Robust under-approximations and application to reachability of non-linear control systems with disturbances

Eric Goubault, Sylvie Putot

Cosynus, LIX, Ecole Polytechnique, CNRS, IP-Paris

International Online Seminar on Interval Methods in Control Engineering

Table of Contents

Table of Contents

Reachability-based verification

Safety verification, temporal properties

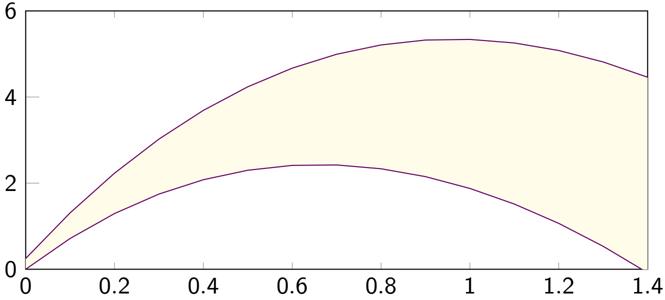
- Compute (outer) enveloppes of all possible trajectories (not possible to compute exact envelopes)
- If these enveloppes do not intersect with sets of unsafe states, then the system is safe
- Compute inner enveloppes, for applications to additional temporal properties (e.g. reach-avoid)

This talk: focus on robust reachability analysis for uncertain non-linear discrete dynamical systems and ODEs

- Robust reachability: what states can control systems reach, for some class of disturbance and for some class of control?
- How to compute precisely and efficiently inner and outer approximations of these robust reachable sets?
- Applications: using these envelopes for the verification of control systems

Inner and outer approximations of reachable sets for uncertain dynamical systems

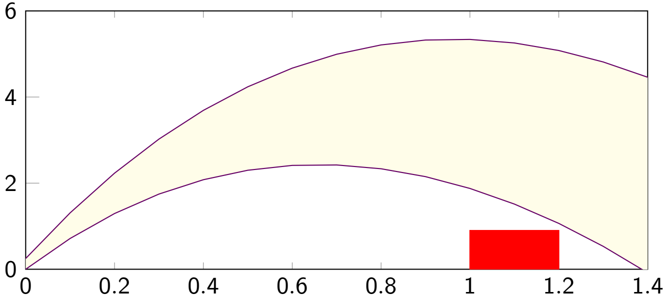
- Outer or over-approximating (maximal) flowpipes = guaranteed to include all reachable states



See e.g. Eric Goubault and Sylvie Putot, Inner and Outer Reachability for the Analysis of Control Systems, HSCC 2019

Inner and outer approximations of reachable sets for uncertain dynamical systems

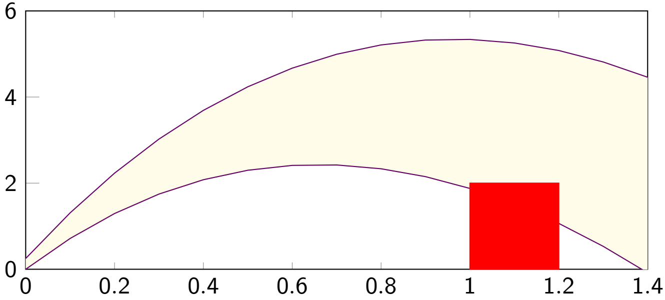
- Outer or over-approximating (maximal) flowpipes = guaranteed to include all reachable states
  - provide safety proof



See e.g. Eric Goubault and Sylvie Putot, Inner and Outer Reachability for the Analysis of Control Systems, HSCC 2019

Inner and outer approximations of reachable sets for uncertain dynamical systems

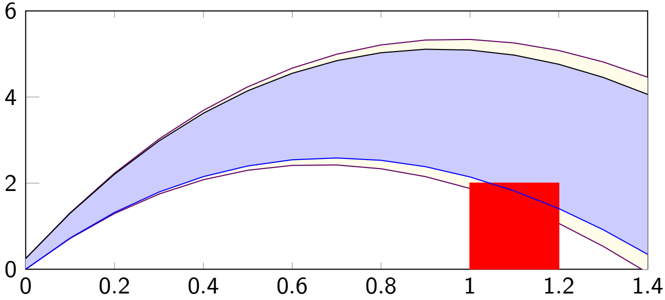
- Outer or over-approximating (maximal) flowpipes = guaranteed to include all reachable states
  - provide safety proof but conservative ("false alarms")



See e.g. Eric Goubault and Sylvie Putot, Inner and Outer Reachability for the Analysis of Control Systems, HSCC 2019

Inner and outer approximations of reachable sets for uncertain dynamical systems

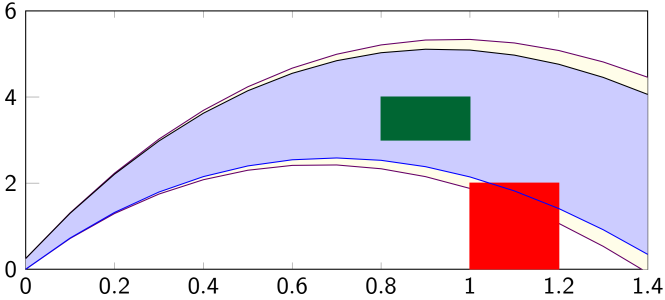
- Outer or over-approximating (maximal) flowpipes = guaranteed to include all reachable states
  - provide safety proof but conservative ("false alarms")
- Inner or under-approximating (maximal) flowpipes = states guaranteed to be reached
  - falsification of safety properties, precision estimates



See e.g. Eric Goubault and Sylvie Putot, Inner and Outer Reachability for the Analysis of Control Systems, HSCC 2019

Inner and outer approximations of reachable sets for uncertain dynamical systems

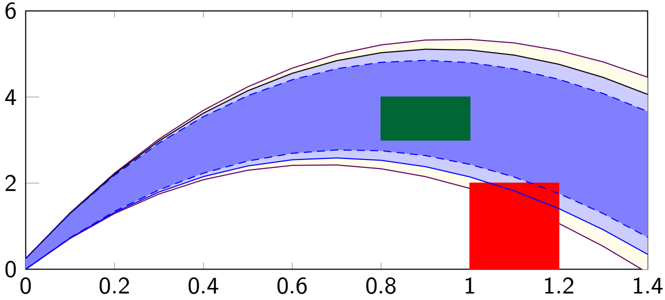
- Outer or over-approximating (maximal) flowpipes = guaranteed to include all reachable states
  - provide safety proof but conservative ("false alarms")
- Inner or under-approximating (maximal) flowpipes = states guaranteed to be reached
  - falsification of safety properties, precision estimates
 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



See e.g. Eric Goubault and Sylvie Putot, Inner and Outer Reachability for the Analysis of Control Systems, HSCC 2019

