Forward inner-approximated reachability of non-linear continuous systems

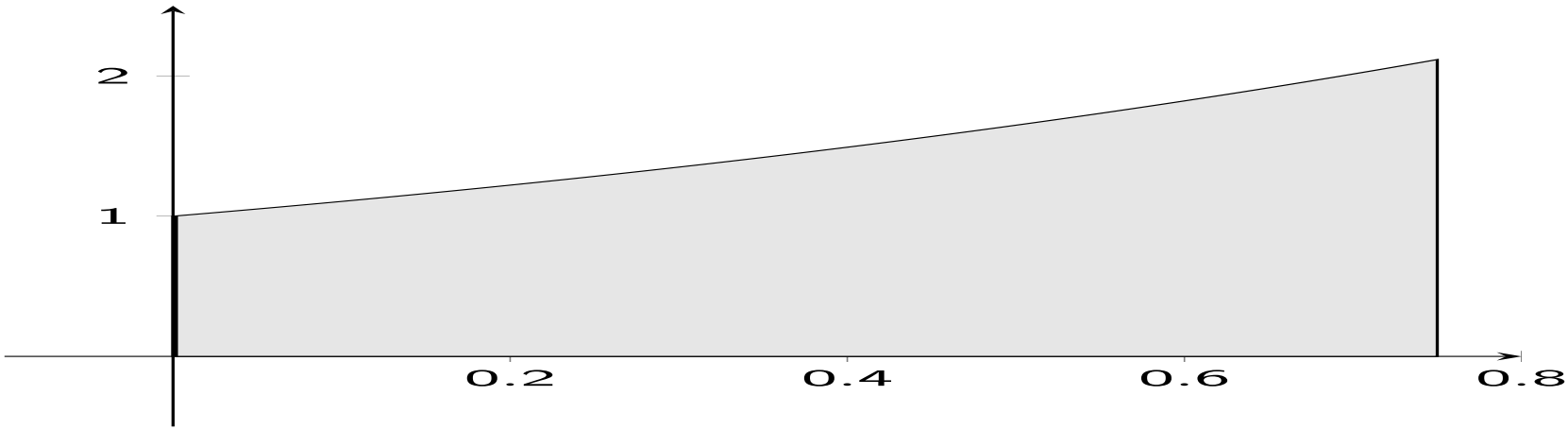
Eric Goubault [1] Sylvie Putot [1]

[1] **LIX, Ecole Polytechnique - CNRS, Université Paris-Saclay**

HSCC, Pittsburgh, April 18, 2017

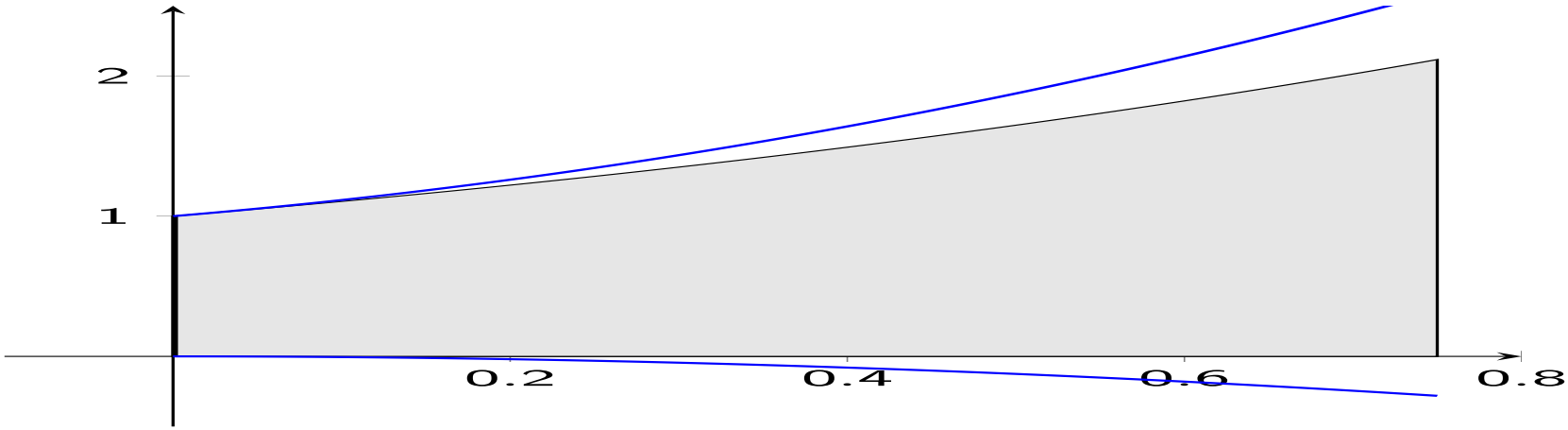
Motivation: bounded-time reachable sets for uncertain dynamical systems $\dot{z}(t) = f(z),\ z(t_0) \in [z_0]$

- Computing reachable sets is central to program analysis, control theory
  - including discretization/roundoff errors, parameters and data uncertainty



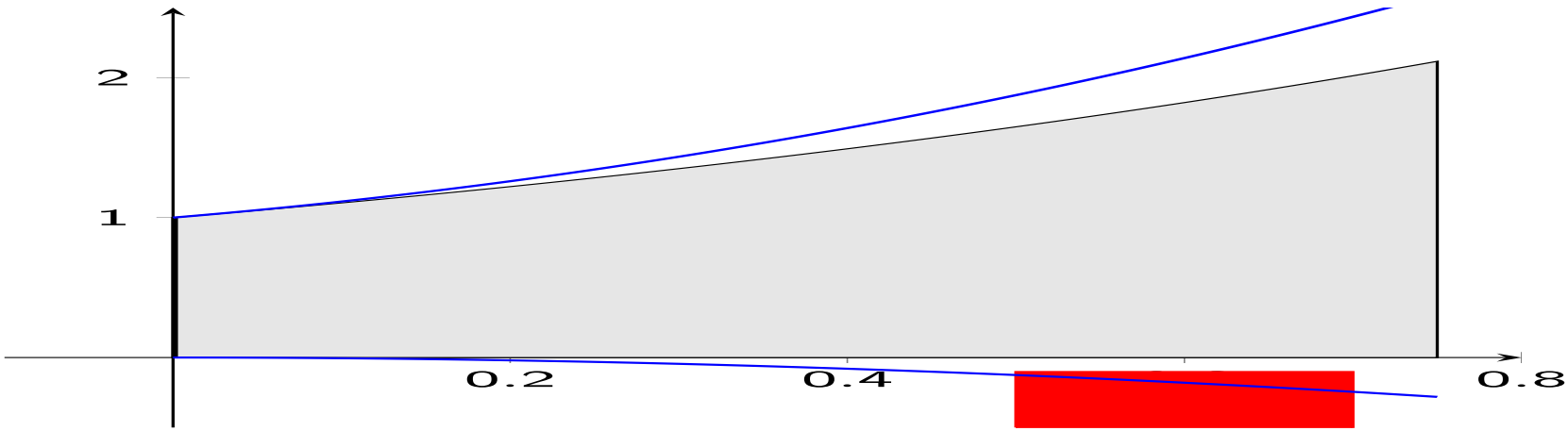
Motivation: bounded-time reachable sets for uncertain dynamical systems $\dot{z}(t) = f(z),\ z(t_0) \in [z_0]$

