Set-based methods for the analysis of dynamical systems

Eric Goubault, Sylvie Putot

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

Table of Contents

Cyber-Physical Systems ?

Some examples

- Autonomous systems, such as autonomous cars (e.g. robotics)
- Health systems
- Energy production (e.g. smart grids)
- All safety critical control systems (e.g. primary flight computers) etc.

In this course

We consider "formal" verification of robotics systems mostly :

- "low-level" control systems
- "high-level" planification and navigation algorithms

More and more of these aspects are implemented using AI-based (learning) mechanisms (localization through vision, even control through learning - some other talk)

All these systems are programmed systems with numerically-intensive aspects, in relation with physical aparatus.

Example: the automotive industry

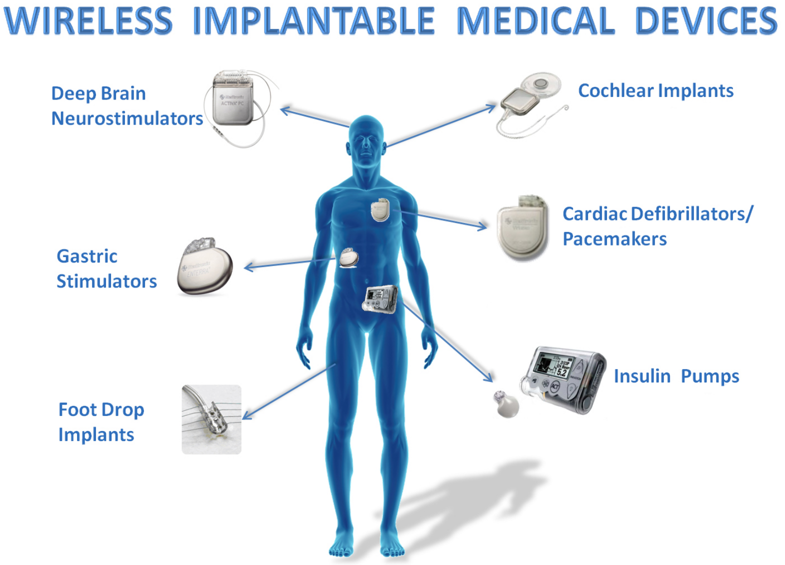
- Security functions: ABS, airbags, opening policy of doors
- Comfort functions (cruise control, rain sensing control, etc), with interactions with the security functions
- Embedded navigation system (some communication)
- Towards autonomous vehicles (parking assistance, collision avoidance, etc) ; lots of learning based algorithms
- Complex mapping of functions onto the ECUs

Example: aeronautics

- Airplanes rely heavily on computer-enabled control
  - Fly-by-Wire vs. cable/hydraulic
  - Collision avoidance
- Flight computers can override pilot commands

We must ensure that safe envelopes are maintained, for every possible configuration.

Closed-loop medical devices



Closed-loop medical devices

They present all the challenges of safe CPS design:

Complex modeling

- Modeling the relevant aspects of human physiology: insulin-glucose regulatory models, cardiac modeling, etc.
- Reasoning with uncertainties: in models, sensors of limited capacity, human behavior, etc.
- Control: sophisticated algorithms to control critical physiological functions with sensing/actuation/computing limitations

Find the right level of abstraction to reason efficiently

- For example, timed automata may be sufficient for the temporal reasoning to validate a simple pacemaker model

Safety and security issues

- Closed-loop medical devices are safety-critical: malfunctions result in serious injury or death to the patient
- Security issues: August 2017 - hacking risk leads to recall of 500000 pacemaker

There is a need for safe design !

Fully autonomous cars soon (with at a higher level, smart road infrastructure)... but their safety remains a big challenge.

Warning: Traffic-Aware Cruise Control can not detect all objects and may not brake/ decelerate for stationary vehicles, especially in situations when you are driving over 50 mph (80 km/h) and a vehicle you are following moves out of your driving path and a stationary vehicle or object is in front of you instead. Always pay attention to the road ahead and stay prepared to take immediate corrective action. Depending on Traffic-Aware Cruise Control to avoid a collision can result in serious injury or death. In addition, Traffic-Aware Cruise Control may react to vehicles or objects that either do not exist or are not in the lane of travel, causing Model X to slow down unnecessarily or inappropriately.

Many possible models

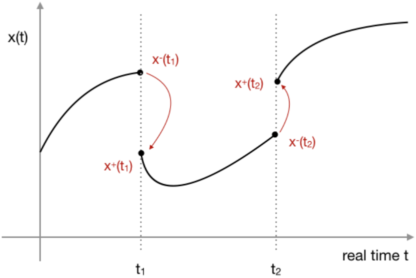
- ODEs, switched systems, hybrid systems
- DAEs etc.
- data based

We will focus on ODE based models, like hybrid systems (next slides) - control may as well be implemented with a neural network in what we did up to now.