Inner and outer approximations of reachable sets for uncertain dynamical systems

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

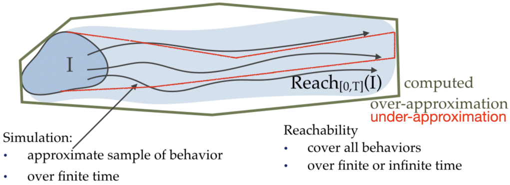


See e.g. Eric Goubault and Sylvie Putot, Inner and Outer Reachability for the Analysis of Control Systems, HSCC 2019

Reachable sets of continuous (and hybrid) dynamics

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

under classical hypotheses, solutions (flows) $\varphi^f(s; x_0, u)$



Robust (forward) reachability

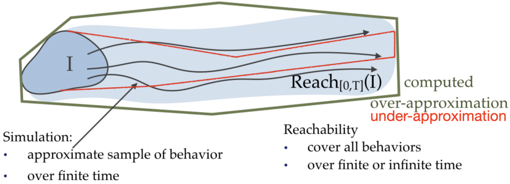
States that trajectories will reach whatever some components u_A of the input signal is, and for some other components u_E of the input signal

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

Reachable sets of continuous (and hybrid) dynamics

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

under classical hypotheses, solutions (flows) $\varphi^f(s; x_0, u)$



Robust (forward) 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

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

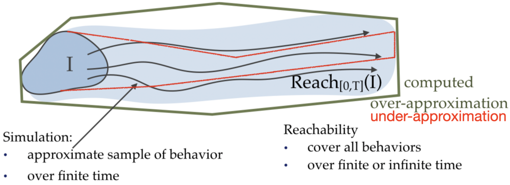
Think of non controllable disturbances for u_A, and controls for u_E; classical maximal reachability is for $\mathbb{U}_{\mathbb{A}} = \emptyset$, minimal reachability is for $\mathbb{U}_{\mathbb{E}} = \emptyset$ as defined in e.g.

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

Reachable sets of continuous (and hybrid) dynamics

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

under classical hypotheses, solutions (flows) $\varphi^f(s; x_0, u)$



Robust (forward) 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

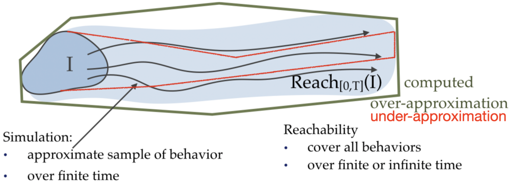
$$R^f_{\mathcal{AE}}(t; \boldsymbol{Z}_0, \mathbb{U}) = \{z \in \mathcal{D} \,|\, \forall u_A \in \mathbb{U}_{\mathbb{A}}, \exists u_E \in \mathbb{U}_{\mathbb{E}}, \exists z_0 \in \boldsymbol{Z}_0,\ z = \varphi^f(t; z_0, u_A, u_E)\}$$

We cover also time-dependent inputs - control - and disturbances ; other notion of robustness is $\exists u_E,\ \forall u_A$ is ongoing work

Reachable sets of continuous (and hybrid) dynamics

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

under classical hypotheses, solutions (flows) $\varphi^f(s; x_0, u)$



Robust (forward) 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

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

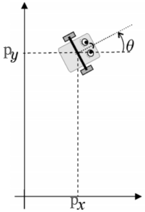
These reachable sets are not computable in general: we compute inner and outer approximations precisely and efficiently

A simple example (Eric Goubault, Sylvie Putot: Robust Under-Approximations and Application to Reachability of Non-Linear Control Systems With Disturbances. IEEE Control. Syst. Lett. 4(4), 2020)

Dubbins vehicle

Its position (p_x, p_y) and its heading θ are given by:

$$\begin{pmatrix} \dot{p}_x \\ \dot{p}_y \\ \dot{\theta} \end{pmatrix} = \begin{pmatrix} vcos(\theta) + b_1 \\ vsin(\theta) + b_2 \\ a + b_3 \end{pmatrix}$$



where a is the (angular) control, and $b = (b_1, b_2, b_3)$ is the disturbance. ($v = 5$, $a \in [-1, 1]$, $-1 \leq b_1 \leq 1$, $-1 \leq b_2 \leq 1$, $-5 \leq b_3 \leq 5$).

Backward reachable set (BRS)

$$\mathcal{G}(t) = \{x_0 | \forall u_{\mathcal{A}}, \exists u_{\mathcal{E}}, \exists x \in \mathcal{G}_0, x = \varphi^f(t; x_0, u))\} \text{ from}$$

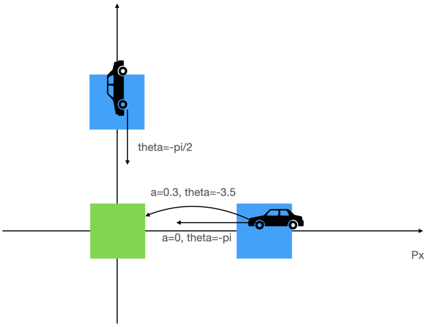
$$\mathcal{G}_0 = \{(p_x, p_y, \theta) || p_x| \leq 0.5, |p_y| \leq 0.5, \; 0 \leq \theta \leq 2\pi\}$$

We compute BRS as forward reachability (FRS) for the inverse flow:

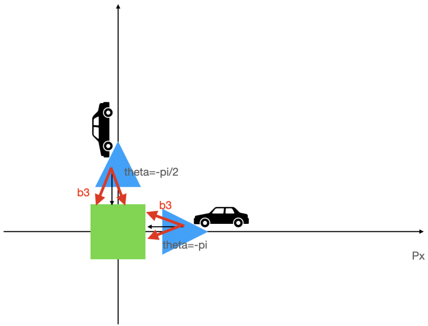
$$\{x_0 | \forall u_{\mathcal{A}}, \exists u_{\mathcal{E}}, \exists x \in \mathcal{G}_0, x_0 = \varphi^{-f}(t; x, u))\}$$

Dubbins vehicle

What happens



Without disturbance

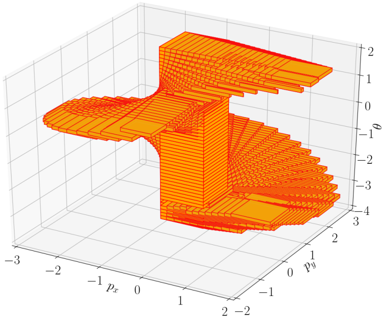


With disturbance

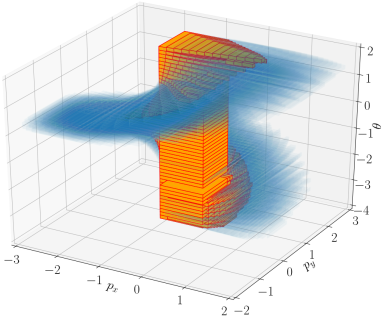
Robust approximation of BRS for the Dubbins vehicle