- Computing reachable sets is central to program analysis, control theory
  - including discretization/roundoff errors, parameters and data uncertainty
- Classically: compute guaranteed (over ou outer-approximated) enclosures



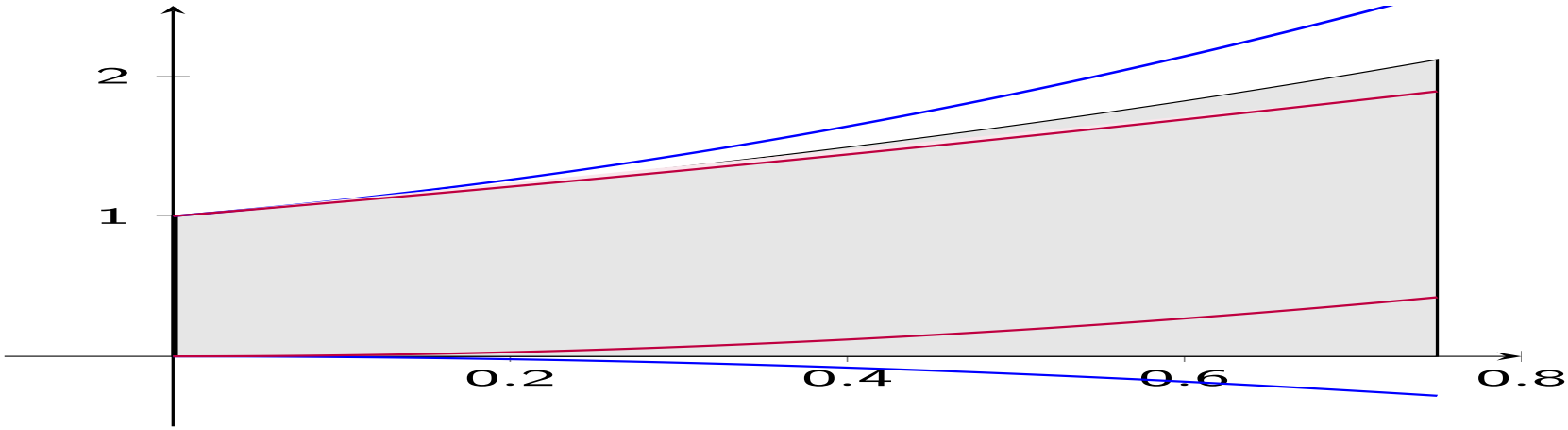
Motivation: bounded-time reachable sets for uncertain dynamical systems $\dot{z}(t) = f(z),\ z(t_0) \in [z_0]$

- Computing reachable sets is central to program analysis, control theory
  - including discretization/roundoff errors, parameters and data uncertainty
- Classically: compute guaranteed (over ou outer-approximated) enclosures
- But: outer approximations provide safety proof but are conservative ("false alarms")



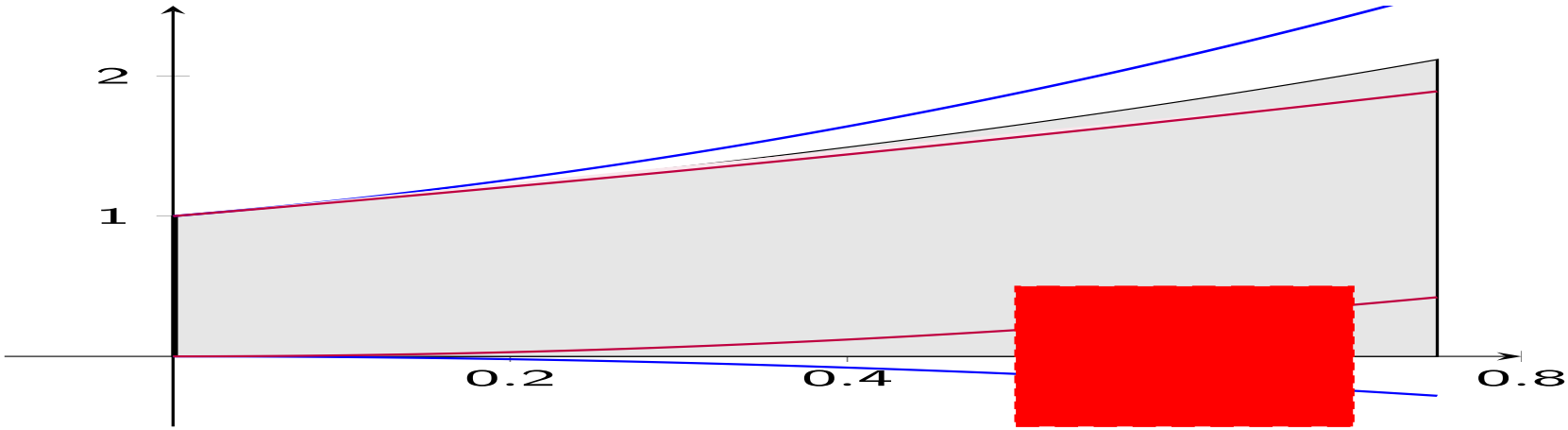
Motivation: bounded-time reachable sets for uncertain dynamical systems $\dot{z}(t) = f(z),\ z(t_0) \in [z_0]$

- Computing reachable sets is central to program analysis, control theory
  - including discretization/roundoff errors, parameters and data uncertainty
- Classically: compute guaranteed (over ou outer-approximated) enclosures
- But: outer approximations provide safety proof but are conservative ("false alarms")
- Here: compute under or inner-approximated flowpipes = sets of values that are guaranteed to be reached, for some value of the uncertain parameters