From dynamical to hybrid systems, informally

Simple hybrid system:

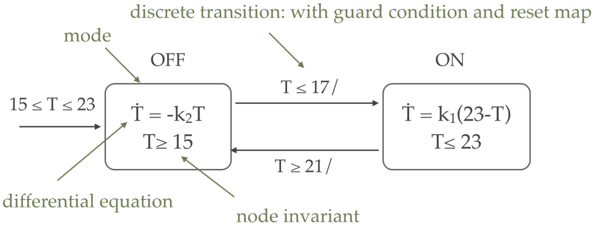
- smooth dynamics almost all the time, except for state jumps $x^+ = g(x^-)$ at some discrete t.
- transitions can be time-dependent or state-dependent

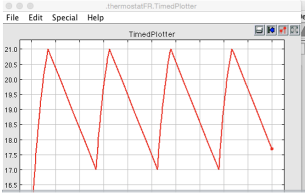


Hybrid Automata: the most classical model for hybrid systems

Example (Self-regulating switching thermostat with hysteresis)

- State machine with continuous state variable T
- Time progresses within modes (ON/OFF) and T changes continuously according to differential equations
- Transitions between modes are instantaneous and enabled by the satisfaction of guards on T; T can be discontinuously updated during mode-switches
- Invariants constrain how long the system can stay in a discrete mode



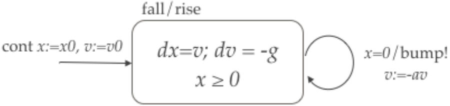


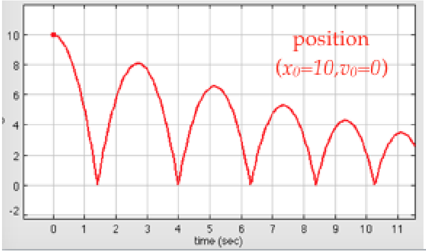
A very rich model: even before verification, well-posedness and existence of solutions on $t \in [0, \infty[$ can already be a problem

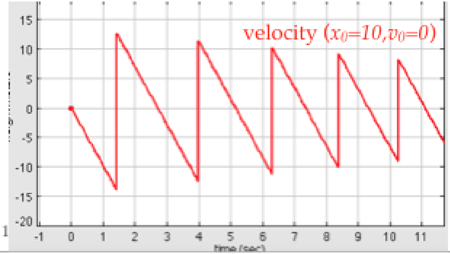
A classical example: the bouncing ball

Hybrid systems are useful to model also purely physical phenomena such as collisions (and not only interaction between controller and physical world)

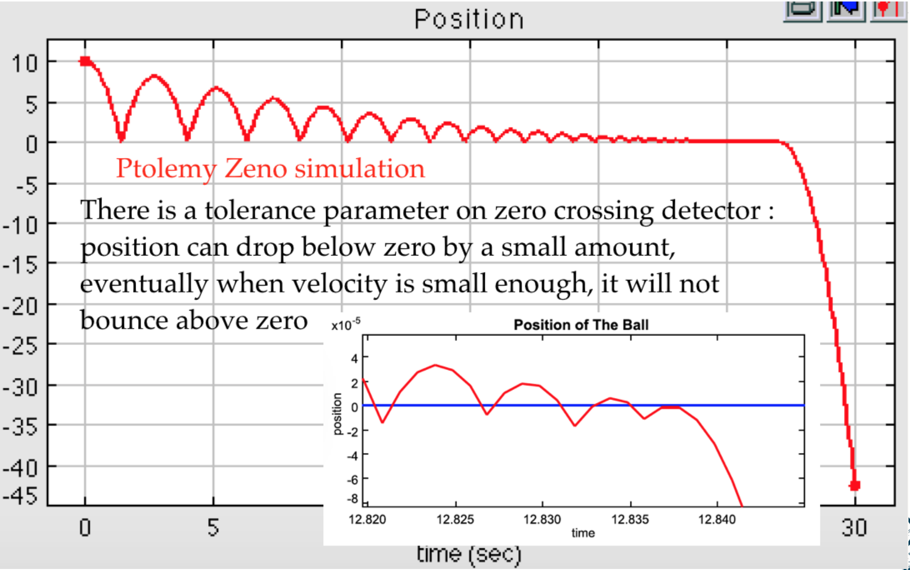
- Ball dropped from initial height x_0 with initial vertical velocity v_0
- Dynamics subject to $\dot{x}(t) = v, \dot{v}(t) = -g$
- When the ball hits the ground ($x = 0$), velocity changes discretely: $v := -a.v$, with $0 < a < 1$ dampening constant







Zeno bouncing ball: simulation in practice



Ptolemy Zeno simulation

There is a tolerance parameter on zero crossing detector : position can drop below zero by a small amount, eventually when velocity is small enough, it will not bounce above zero

Reachability and invariance

Reachability

- (forward) Characterize the set of final states from a given state of initial conditions.
- (backward) Characterize the set of initial conditions that reach a desired goal set.
- In case there is a control input, possibly design a controller such that the state trajectory starting from a given initial condition reaches the desired set.