Union of BRS for $t \leq 0.5s$

(2 seconds, Taylor order 3, time horizon 0.5 s, step size 0.025 s, 50 subdivisions on heading θ, constant controls)



Maximal inner with no disturbance

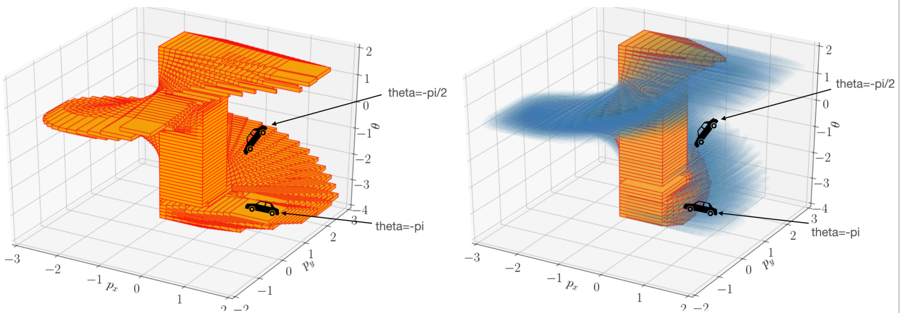


Robust inner (with disturbances), maximal inner (with disturbances)

Joint p_x, p_y and θ for Dubbins, constant controls (results, also obtained in 2 seconds)

Robust approximation of BRS for the Dubbins vehicle

Union of BRS for $t \leq 0.5s$



Maximal inner with no disturbance

Robust inner (with disturbances), maximal inner (with disturbances)

Joint p_x, p_y and θ for Dubbins, constant controls (results, also obtained in 2 seconds)

Very precise results comparable to e.g. Decomposition of Reachable Sets and Tubes for a Class of Nonlinear Systems, M. Chen, S. L. Herbert, M. S. Vashishtha, S. Bansal and C. J. Tomlin, IEEE Trans. Aut. Control, 2018

Table of Contents

Ingredients

- compute robust inner and outer approximations of 1-D function range (mean-value theorem)
- robust version (robust mean-value theorem) can also be used to produce n-D inner-approximations
- Can be applied to discrete dynamical systems
- Can be applied on the flow map for a continuous system
  - for this, we need to outer-approximate both the flow map and its Jacobian wrt control, initial states and disturbances (here, using Taylor models)
  - Robust mean value theorem that produce inner and outer approximations of flowpipes using trajectory and Jacobian approximants
- Improvements using subdivisions and skewing

Inner-approximation and mean-value theorems

Generalized interval mean-value theorem

- $f : \mathbb{R}^m \to \mathbb{R}$ be a continuously differentiable function, $\boldsymbol{x} \in \boldsymbol{I}^m$
- $\boldsymbol{f}_0 = [\underline{f_0}, \overline{f_0}]$, inclusion of $f(c(\boldsymbol{x}))$
- $\Delta_i = [\underline{\Delta_i}, \overline{\Delta_i}]$ such that $\{|f_i'(c(\boldsymbol{x}_1), \ldots, c(\boldsymbol{x}_{i-1}), x_i, \ldots, x_m)|, x \in \boldsymbol{x}\} \subseteq \Delta_i$

Then:

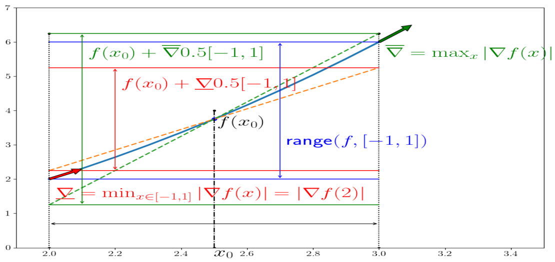
$$\text{range}(f, \boldsymbol{x}) \subseteq [\underline{f_0}, \overline{f_0}] + \sum_{i=1}^{m} \overline{\Delta_i} r(\boldsymbol{x}_i)[-1, 1]$$

$$[\overline{f_0} - \sum_{i=1}^{m} \underline{\Delta_i} r(\boldsymbol{x}_i), \underline{f_0} + \sum_{i=1}^{m} \underline{\Delta_i} r(\boldsymbol{x}_i)] \subseteq \text{range}(f, \boldsymbol{x})$$

A. Goldsztejn, "Modal intervals revisited, part 2: A generalized interval mean value extension," Reliable Computing, vol. 16, 2012.

Inner-approximation and mean-value theorems

An illustrative example $f(x) = x^2 - x$ over $\boldsymbol{x} = [2, 3]$



$f(2.5) = 3.75$ and $\boldsymbol{\nabla f}([2,3]) \subseteq [3,5]$. Then,

$$3.75 + 1.5[-1,1] \subseteq \text{range}(f, [2,3]) \subseteq 3.75 + 2.5[-1,1],$$

from which we deduce

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

Robust mean value

Consider now: $f(w,u) = u^2 - 2w$ for $(w,u) \in [2,3] \times [2,3]$

w is a disturbance, we want to compute the robust range:

$$\{z \mid \forall w \in [2,3],\ \exists u \in [2,3], z = f(w,u)\}$$

Principle

- Disturbances act as an adversary: shrinks down the outer (resp. inner) approximation by $\langle \underline{\nabla}_w, r(\boldsymbol{x}_{\mathcal{A}}\rangle)[-1,1]$ (resp. by $\langle \overline{\nabla}_w, r(\boldsymbol{x}_{\mathcal{A}}\rangle)[-1,1]$)
- Controls act positively on the range: widens the outer (resp. inner) approximation by $\langle \overline{\nabla}_u, r(\boldsymbol{x}_{\mathcal{E}}\rangle)[-1,1]$ (resp. $\langle \underline{\nabla}_u, r(\boldsymbol{x}_{\mathcal{E}}\rangle)[-1,1]$)
- See Theorem 2 of Eric Goubault, Sylvie Putot: Robust Under-Approximations and Application to Reachability of Non-Linear Control Systems With Disturbances. IEEE Control. Syst. Lett. 4(4), 2020

Calculation

$f(2.5, 2.5) = 1.25$ and $\nabla f(\boldsymbol{x}) \subseteq ([-2,-2],[4,6])$, so:

$$[1.25 - 2 + 1, 1.25 + 2 - 1] \subseteq \text{range}(f, \boldsymbol{x}, 1, 2) \subseteq [1.25 - 3 + 1, 1.25 + 3 - 1]$$

$$i.e.\ [0.25, 2.25] \subseteq \text{range}(f, \boldsymbol{x}, 1, 2) \subseteq [-0.75, 3.25]$$