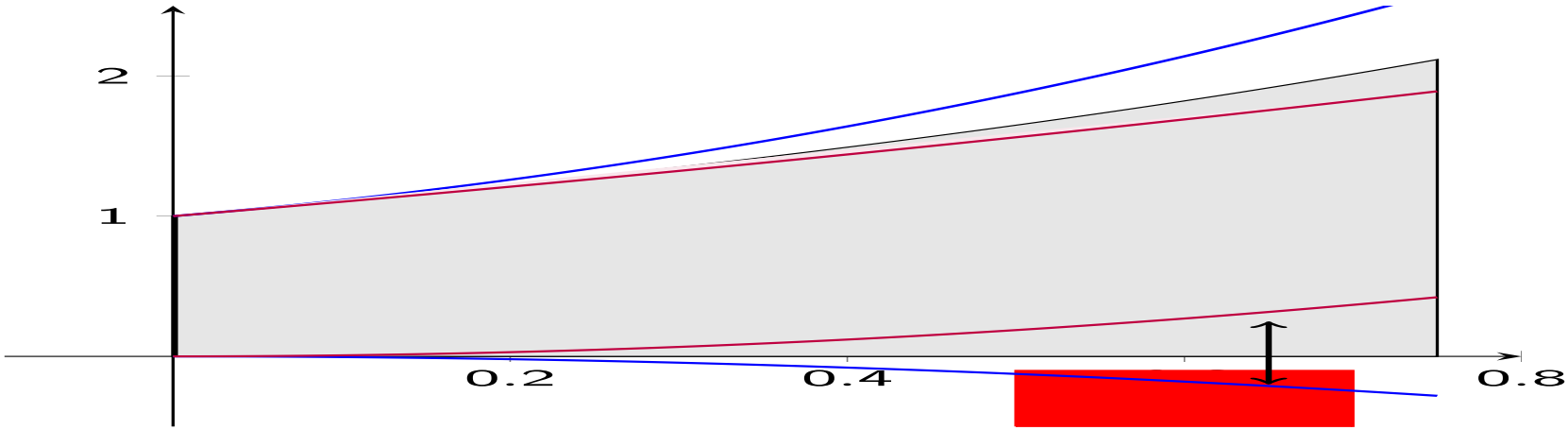
Motivation: bounded-time reachable sets for uncertain dynamical systems $\dot{z}(t) = f(z),\ z(t_0) \in [z_0]$

- Computing reachable sets is central to program analysis, control theory
  - including discretization/roundoff errors, parameters and data uncertainty
- Classically: compute guaranteed (over ou outer-approximated) enclosures
- But: outer approximations provide safety proof but are conservative ("false alarms")
- Here: compute under or inner-approximated flowpipes = sets of values that are guaranteed to be reached, for some value of the uncertain parameters
  - falsification of safety properties



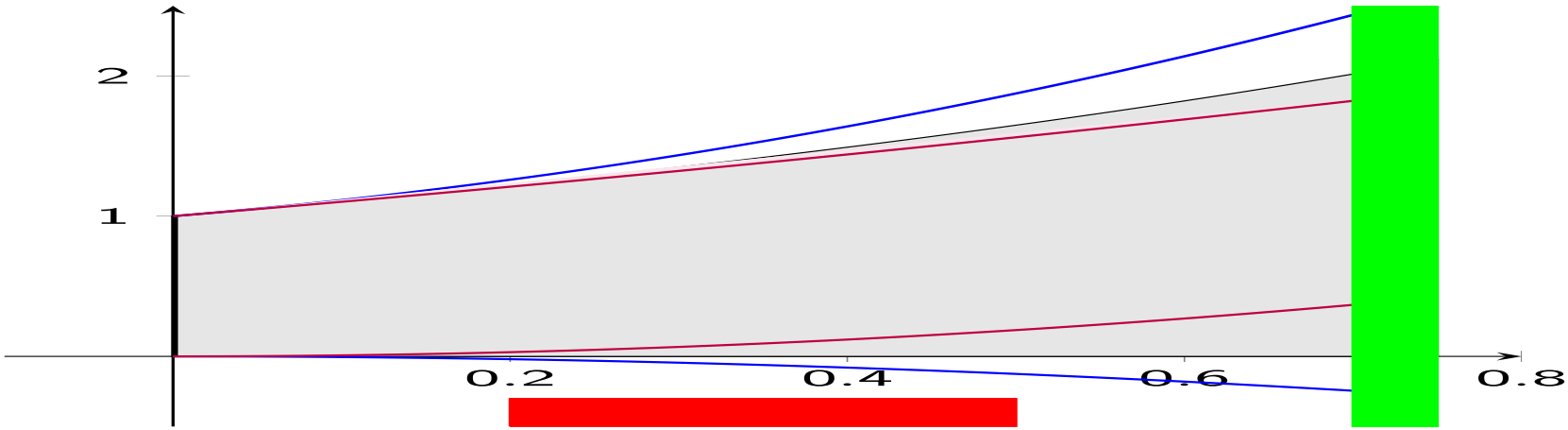
Motivation: bounded-time reachable sets for uncertain dynamical systems $\dot{z}(t) = f(z),\ z(t_0) \in [z_0]$

- Computing reachable sets is central to program analysis, control theory
  - including discretization/roundoff errors, parameters and data uncertainty
- Classically: compute guaranteed (over ou outer-approximated) enclosures
- But: outer approximations provide safety proof but are conservative ("false alarms")
- Here: compute under or inner-approximated flowpipes = sets of values that are guaranteed to be reached, for some value of the uncertain parameters
  - falsification of safety properties
  - when inconclusive, Hausdorff distance between inner and outer tubes gives precision estimates



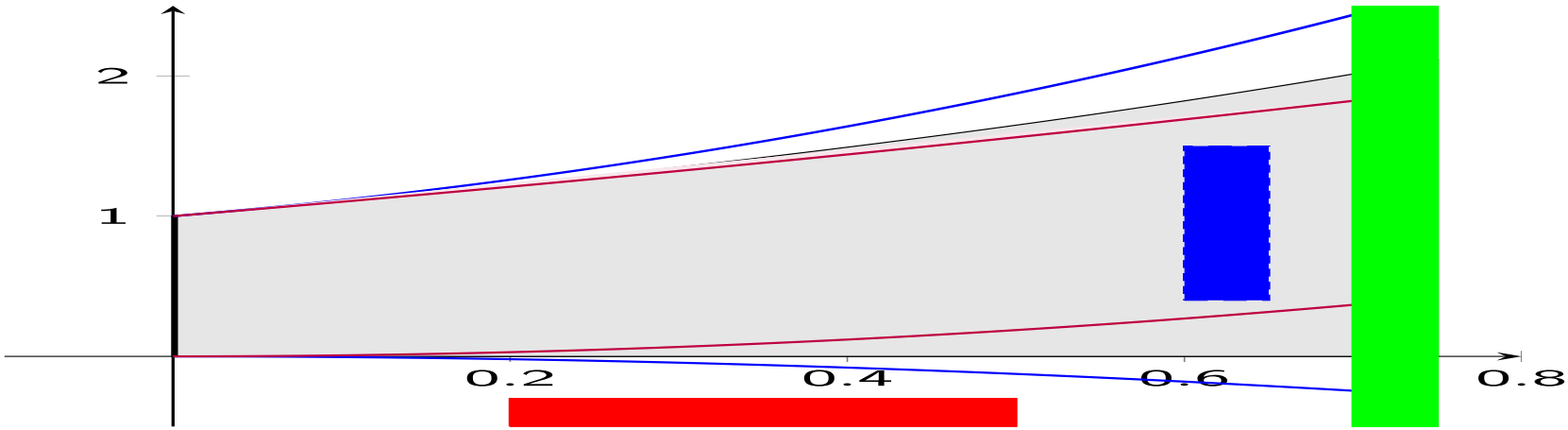
Motivation: bounded-time reachable sets for uncertain dynamical systems $\dot{z}(t) = f(z),\ z(t_0) \in [z_0]$

