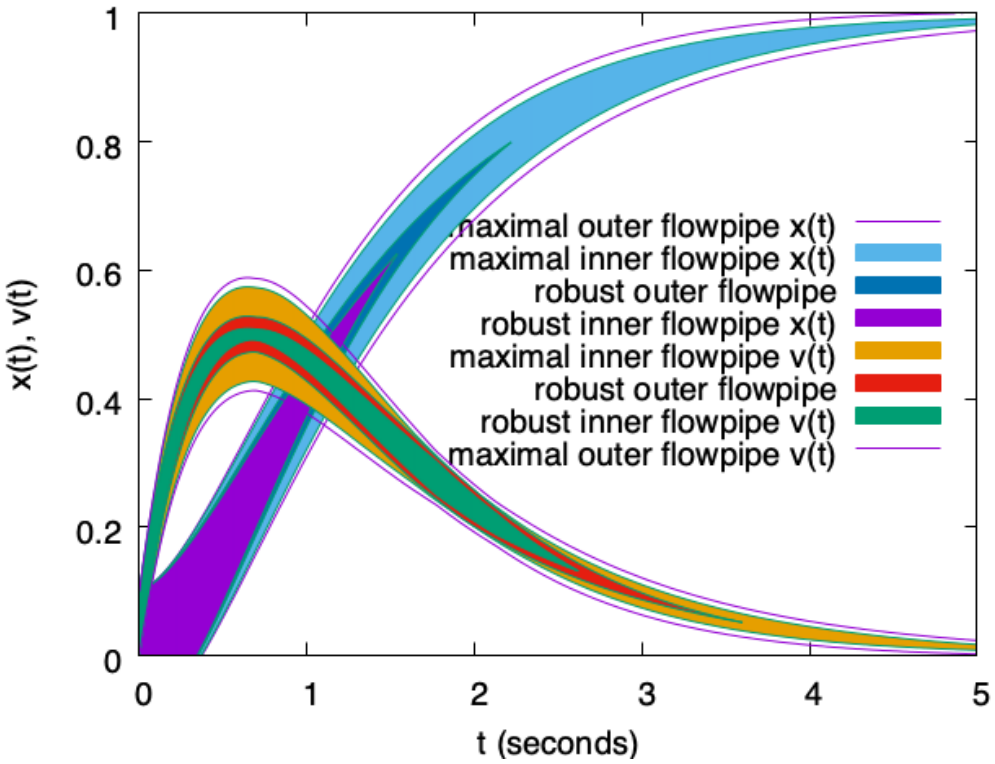
Basic PD-controller for a self-driving car

- controlling the car's position x and velocity v by adjusting its acceleration depending on the current distance to a reference position p_r.
- possibly uncertain (but constant here) coefficients K_p and K_d : $(K_p, K_d) \in [1.95, 2.05] \times [2.95, 3.05]$

$$\begin{cases} \dot{x}(t) = v(t) \\ \dot{v}(t) = -K_p\big(x(t) - p_r\big) - K_d\, v(t) \end{cases}$$