Robust mean-value, more formally

Similar to the generalized interval mean-value theorem, but with adversarial terms

- $f : \mathbb{R}^m \to \mathbb{R}$ be continuously differentiable, $\boldsymbol{x} = \boldsymbol{x}_{\mathcal{A}} \times \boldsymbol{x}_{\mathcal{E}} \in \boldsymbol{I}^m$
- $\boldsymbol{f}^0$ such that $f(c(\boldsymbol{x})) \subseteq \boldsymbol{f}^0$
- $\boldsymbol{\nabla}_w$ and $\boldsymbol{\nabla}_u$ such that $\{|\nabla_w f(w, c(\boldsymbol{x}_{\mathcal{E}}))|, w \in \boldsymbol{x}_{\mathcal{A}}\} \subseteq \boldsymbol{\nabla}_w$ and $\{|\nabla_u f(w,u)|, w \in \boldsymbol{x}_{\mathcal{A}}, u \in \boldsymbol{x}_{\mathcal{E}}\} \subseteq \boldsymbol{\nabla}_u$

$$\text{range}(f, \boldsymbol{x}, I_{\mathcal{A}}, I_{\mathcal{E}}) \subseteq [\underline{f^0} - \langle \overline{\nabla}_u, r(\boldsymbol{x}_{\mathcal{E}})\rangle + \langle \underline{\nabla}_w, r(\boldsymbol{x}_{\mathcal{A}})\rangle, \overline{f^0} + \langle \overline{\nabla}_u, r(\boldsymbol{x}_{\mathcal{E}})\rangle - \langle \underline{\nabla}_w, r(\boldsymbol{x}_{\mathcal{A}})\rangle]$$

$$[\overline{f^0} - \langle \underline{\nabla}_u, r(\boldsymbol{x}_{\mathcal{E}})\rangle + \langle \overline{\nabla}_w, r(\boldsymbol{x}_{\mathcal{A}})\rangle, \underline{f^0} + \langle \underline{\nabla}_u, r(\boldsymbol{x}_{\mathcal{E}})\rangle - \langle \overline{\nabla}_w, r(\boldsymbol{x}_{\mathcal{A}})\rangle] \subseteq \text{range}(f, \boldsymbol{x}, I_{\mathcal{A}}, I_{\mathcal{E}})$$

See e.g. Eric Goubault and Sylvie Putot, Inner and Outer Reachability for the Analysis of Control Systems, HSCC 2019

Use of robust mean-value for n-D inner-approximations

Products of 1-D outer-approximations are n-D outer-approximations, but this is not the case for inner-approximations!

For instance suppose:

$$\forall z_1 \in \boldsymbol{z}_1, \exists x_1 \in \boldsymbol{x}_1,\ \exists x_2 \in \boldsymbol{x}_2,\ z_1 = f_1(x)$$
$$\forall z_2 \in \boldsymbol{z}_2, \exists x_1 \in \boldsymbol{x}_1,\ \exists x_2 \in \boldsymbol{x}_2,\ z_2 = f_2(x)$$

This does not imply $\forall z_1 \in \boldsymbol{z}_1$ and $\forall z_2 \in \boldsymbol{z}_2$ there exists x_1 and x_2 such that $z = f(x)$.

Use of robust mean-value for n-D inner-approximations

A solution (particular case - can be generalized to n-D)

Compute 1-D inner range $\boldsymbol{z}_1$ of f_1 robust to x_1 and 1-D inner range $\boldsymbol{z}_2$ of f_2 robust to x_2:

$$\forall z_1 \in \boldsymbol{z}_1, \forall x_1 \in \boldsymbol{x}_1, \exists x_2 \in \boldsymbol{x}_2, \; z_1 = f_1(x)$$
$$\forall z_2 \in \boldsymbol{z}_2, \forall x_2 \in \boldsymbol{x}_2, \exists x_1 \in \boldsymbol{x}_1, \; z_2 = f_2(x)$$

Then

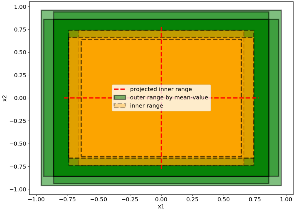
$$\boldsymbol{z}_1 \times \boldsymbol{z}_2 \subseteq range(f, \boldsymbol{x}_1 \times \boldsymbol{x}_2)$$

with continuous selections x_2 and x_1. (case of Goldsztejn "elementary functions")

Example in 2-D:

$$f(x) = (5x_1^2 + x_2^2 - 2x_1x_2 - 4, x_1^2 + 5x_2^2 - 2x_1x_2 - 4)^{\intercal}$$

with $\boldsymbol{x} = [0.9, 1.1]^2$



$$[-0.66, 0.66] \times [-0.66, 0.66] \subseteq \text{range}(f, x) \subseteq [-0.94, 0.94] \times [-0.94, 0.94]$$

This result can be generalized to functions $f \; : \mathbb{R}^m \to \mathbb{R}^n$

Example in 2-D

$f(x) = (5x_1^2 + x_2^2 - 2x_1x_2 - 4, x_1^2 + 5x_2^2 - 2x_1x_2 - 4)^\intercal$ with $\boldsymbol{x} = [0.9, 1.1]^2$

- $f(1,1) = 0$, $\nabla f(\boldsymbol{x}) \subseteq (([6.8, 9.2], [-0.4, 0.4])^\intercal, ([-0.4, 0.4], [6.8, 9.2])^\intercal)$.
- Thus $\text{range}(f, \boldsymbol{x}) \subseteq [-0.96, 0.96]^2$ by the mean-value theorem.

1-D inner-approximation

$$[-0.7, 0.7] \subseteq \text{range}(f_1, x)$$
$$[-0.68, 0.68] \subseteq \text{range}(f_2, x)$$

2-D inner-approximation

- We obtain $[-0.64, 0.64]^2 \subseteq \text{range}(f, \boldsymbol{x})$ interpreting
  $\forall z_1 \in \boldsymbol{z}_1, \forall x_2 \in \boldsymbol{x}_2, \exists x_1 \in \boldsymbol{x}_1, z_1 = f(\boldsymbol{x})$
  $\forall z_2 \in \boldsymbol{z}_2, \forall x_1 \in \boldsymbol{x}_1, \exists x_2 \in \boldsymbol{x}_2, z_2 = f(\boldsymbol{x})$
- E.g. $f_1(1,1) + [-0.68 + 0.4 * 0.1, 0.68 - 0.4 * 0.1] = [-0.64, 0.64] \subseteq \text{range}(f_1, \boldsymbol{x}, 2)$.