- Computing reachable sets is central to program analysis, control theory
  - including discretization/roundoff errors, parameters and data uncertainty
- Classically: compute guaranteed (over ou outer-approximated) enclosures
- But: outer approximations provide safety proof but are conservative ("false alarms")
- Here: compute under or inner-approximated flowpipes = sets of values that are guaranteed to be reached, for some value of the uncertain parameters
  - falsification of safety properties
  - when inconclusive, Hausdorff distance between inner and outer tubes gives precision estimates
  - property verification: reach-avoid



Motivation: bounded-time reachable sets for uncertain dynamical systems $\dot{z}(t) = f(z),\ z(t_0) \in [z_0]$

- Computing reachable sets is central to program analysis, control theory
  - including discretization/roundoff errors, parameters and data uncertainty
- Classically: compute guaranteed (over ou outer-approximated) enclosures
- But: outer approximations provide safety proof but are conservative ("false alarms")
- Here: compute under or inner-approximated flowpipes = sets of values that are guaranteed to be reached, for some value of the uncertain parameters
  - falsification of safety properties
  - when inconclusive, Hausdorff distance between inner and outer tubes gives precision estimates
  - property verification: reach-avoid, sweep-avoid; parameter synthesis,



In this talk: inner-approximated flowpipes for uncertain dynamical systems

Inner approximation of the range of $f : \mathbb{R}^n \to \mathbb{R}^p$ on a set $[x]$ using ([HSCC'14])

- 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 $\dot{z}(t) = f(z),\ z(t_0) \in [z_0]$ ([HSCC'17])

- 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: "classical" Taylor model based outer-approximated flowpipes
- then we can apply generalized mean value theorem on z

Implementation and experimental results

Intervals, outer and inner approximations

Intervals: closed connected subsets of $\mathbb{R}$, noted $[x] \in \mathbb{I}$; by extension $[x] \in \mathbb{I}^n$ 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 (or over) approximation

- An *outer approximating extension* of $f : \mathbb{R}^n \to \mathbb{R}$ over intervals is $[f] : \mathbb{I}^n \to \mathbb{I}$ such that
$$\forall [x] \in \mathbb{I}^n, \text{range}(f, [x]) \subseteq [z] = [f]([x])$$
- 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 (or under) approximation

An interval inner approximation $[z] \in \mathbb{I}$ 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 $K = \{[a, b],\ a \in \mathbb{R}, b \in \mathbb{R}\}$
- 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 $[x] \in K^n$, decomposed in $[x]_{\mathcal{A}} \in I^p$ and $[x]_{\mathcal{E}} \in (\text{dual } I)^q$ with $p + q = n$. A generalized interval $[z] \in K$ 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 $[x] \in K^n$, $f([x])$, computed using Kaucher arithmetic, is $(f, [x])$-interpretable.

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

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

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, $[x] \in K^n$, and suppose that for each $i \in \{1, \ldots, n\}$, we can compute $[\boldsymbol{\Delta}_i] \in I$ 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, $[x] \in K^n$, and suppose that for each $i \in \{1, \ldots, n\}$, we can compute $[\boldsymbol{\Delta}_i] \in I$ 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, $[x] \in K^n$, and suppose that for each $i \in \{1, \ldots, n\}$, we can compute $[\boldsymbol{\Delta}_i] \in I$ 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

Taylor models for outer-approximated flowpipes of ODEs (Berz & Makino)

For uncertain dynamical system $\dot{z}(t) = f(z),\ z(t_0) \in [z_0]$ 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 the $i-1$th Lie derivative of f along vector field f: defined inductively as follows (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 needs 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 $[z_{j+1}] = [z](t_{j+1}, t_j, [z_j])$

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 $\left\{ \frac{\partial z}{\partial z_{0,i}}(t, z_0),\ z_0 \in \text{pro } [z_0] \right\} \subseteq [J_i]$: Taylor models

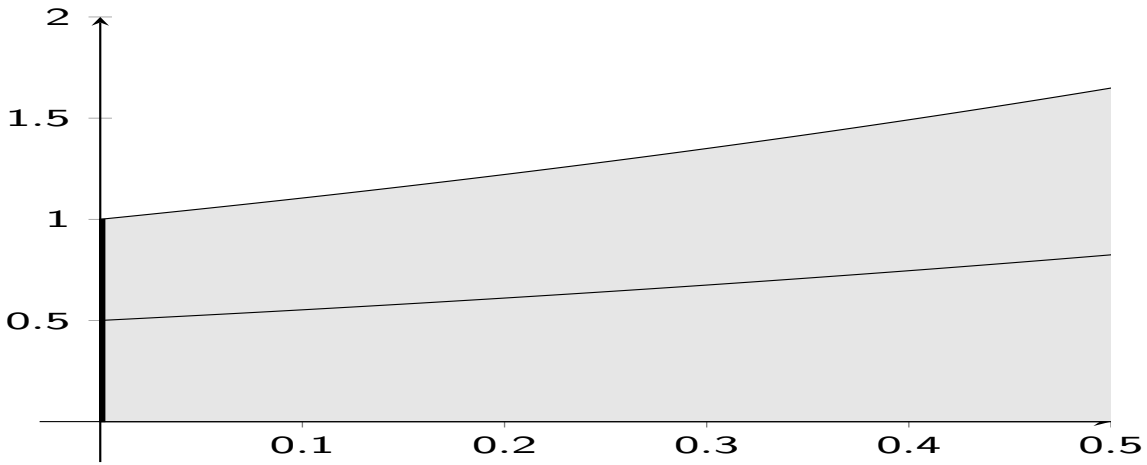
Algorithm (Init: $j = 0$, $t_j = t_0$, $[z_j] = [z_0]$, $[\tilde{z}_j] = \tilde{z}_0 \in [z_0]$, $[J_j] = Id$)