- uncertain initial state $(x_0, v_0) \in [-0.1, 0.1] \times [0, 0.1]$

Graphically

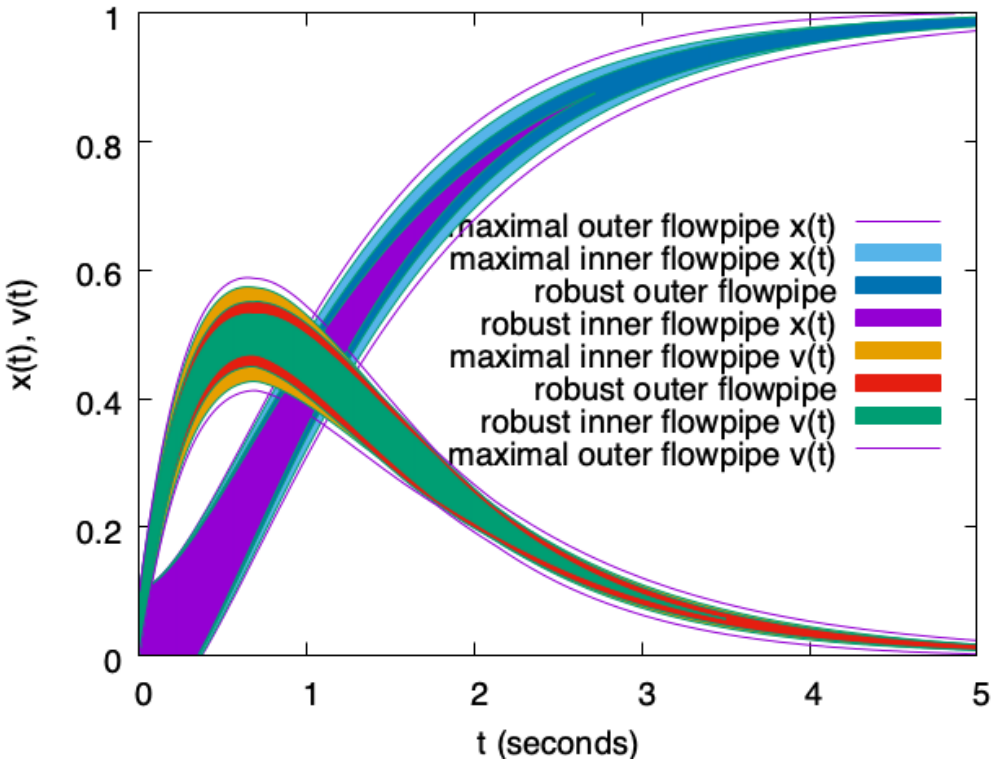


- Maximal outer flowpipes = states that may be reached for some value of input and Kp/Kd
- Maximal inner flowpipes = states guaranteed to be reached for some value of input and Kp/Kd
- Robust outer flowpipes = states that may be reached for some input, whatever Kp/Kd (for any state in the complement, there thus exist some Kp/Kd for which it cannot be reached)
- Robust inner flowpipes = states that are guaranteed to be reached for some input whatever the value of Kp/Kd

Robustness to both Kp and Kd

- The outer-approximations prove safety (the velocity never becomes negative)
- The inner-approximations provide falsification when relevant, and the combinaison of outer and inner approx an accuracy measure γ
- The robust inner-approximation additionally provides falsification with robustness to uncertainty/perturbation in K_p and K_d

Graphically



- Maximal outer flowpipes = states that may be reached for some value of input and Kp/Kd
- Maximal inner flowpipes = states guaranteed to be reached for some value of input and Kp/Kd
- Robust outer flowpipes = states that may be reached for some input, whatever Kp/Kd (for any state in the complement, there thus exist some Kp/Kd for which it cannot be reached)
- Robust inner flowpipes = states that are guaranteed to be reached for some input whatever the value of Kp/Kd

Robustness to Kp only

- The outer-approximations prove safety (the velocity never becomes negative)
- The inner-approximations provide falsification when relevant, and the combinaison of outer and inner approx an accuracy measure γ
- The robust inner-approximation additionally provides falsification with robustness to uncertainty/perturbation in K_p and K_d

Future work

Approximate reachability and verification of temporal properties

- STL-like properties are requirements along traces (or trajectories) but for an uncertain system, we have tubes of trajectories
- Inner and outer approximating tubes of trajectories considered "geometrically" provide some sufficient/necessary conditions
- But these conditions are often too weak/strong
  - reasoning on the envelope will often not be sufficient to prove a property that holds for each trace individually
  - the inner-approximation is fine for proving state reachability, but limited when speaking about trace existence: consider 2 states, inner-approximation proves that both are reached, not that there exist a same trace going through both
- Use the parametrization of the Taylor coefficients by the noise symbols to refine the verification conditions ? (on-going work)

More challenges/applications

- Embedding lightweight verification techniques in autonomous vehicles (limited computation/transmission)
- Distributed hybrid systems (variable transmission delays, coordination problems, etc)

Any questions?

Eric.Goubault@polytechnique.edu
Sylvie.Putot@polytechnique.edu
See also :

- [SAS 2007] E. Goubault and S. Putot, Under-Approximations of Computations in Real Numbers Based on Generalized Affine Arithmetic
- [HSCC 2014] E. Goubault, M. Kieffer, O. Mullier and S. Putot, Inner approximated reachability analysis
- [HSCC 2017] E. Goubault and S. Putot, Forward inner-approximated reachability of non-linear continuous systems
- [CAV 2018] E. Goubault, S. Putot and L. Sahlmann, Inner and Outer Approximating Flowpipes for Delay Differential Equations
- [HSCC 2019] E. Goubault and S. Putot, Inner and Outer Reachability for the Verification of Control Systems