New AE extensions

Base theorem

Suppose an approximation function g for f, elementary function s.t.:

$$\forall w \in \mathrm{x}_{\mathcal{A}},\ \forall u \in \mathrm{x}_{\mathcal{E}},\ \exists \xi \in \mathrm{x},\ f(w,u) = g(w,u,\xi)$$

Then any under-approx (resp. over-approx) of robust range of g with respect to $x_{\mathcal{A}}$ and ξ, $\mathcal{I}_g \subseteq \mathrm{range}(g, \mathrm{x} \times \mathrm{x}, I_{\mathcal{A}} \cup \{m+1,\ldots,2m\}, I_{\mathcal{E}})$ is under-approx (resp. over-approx) of robust range of f with respect to $x_{\mathcal{A}}$, i.e.

$$\mathcal{I}_g \subseteq \mathrm{range}(f, \mathrm{x}, I_{\mathcal{A}}, I_{\mathcal{E}})$$

(resp. $\mathrm{range}(f, \mathrm{x}, I_{\mathcal{A}}, I_{\mathcal{E}}) \subseteq \mathcal{O}_g$)

Typically

$g(w,u,\xi)$ is the Taylor expansion of f ($x = (w,u)$, ξ accounting for the Lagrange remainder):

$$g(x,\xi) = f(x^0) + \sum_{i=1}^{n} \frac{(x-x^0)^i}{i!} D^i f(x^0) + D^{n+1} f(\xi) \frac{(x-x^0)^{n+1}}{(n+1)!}$$

New AE extensions

Furthermore

- Let g be an elementary function $g(w,u,\xi) = \alpha(w,u) + \beta(w,u,\xi)$ over $x = (w,u) \in \mathrm{x} \subseteq \boldsymbol{I}^m$ and $\xi \in \mathrm{x}$.
- $\mathcal{I}_\alpha$ under-approximation of robust range of α with respect to w, $\mathcal{O}_\beta$ over-approximation of range of β

The robust range of g with respect to $w \in \mathrm{x}_{\mathcal{A}}$ and $\xi \in \mathrm{x}$ is under-approximated by

$$\mathcal{I}_g = [\underline{\mathcal{I}}_\alpha + \overline{\mathcal{O}}_\beta, \overline{\mathcal{I}}_\alpha + \underline{\mathcal{O}}_\beta]$$

Typically again

$g(w,u,\xi)$ is the Taylor expansion of f ($x = (w,u)$, ξ accounting for the Lagrange remainder):

$$g(x,\xi) = f(x^0) + \sum_{i=1}^{n} \frac{(x-x^0)^i}{i!} D^i f(x^0) + D^{n+1} f(\xi) \frac{(x-x^0)^{n+1}}{(n+1)!}$$

$$= f(x^0) + \sum_{i=1}^{n} \frac{(x-x^0)^i}{i!} D^i f(x^0) + \beta(x,\xi) = \alpha(x) + \beta(x,\xi)$$

Application and Example

Application to Taylor Models

- f continuously $(n+1)$-differentiable f, approximant:

$$g(x,\xi) = f(x^0) + \sum_{i=1}^{n} \frac{(x-x^0)^i}{i!} D^i f(x^0) + D^{n+1} f(\xi) \frac{(x-x^0)^{n+1}}{(n+1)!}$$
$$= f(x^0) + \sum_{i=1}^{n} \frac{(x-x^0)^i}{i!} D^i f(x^0) + \beta(x,\xi)$$

- Easily applicable for $n = 1$

Example: $f(x) = x^3 + x^2 + x + 1$ on $[-\frac{1}{4}, \frac{1}{4}]$

- Exact range is: $[0.796875, 1.328125]$.
- $f^{(1)}(x) = 3x^2 + 2x + 1$, $f^{(2)}(x) = 6x + 2$ and $g(x,\xi) = 1 + x + x^2(3\xi + 1)$.
- The under approximation of $1 + x$ over $[-\frac{1}{4}, \frac{1}{4}]$ is $[\frac{3}{4}, \frac{5}{4}]$
- $[0, \frac{1}{16}][\frac{1}{4}, \frac{7}{4}] = [0, \frac{7}{64}]$ is over approximation of $x^2(3\xi + 1)$ for x, ξ in $[-\frac{1}{4}, \frac{1}{4}]$
- $[0.859375, 1.25] \subseteq \text{range}(f, \boldsymbol{x})$
- Compare with previous mean-value AE extension method: $[0.875, 1.125]$.

Skewing

In general: compute a skewed box as under-approximation instead of a box

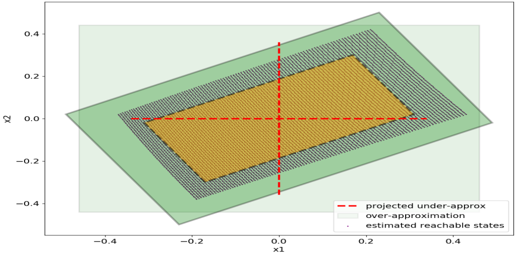
- Let $C \in \mathbb{R}^{n \times n}$ be a non-singular matrix
- If $\boldsymbol{z} \subseteq \text{range}(Cf, \boldsymbol{x})$:

$$\{C^{-1}z | z \in \boldsymbol{z}\}$$

is in $\text{range}(f, \boldsymbol{x})$ (classical choice: $C = (c(\boldsymbol{\nabla}))^{-1}$).

An example: $f(x) = (2x_1^2 - x_1x_2 - 1, x_1^2 + x_2^2 - 2)^\intercal$, $\boldsymbol{x} = [0.9, 1.1]^2$

Empty inner boxes with mean-value; Non-empty yellow approx with skewing

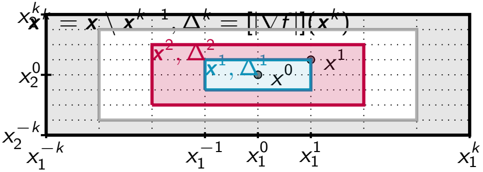


Quadrature

First idea: subdivision

- Partition each dimension $j = [1 \dots m]$ of the m-dimensional input box $\boldsymbol{x} = \boldsymbol{x}_1 \times \dots \times \boldsymbol{x}_m$ in $2k$ sub-intervals
- Define, for all $j = [1 \dots m]$, $x_j^{-k} \leq x_j^{-(k-1)} \leq \dots \leq x_j^0 \leq \dots \leq x_j^k$, with $x_j^{-k} = \underline{\boldsymbol{x}_j}$, $x_j^0 = c(\boldsymbol{x}_j)$, $x_j^k = \overline{\boldsymbol{x}_j}$ ($dx^i = x^i - x^{i-1}$ the vector-valued deviation)
- Compute under-approximation for each sub-box
- But convex union of the under-approximating boxes is in general not an under-approximation of range$(f, \boldsymbol{x})$, and expensive (not linear in k).