- 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

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

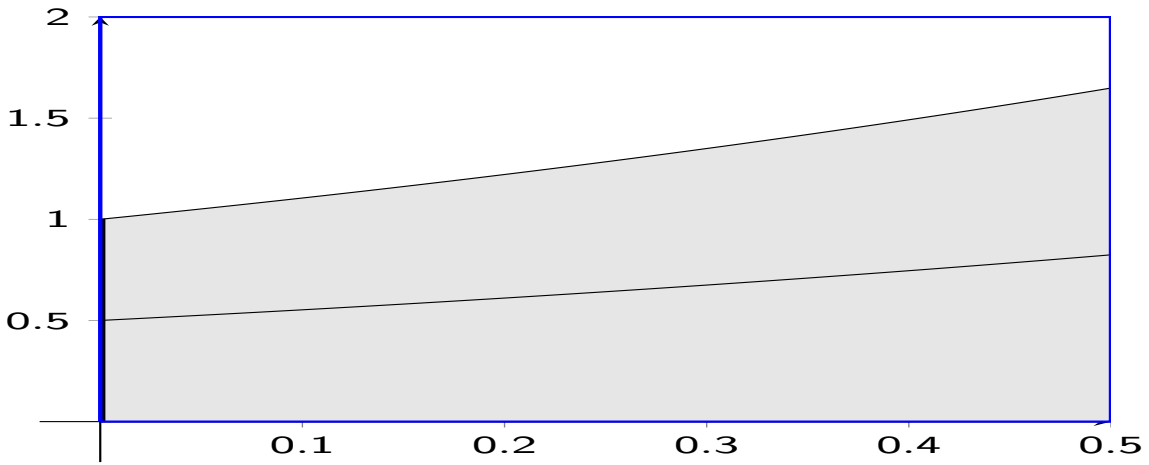
  is an improper interval, then pro $]z[(t, t_j)$ is an inner-approximation of the set of solutions $\{z(t, z_0),\ z_0(t_0) \in z_0\}$, otherwise the inner-approximation is empty.
- $[z_{j+1}] = [z](t_{j+1}, t_j, [z_j])$, $[\tilde{z}_{j+1}] = [\tilde{z}](t_{j+1}, t_j, [\tilde{z}_j])$, $[J_{j+1}] = [J](t,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

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



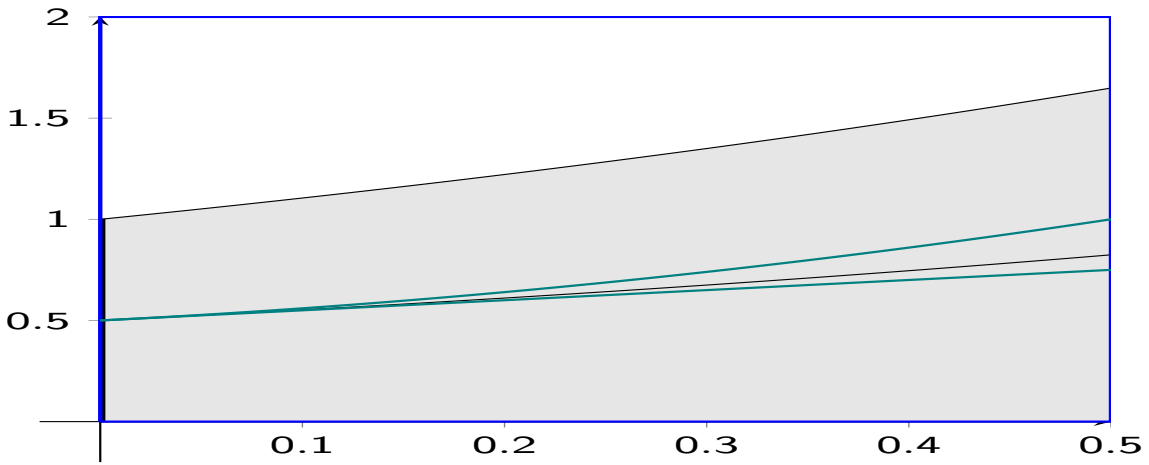
- Init: $[z_0] = [0, 1]$, $\tilde{z}_0 = 0.5$, $[J_0] = 1$

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 $J(t, z_0) \in [1, 2]$

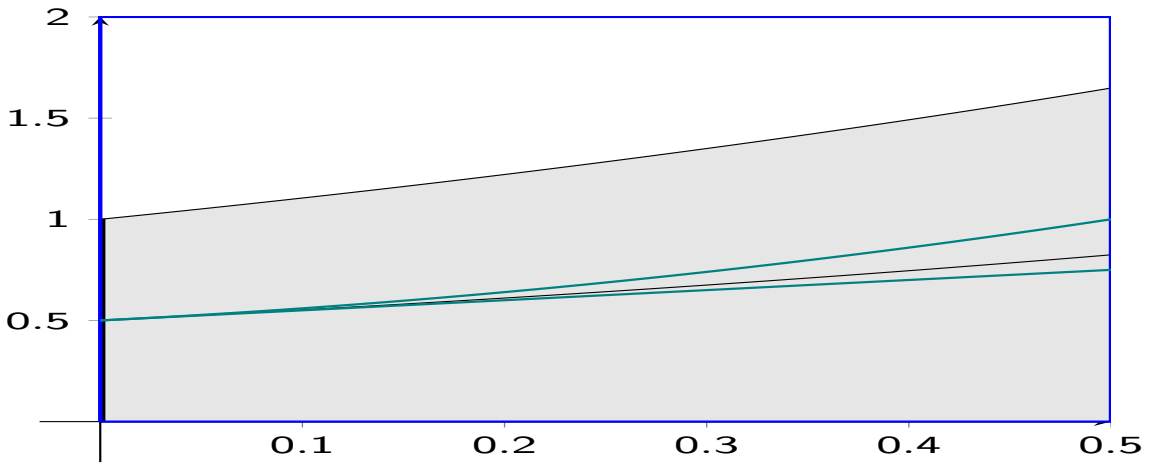
Example: simple ODE $\dot{z} = z$ with $z_0 \in [z_0] = [0, 1]$, on $t \in [0, 0.5]$



- 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:

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

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

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

Mean-value theorem, with $\tilde{z}_0 = \text{mid}([z_0]) = 0.5$ for inner tube:

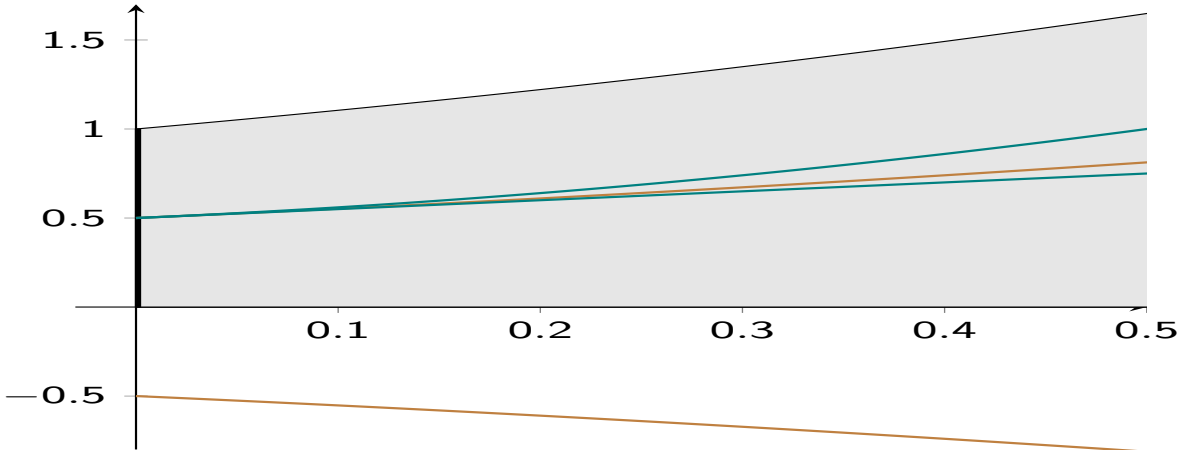
$$
\begin{aligned}
]z[(t,[z_0]) &= [\tilde{z}](t,t_j,[\tilde{z}_j]) + [J](t,t_j,[z_j]) \times ([\overline{z_0},\underline{z_0}] - \tilde{z}_0) \\
&= [\tilde{z}](t,0.5) + [J](t,[z_0]) * ([1,0] - 0.5) \\
&= \underbrace{0.5 + 0.5t + [0,1]t^2}_{\text{proper}} + \underbrace{[(1 + t + [0.5,1]t^2) \times [0.5,-0.5]}_{\text{improper}} = \text{improper?}
\end{aligned}
$$

Mean-value theorem, with $\tilde{z}_0 = \text{mid}([z_0]) = 0.5$ for inner tube:

$$
\begin{aligned}
]z[(t,[z_0]) &= [\tilde{z}](t,t_j,[\tilde{z}_j]) + [J](t,t_j,[z_j]) \times ([\overline{z_0},\underline{z_0}] - \tilde{z}_0) \\
&= [\tilde{z}](t,0.5) + [J](t,[z_0]) * ([1,0] - 0.5) \\
&= \underbrace{0.5 + 0.5t + [0,1]t^2}_{\text{proper}} + \underbrace{[(1 + t + [0.5,1]t^2) \times [0.5,-0.5]}_{\text{improper}} = \text{improper?} \\
&= [0.5 + 0.5t, 0.5 + 0.5t + t^2] + \underbrace{[1 + t + 0.5t^2, 1 + t + t^2]}_{\in \mathcal{P}} \times \underbrace{[0.5,-0.5]}_{\in \text{dual } \mathcal{Z}}
\end{aligned}
$$

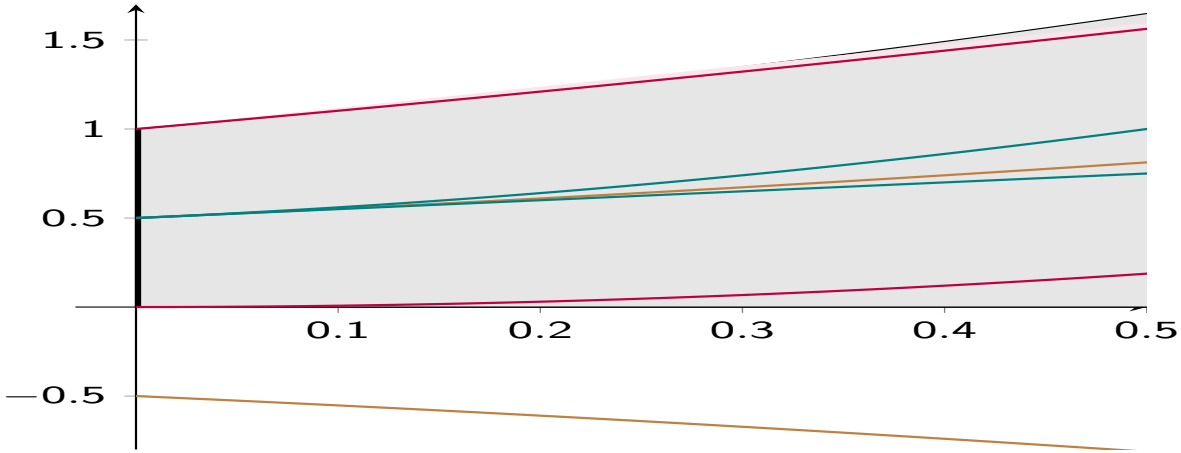
Mean-value theorem, with $\tilde{z}_0 = \text{mid}([z_0]) = 0.5$ for inner tube:

$$
\begin{aligned}
]z[(t,[z_0]) &= [\tilde{z}](t,t_j,[\tilde{z}_j]) + [J](t,t_j,[z_j]) \times ([\overline{z_0},\underline{z_0}] - \tilde{z}_0) \\
&= [\tilde{z}](t,0.5) + [J](t,[z_0]) * ([1,0] - 0.5) \\
&= \underbrace{0.5 + 0.5t + [0,1]t^2}_{\text{proper}} + \underbrace{[(1 + t + [0.5,1]t^2) \times [0.5,-0.5]}_{\text{improper}} = \text{improper?} \\
&= [0.5 + 0.5t, 0.5 + 0.5t + t^2] + \underbrace{[1 + t + 0.5t^2, 1 + t + t^2]}_{\in \mathcal{P}} \times \underbrace{[0.5,-0.5]}_{\in \text{dual } \mathcal{Z}} \\
&= \underbrace{[0.5 + 0.5t, 0.5 + 0.5t + t^2]}_{\text{proper x1}} + \underbrace{[0.5 + 0.5t + 0.25t^2, -0.5 - 0.5t - 0.25t^2]}_{\text{x2 improper (iff } 0 \notin [J])}
\end{aligned}
$$



Mean-value theorem, with $\tilde{z}_0 = \text{mid}([z_0]) = 0.5$ for inner tube:

$$
\begin{aligned}
]z[(t,[z_0]) &= [\tilde{z}](t,t_j,[\tilde{z}_j]) + [J](t,t_j,[z_j]) \times ([\overline{z_0},\underline{z_0}] - \tilde{z}_0) \\
&= [\tilde{z}](t,0.5) + [J](t,[z_0]) * ([1,0] - 0.5) \\
&= \underbrace{0.5 + 0.5t + [0,1]t^2}_{\text{proper}} + \underbrace{[(1 + t + [0.5,1]t^2) \times [0.5,-0.5]}_{\text{improper}} = \text{improper?} \\
&= [0.5 + 0.5t, 0.5 + 0.5t + t^2] + \underbrace{[1 + t + 0.5t^2, 1 + t + t^2]}_{\in \mathcal{P}} \times \underbrace{[0.5,-0.5]}_{\in \text{dual } \mathcal{Z}} \\
&= \underbrace{[0.5 + 0.5t, 0.5 + 0.5t + t^2]}_{\text{proper x1}} + \underbrace{[0.5 + 0.5t + 0.25t^2, -0.5 - 0.5t - 0.25t^2]}_{\text{x2 improper (iff } 0 \notin [J])} \\
&= [1 + t + 0.25t^2, 0.75t^2] \text{ is improper! (width }]z[= \text{width x2 - width x1)}
\end{aligned}
$$