(can be made probabilistic etc.)

Robust Reachability

If both control and disturbance inputs are available, the reachability problem can be thought of as a pursuit-evasion game, where the controller wins if it can keep the system from entering a "bad" subset of the state space, called the capture set, while the disturbance wins if it can drive the state into the bad set.

Invariance

"Unbounded-time" reachability. The control synthesis concerns with designing a controller such that the state trajectories remain inside the safe set. In the presence of uncertainties: viability.

A logical view: safety and liveness properties, as temporal logic formulas

Proof or falsification of general temporal formulas

Temporal logics is a logics building on classical logics, plus "modal" operators such as "eventually", "always" etc.

Safety properties [invariants]

Informally, for proving that something bad never happens (using modality "always"). E.g. never hit an obstacle

Liveness properties [reachability]

Informally, for proving that something good eventually happens (using modality "eventually"). E.g. eventually reaches target.

An arbitrary property can be expressed as intersection of a safety and a liveness property. E.g. reach-avoid properties.

Logical specifications (more complex quantified reachability, 2nd part)

E.g. STL "Signal Temporal Logic"

Properties are temporal relations between signal predicates

$$\varphi := \ \mathit{true} \mid x_i \geq 0 \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi U_I \varphi$$

- x_i is a system variable
- I is an interval $[a, b]$ (of times)
- U is the "until" operator
- Common syntactic sugar: $\Box_I \varphi = \mathit{true}\ U_I \neg\varphi$, $\Diamond_I \varphi = \neg \Box_I \neg \varphi$

Examples

- Velocity will be non-negative until a collision occurs $v \geq 0 U_{[0,\infty]} x \geq L$
- Collision will not occur $\Box_{[0,\infty]} x < L$ (its negation is a reachability property)

(and extensions of the logics to deal with *sets* of traces)

Semantics of STL

STL formulas are evaluated over execution traces

- A trace w is a set of signals $t \to x_i(t)$
- Signal is the value of a variable as a function of time: $\mathbb{R}^+ \to \mathbb{R} \cup \{\perp, \top\}$

Rules

$$
\begin{array}{lcll}
w, t & \models & true & \\
w, t & \models & x_i \geq 0 & \text{iff } x_i(t) \geq 0 \\
w, t & \models & \neg\varphi & \text{iff } w, t \not\models \varphi \\
w, t & \models & \varphi \wedge \psi & \text{iff } w, t \models \varphi \text{ and } w, t \models \psi \\
w, t & \models & \varphi U_I \psi & \text{iff } \exists t' \in t + I,\ w, t' \models \psi \wedge (\forall t'' \in [t, t'],\ w, t'' \models \varphi)
\end{array}
$$

Needs interpreting at least, generally quantified formulas (end of this talk)

Reachability-based verification (1st part)

Safety verification, temporal properties

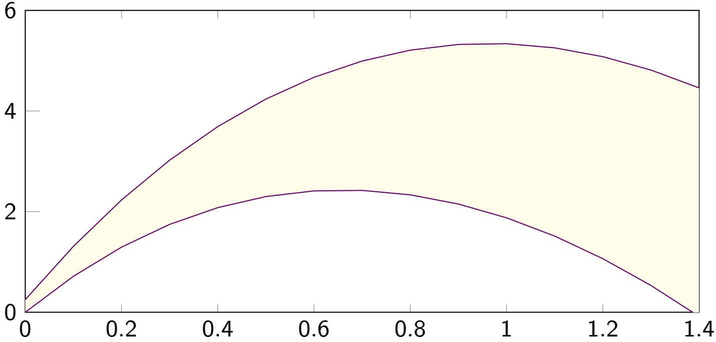
- Compute (outer) enveloppes of all possible trajectories (not possible to compute exact envelopes)
- If these enveloppes do not intersect with sets of unsafe states, then the system is safe
- Compute inner enveloppes, for applications to additional temporal properties (e.g. reach-avoid)

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

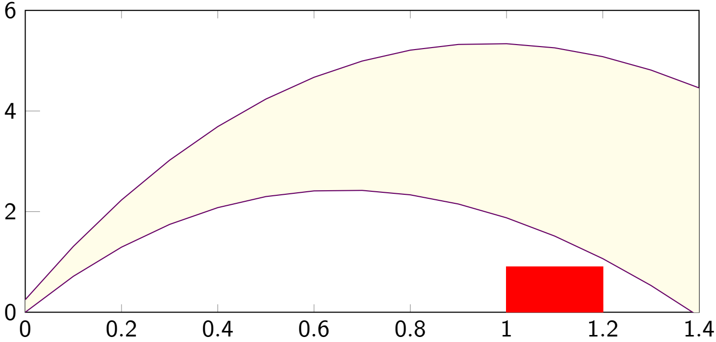
Inner and outer approximations of reachable sets for uncertain dynamical systems