Instead: quadrature



Quadrature: example

$f(x) = (2x_1^2 + 2x_2^2 - 2x_1x_2 - 2, x_1^3 - x_2^3 + 4x_1x_2 - 3)^\intercal$, $\boldsymbol{x} = [0.9, 1.1]^2$

- Skewing without partitioning: over-approximation in larger light green, empty inner-approximation
- quadrature formula for mean-value extension ($k = 10$ partitions) and order 2 extension: very similar under-approximating in yellow
- light green box is order 2 over-approximation without preconditioning.

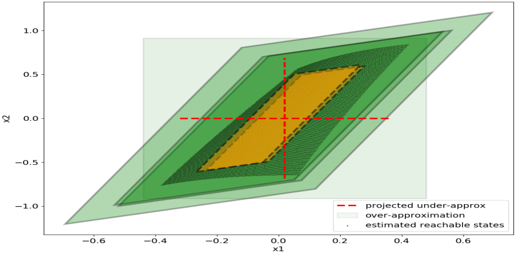


Table of Contents

Application to reachability of discrete systems

Principles

- Based on range estimation
- Two methods:
  - Method 1: propagates under-approximations at each step
  - Method 2: propagates over-approximations of the Jacobian, and deduce under-approximations at each step (could be empty at some step, and non-empty later)

Method 2 more costly (differentiation of iterated functions)

See e.g. Eric Goubault and Sylvie Putot, Tractable higher-order under-approximating AE extensions for non-linear systems, ADHS 2021

Method 1

- Iteratively compute function image, with as input, the previously computed approximations (under and over-approximations I^k and O^k of the reachable set $\boldsymbol{z}^k$):

$$\begin{cases} I^0 = \boldsymbol{z}^0,\ O^0 = \boldsymbol{z}^0 \\ I^{k+1} = \mathcal{I}(f, I^k, \pi),\ O^{k+1} = \mathcal{O}(f, O^k, \pi) \end{cases}$$

Input: $f : \mathbb{R}^n \to \mathbb{R}^n$, $\boldsymbol{z}^0 \subseteq \boldsymbol{I}^n$ initial state, $K \in \boldsymbol{N}^+$, an over-approximating extension $[\nabla f]$
Output: I^k and O^k for $k \in [1, K]$

$I^0 := \boldsymbol{z}^0, O^0 := \boldsymbol{z}^0$; choose $\pi : [1 \ldots n] \mapsto [1 \ldots n]$
for k from 0 to $K-1$ **do**
  $\boldsymbol{\nabla}_I^k := |[\nabla f](I^k)|$, $\boldsymbol{\nabla}_O^k := |[\nabla f](O^k)|$
  $A_I^k := c(\boldsymbol{\nabla}_I^k)$, $A_O^k := c(\boldsymbol{\nabla}_O^k)$ (supposed non-singular)
  $C_I^k := (A_I^k)^{-1}$, $C_O^k := (A_O^k)^{-1}$
  $\boldsymbol{z}_I^{k+1} := \mathcal{I}(C_I^k f, I^k, \pi)$, $\boldsymbol{z}_O^{k+1} := \mathcal{O}(C_O^k f, O^k, \pi)$
  if $\boldsymbol{z}_I^k = \emptyset$ **then**
    return
  end
  $I^{k+1} := A_I^k \boldsymbol{z}_I^{k+1}$, $O^{k+1} := A_O^k \boldsymbol{z}_O^{k+1}$
end for

Method 2

- Compute the sensitivity to initial states
- At each step k, compute under/over-approximation of range($f^k, \mathbf{z}^0$), i.e. the loop body f iterated k times, starting from $\mathbf{z}^0$.

for k from 0 to $K-1$ **do**

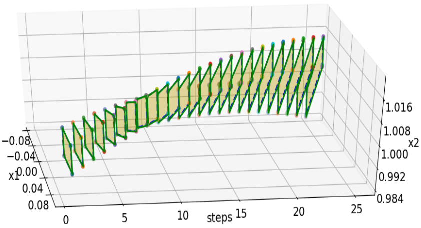
$I^{k+1} := \mathcal{I}(f^{k+1}, \mathbf{z}^0, \pi)$, $O^{k+1} := \mathcal{O}(f^{k+1}, \mathbf{z}^O, \pi)$

end for

Test model

$$x_1^{k+1} = x_1^k + (0.5(x_1^k)^2 - 0.5(x_2^k)^2)\Delta$$
$$x_2^{k+1} = x_2^k + 2x_1^k x_2^k \Delta$$

with as initial set $x_1 \in [0.05, 0.1]$ and $x_2 \in [0.99, 1.00]$, and $\Delta = 0.01$.



Under- (yellow) and over-approximated (green) reachable sets over time up to 25 steps with Algorithm 1, skewed boxes (0.02s computation time)

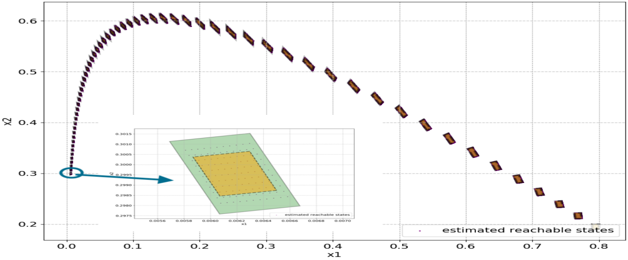
SIR Epidemic Model

Model

x_1 healthy; x_2 infected; x_3 recovered. β, contract. rate, γ, mean infect. period, Δ step.

$$x_1^{k+1} = x_1^k - \beta x_1^k x_2^k \Delta$$
$$x_2^{k+1} = x_2^k + (\beta x_1^k x_2^k - \gamma x_2^k)\Delta$$
$$x_3^{k+1} = x_3^k + \gamma x_2^k \Delta$$

Algorithm 1: 60 steps from $(x_1, x_2, x_3) \in [0.79, 0.80] \times [0.19, 0.20] \times [0, 0.1]$ (in 0.05s).