Implementation and experiments

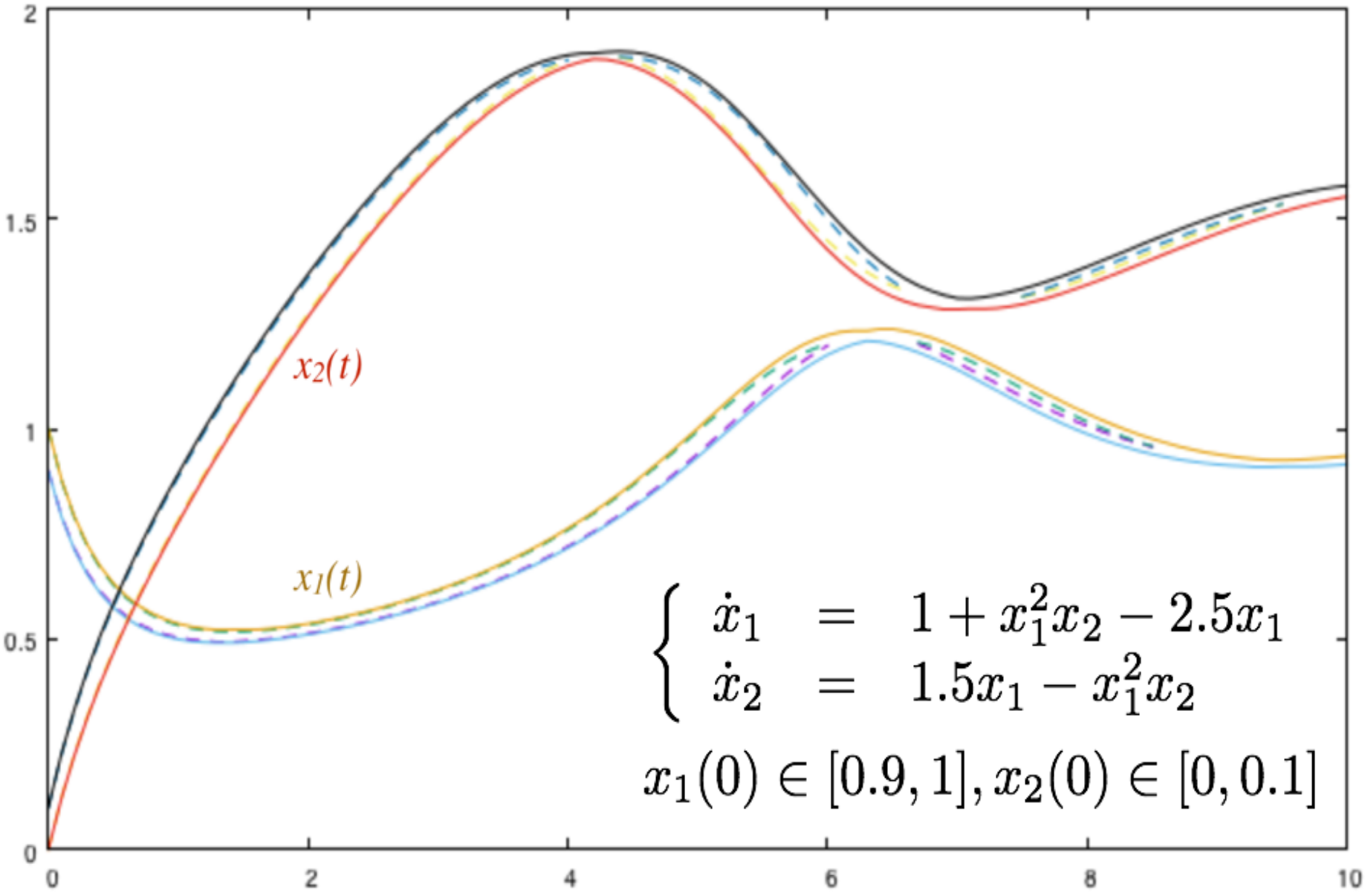
First prototype implementation in C++ (fixed stepsize, etc)

- relying on external packages (FILIB++ for intervals, FADBAD++ for automatic differentiation, aaflib for affine arithmetic)
- repeatibility package available from `http://www.lix.polytechnique.fr/Labo/Sylvie.Putot/software.html`
- the library should evolve in the future (hybrid systems, property verification)

Comparison to the related work

- Chen, Sankaranarayanan, and Abraham, *Under-approximate flowpipes for non-linear continuous systems* [FMCAD'14]
- Xue, She, and Easwaran, *Under-approx. backward reachable sets by polytopes* [CAV'16]
- Our method is forward whereas the above are rather backward, and involve some constraint solving
- We study the range of each variable separately (but we can also characterize joint ranges, simply relying on the outer-approximated Jacobian)
- Fair comparison is not easy

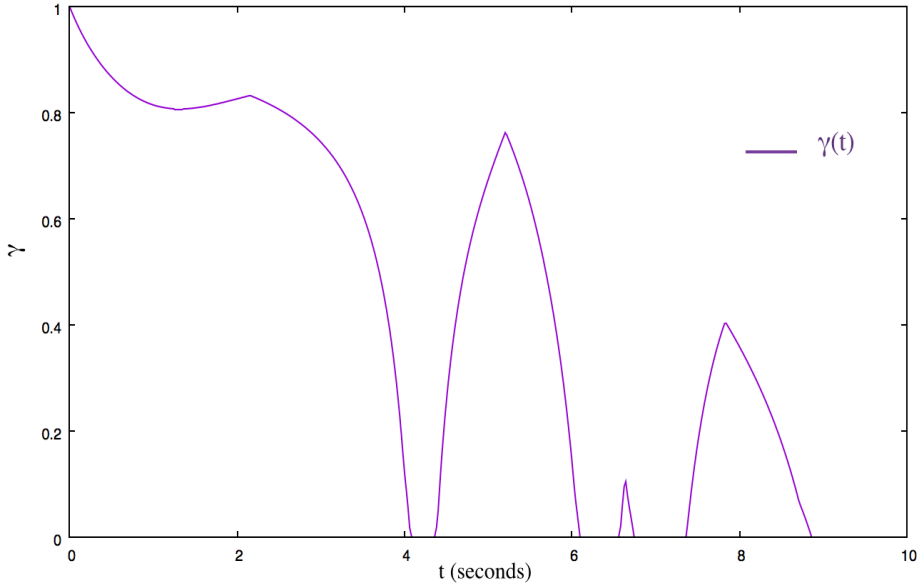
Brusselator example: inner and outer reachable sets (Taylor Models order 4)