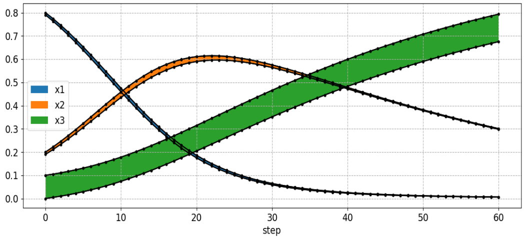
SIR Epidemic Model

Model

x_1 healthy; x_2 infected; x_3 recovered. β, contract. rate, γ, mean infect. period, Δ step.

$$x_1^{k+1} = x_1^k - \beta x_1^k x_2^k \Delta$$
$$x_2^{k+1} = x_2^k + (\beta x_1^k x_2^k - \gamma x_2^k)\Delta$$
$$x_3^{k+1} = x_3^k + \gamma x_2^k \Delta$$

Only algorithm 2 finds non-empty, tight approx (in 0.05s, init. $x_3 = 0$ instead of $x_3 \in [0, 0.1]$)



Honeybees Site Choice Model

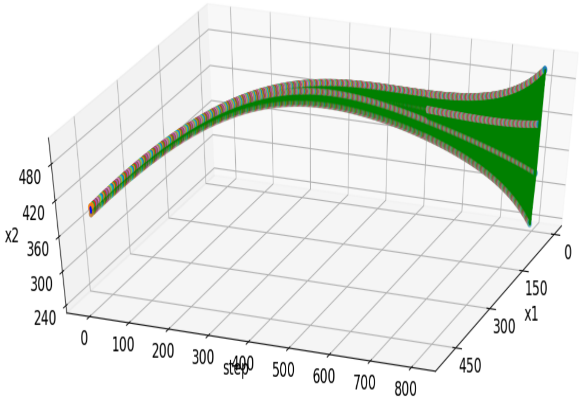
Model

$$
\begin{aligned}
x_1^{k+1} &= x_1^k - (\beta_1 x_1^k x_2^k + \beta_2 x_1^k x_3^k)\Delta \\
x_2^{k+1} &= x_2^k + (\beta_1 x_1^k x_2^k - \gamma x_2^k + \delta\beta_1 x_2^k x_4^k + \alpha\beta_1 x_2^k x_5^k)\Delta \\
x_3^{k+1} &= x_3^k + (\beta_2 x_1^k x_3^k - \gamma x_3^k + \delta\beta_2 x_3^k x_5^k + \alpha\beta_2 x_3^k x_4^k)\Delta \\
x_4^{k+1} &= x_4^k + (\gamma x_2^k - \delta\beta_1 x_2^k x_4^k - \alpha\beta_2 x_3^k x_4^k)\Delta \\
x_5^{k+1} &= x_5^k + (\gamma x_3^k - \delta\beta_2 x_3^k x_5^k - \alpha\beta_1 x_2^k x_5^k)\Delta
\end{aligned}
$$

$x_1 = 500$, $x_2 \in [390, 400]$, $x_3 \in [90, 100]$, $x_4 = x_5 = 0$ and parameters $\beta_1 = \beta_2 = 0.001$, $\gamma = 0.3$, $\delta = 0.5$, $\alpha = 0.7$, and $\Delta = 0.01$.

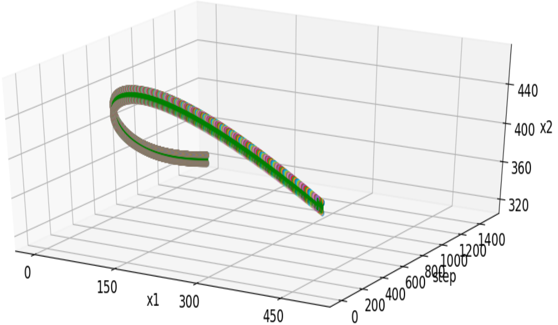
Honeybees Site Choice Model

Algorithm 1 (1.7s analysis time, 800 steps, but imprecise)



Honeybees Site Choice Model

Algorithm 2 (57s analysis time, 1500 steps)



Very tight projected under-approximations: (slightly faster/tighter than Dreossi 2016)

Table of Contents

Application to reachability of continuous systems

For an ODE $\dot{x} = f(x, u)$, flow φ^f

We compute:

1. a maximal over-approximation $\tilde{\mathcal{O}}^f_{\mathcal{E}}(t)$ of the trajectory $\varphi^f(t; \tilde{z}_0, \tilde{u})$ for a given $(\tilde{z}_0, \tilde{u}) \in \boldsymbol{Z}_0 \times \boldsymbol{U}$.
2. a maximal over-approximation $\mathcal{O}^F_{\mathcal{E}}(t)$ of the sensitivity matrix with respect to uncertain initial condition z_0 and input u, over the range $\boldsymbol{Z}_0 \times \boldsymbol{U}$.

We can use any over-approximation method for this ; we use a combination of Taylor models, affine forms (and skewing and subdivisions in some cases) here.

Eric Goubault, Sylvie Putot: Robust Under-Approximations and Application to Reachability of Non-Linear Control Systems With Disturbances. IEEE Control. Syst. Lett. 4(4), 2020

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 $[t_j, t_{j+1}]$:

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

- 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 $[\boldsymbol{r}_{j+1}]$ 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 $[\boldsymbol{z}_{j+1}] = [\boldsymbol{z}](t_{j+1}, t_j, [\boldsymbol{z}_j])$

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

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 $\tilde{z}_0 \in \text{pro}\ [z_0]$ 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

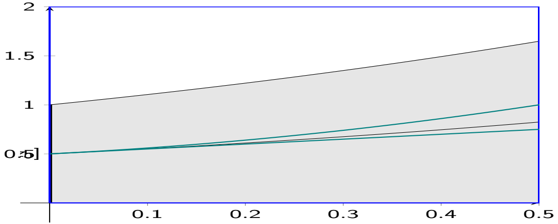
Algorithm (Init: $j = 0,\ t_j = t_0,\ [\boldsymbol{z}_j] = [\boldsymbol{z}_0],\ [\tilde{z}_j] = \tilde{z}_0 \in [\boldsymbol{z}_0],\ [\boldsymbol{J}_j] = Id$)

- 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: $[z_0] = [0,1]$, $\tilde{z}_0 = 0.5$, $[J_0] = 1$
- 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 $z(t, \tilde{z}_0)$, $\tilde{z}_0 \in [z_0] = [0,1]$:

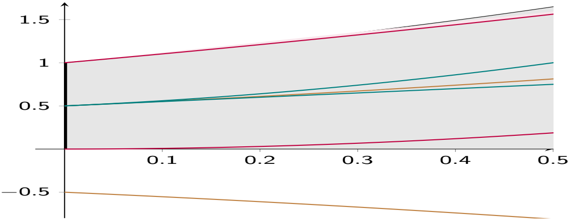
$$z(t, z_0) = z(0, z_0) + z(0, z_0)t + \frac{z(\xi, z_0)}{2} t^2, \quad \xi \in [0, 0.5]$$
$$[z](t, \tilde{z}_0) = \tilde{z}_0 + \tilde{z}_0 t + [0,1] t^2$$

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

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

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

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



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:

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

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) :

$$p_{(u_j^i)}(t) = \sum_{q=0}^{l} u_j^q \frac{(t - t_j)^q}{q!} \qquad (1)$$

  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 (1), 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)).

6D quadrotor

6 dim simplified quadcopter : coordinates (p_x, p_y), pitch ϕ

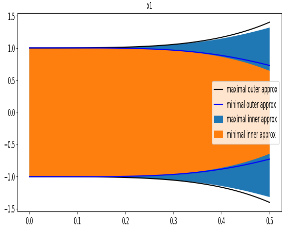
$$
\begin{aligned}
\dot{p}_x &= v_x \\
\dot{v}_x &= \frac{1}{m} C_D^v v_x - \frac{T_1}{m} sin\phi - \frac{T_2}{m} sin\phi \\
\dot{p}_y &= v_y \\
\dot{v}_y &= -\frac{1}{m}(mg + C_D^v v_y) + \frac{T_1}{m} cos\phi + \frac{T_2}{m} cos\phi \\
\dot{\phi} &= \omega \\
\dot{\omega} &= -\frac{1}{I_{yy}} C_D^\phi - \frac{l}{I_{yy}} T_1 + \frac{l}{I_{yy}} T_2
\end{aligned}
$$

- Control T_1 (resp. T_2): cumulated thrust of the two left (resp. right) motors; $T_1 \in [9, 9.5125]$, $T_2 \in [9, 9.5125]$
- $C_D^v = 0.25$, $C_D^\phi = 0.02255$, $g = 9.81$, $m = 1.25$, $l = 0.5$, $I_{yy} = 0.03$

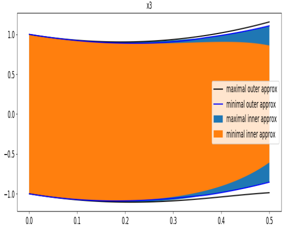
6D quadrotor

- Target set: $\mathcal{G}_0 = \{(p_x, v_x, p_y, v_y, \phi, \omega) | -1 \leq p_x \leq 1,\ -1 \leq p_y \leq 1,\ v_x = 0,\ v_y = 1,\ -0.01 \leq \phi \leq 0.01,\ -0.01 \leq \omega \leq 0.01\}$.

Reachable set for time horizon $t = 0.5$ s, computed in 0.42 seconds for Taylor order 4, step size of 0.01, no disturbance, constant controls



p_x as a function of time



p_y as a function of time

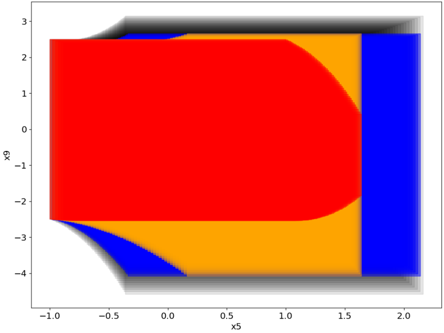
10D quadcopter

Model

$$\begin{pmatrix} \dot{p}_x \\ \dot{v}_x \\ \dot{\theta}_x \\ \dot{\omega}_x \\ \dot{p}_y \\ \dot{v}_y \\ \dot{\theta}_y \\ \dot{\omega}_y \\ \dot{p}_z \\ \dot{v}_z \end{pmatrix} = \begin{pmatrix} v_x + d_x \\ g tan \theta_x \\ -d_1\theta_x + \omega_x \\ -d_0\theta_x + n_0 S_x \\ v_y + d_y \\ g tan \theta_y \\ -d_1\theta_y + \omega_y \\ -d_0\theta_y + n_0 S_y \\ v_z + d_z \\ k_T T_z - g \end{pmatrix}$$

- defining position (p_x, p_y, p_z); velocities (v_x, v_y, v_z); pitch, roll (θ_x, θ_y); pitch, roll rates (ω_x, ω_y); $-\frac{\pi}{18} \leq S_x \leq \frac{\pi}{18}$, $-\frac{\pi}{18} \leq S_y \leq \frac{\pi}{18}$, $0 \leq T_z \leq 2g = 19.62$.
- Wind disturbances (d_x, d_y, d_z); $n_0 = 10$, $d_1 = 8$, $d_0 = 10$, $k_T = 0.91$
- controls S_x, S_y in $[-\frac{\pi}{180}, \frac{\pi}{180}]$ (target pitch, roll); $T_z \in [0, 19.62]$, vertical thrust
- Target set: $-1 \leq p_x, p_y \leq 1$, $-2.5 \leq p_z \leq 2.5$, $v_x = -1.5$, $\theta_x = 0$, $\omega_x = 0$, $v_y = -1.8$, $\theta_y = 0$, $\omega_y = 0$, $v_z = 1.2$.

10D quadrotor

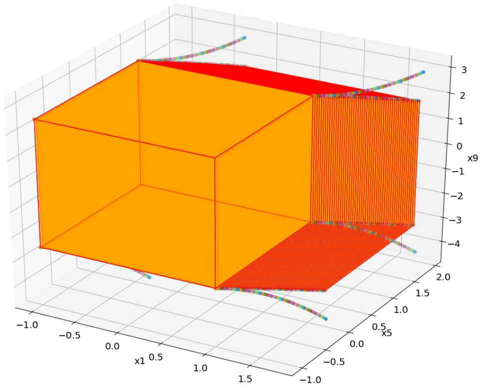


Joint p_y and p_z

Disturbances, time-varying controls (analysis time of 6.49 seconds),

minimal under-approximation of the image in red, close to the robust and maximal under-approximations in orange and blue and maximal over-approximations in grey.

10D quadrotor



Joint p_x, p_y and p_z

Constant controls, no disturbance (1.22 s analysis time), robust inner image in orange (the maximal range=robust range) similar results without decomposition as M. Chen, S. L. Herbert, M. S. Vashishtha, S. Bansal, and C. J. Tomlin, "Decomposition of reachable sets and tubes for a class of nonlinear systems," IEEE Trans. Aut. Control, 2018

Table of Contents

Efficiency

ODE	*dim*	*param*	*t hor*	*stepsize*	*order*	*disturb*	*time − var*	*subd*	*time s*
Bru	2	2	4	0.02	4				1.26
*B*24	2	1	1	0.1	3	✓	✓		0.02
Dub	3	4	1	0.01	3				0.14
−	−	−	−	−	−			100	11.58
−	−	−	−	−	−	✓	✓	100	428.1
6*D*	6	2	1	0.01	4				0.87
−	−	−	−	−	−		✓		15.56
−	−	−	−	−	−	✓	✓		30.52
L − *L*	7	0	20	0.1	3				24.04
10*D*	10	6	1	0.01	5				1.26
−	−	−	−	−	−		✓		9.98

- d: dim system; p: number of params; time: analysis time (seconds);
- T time horizon; δ step-size; k order; sd: number of subd.
- a checked if adversarial disturbances; v checked when time-varying uncertainties.

Conclusion and future work

- Checkout `https://github.com/cosynus-lix/RINO` !
- General quantified problems and applications to viability
- Larger classes of systems (hybrid/switched, DDEs as in CAV 2018 etc.)

Any questions?

{Eric.Goubault,Sylvie.Putot}@polytechnique.edu