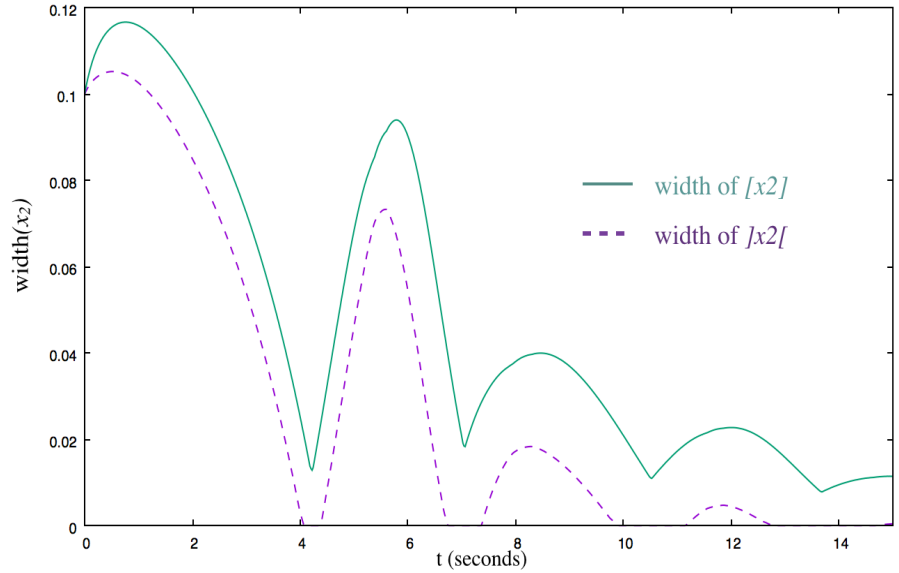


Comparison to Chen, Sankaranarayanan, and Abraham, *Under-approximate flowpipes for non-linear continuous systems* [FMCAD'14]

compare quality measure $\gamma_{\min} = \min \frac{\gamma_u(v)}{\gamma_o(v)}, v \in V$ a set of vectors (the axes here)

where $\gamma_u(v)$ and $\gamma_o(v)$ are the width of the inner/outer-approximation in direction $v \in V$.

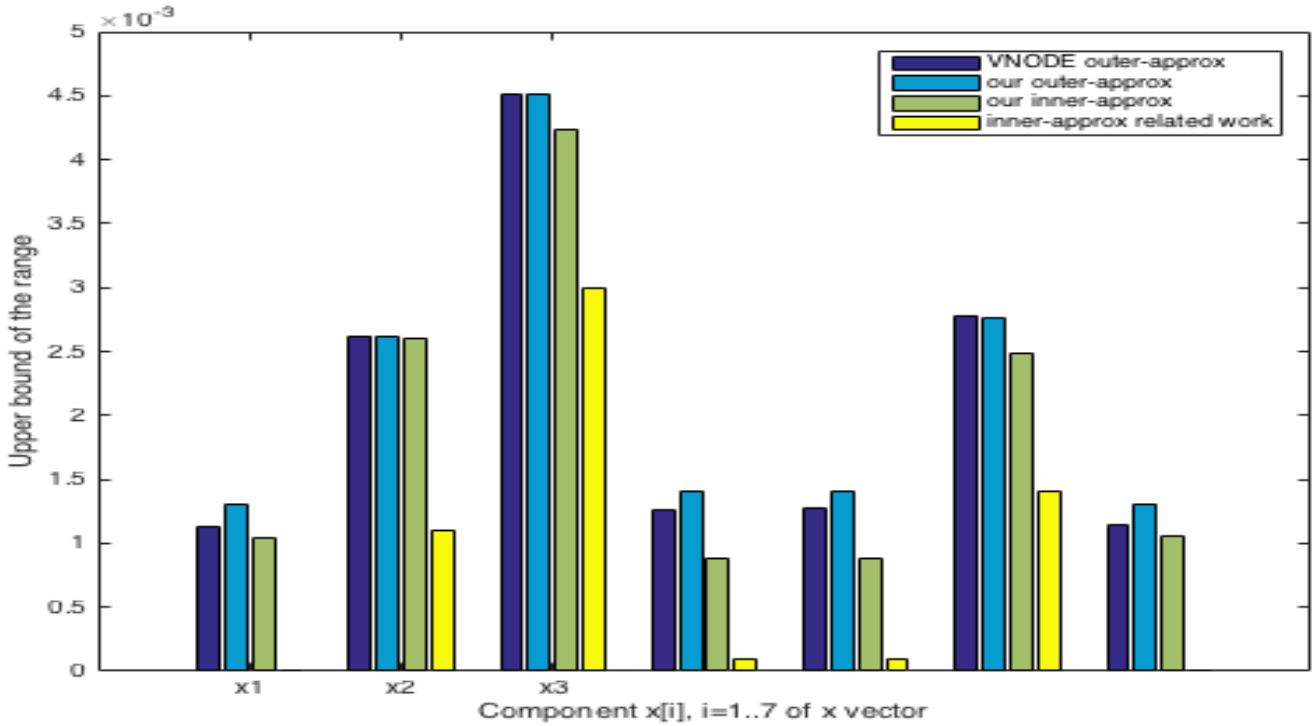




	Brusselator (dim 2, order 4 TM, step h=0.02)			Biological (dim 7, order 5, h=0.01)	
	time (sec)	$\gamma_{\min}(t=3)$	$\gamma_{\min}(t=4)$	time(sec)	$\gamma_{\min}(t=0.2)$
FMCAD	89	0.7	0.55	632	0.25
HSCC'17	3.2 (0.25 if h=0.1)	0.7	0.1	4.7	0.65

Comparison (on the biological system) to Xue, She, and Easwaran, *Under-approximating backward reachable sets by polytopes* [CAV'16]

Comparing upper bounds on inner and outer-approximations on the 7 variables:



Comparing quality measure γ on each of the 7 variables:

	time (sec)	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7
CAV'16	0.67	0.85	0.86	0.22	0.84	0.84	0.85	0.85
HSCC'17	0.2	0.970	0.999	0.973	0.938	0.938	0.970	0.971

Conclusion and future work

A simple and efficient (linear in the size of the Jacobian with respect to outer-approximated Taylor models) computation of inner tubes for continuous systems:

- The method extends quite naturally to hybrid systems, as it relies only on outer-approximations of the flow and its Jacobian with respect to initial conditions (the accuracy still remains to be experimented...)
- In our implementation, the Taylor Models are evaluated with affine arithmetic
  - prevents wrapping effect: only the inner-approximation relies on a pure Kaucher interval evaluation, and it is not propagated
  - allows in the future parameter synthesis: a noise symbol is associated to each uncertain input or parameter, which gives parametric models
- Towards property proof/falsification and parameter synthesis for hybrid systems