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



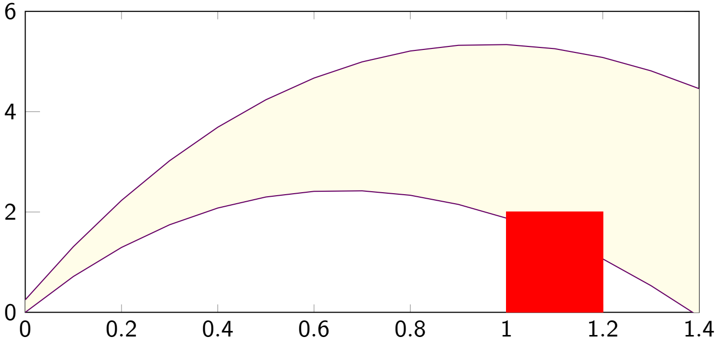
Inner and outer approximations of reachable sets for uncertain dynamical systems

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



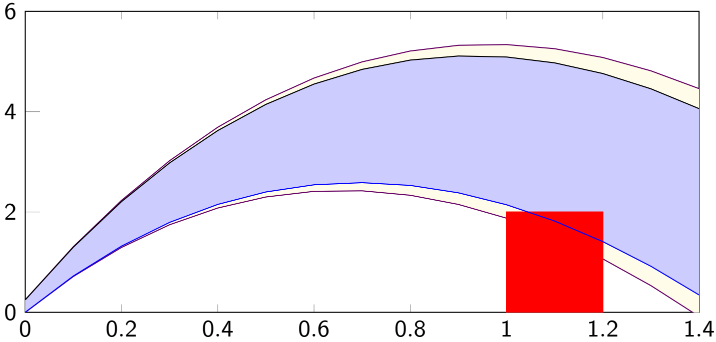
Inner and outer approximations of reachable sets for uncertain dynamical systems

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



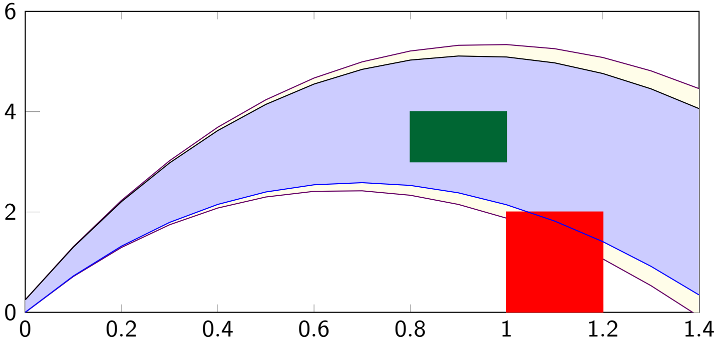
Inner and outer approximations of reachable sets for uncertain dynamical systems

- 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



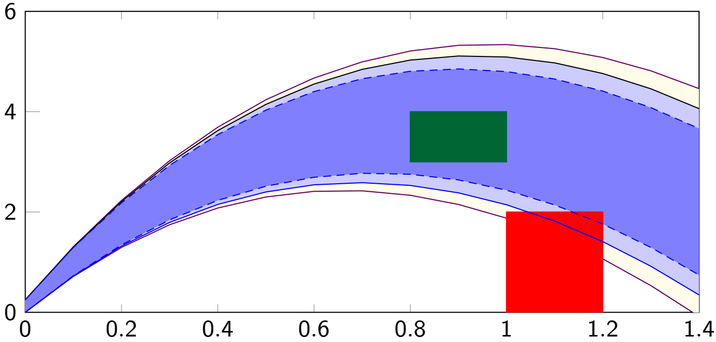
Inner and outer approximations of reachable sets for uncertain dynamical systems

- 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 ?)



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



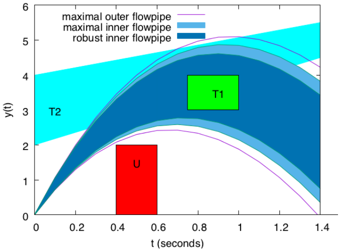
Approximate reachability and verification ?

Example

A cannon shoots bullets. Trajectory (x, y), velocity v and angle γ of the velocity with respect to the x axis:

$$\dot{v} = -g\gamma - \frac{\rho v^2}{2m} a C_d \qquad \dot{x} = v(1-\gamma^2/2)$$
$$\dot{\gamma} = -\frac{g(1-\gamma^2/2)}{v} \qquad \dot{y} = v\gamma$$

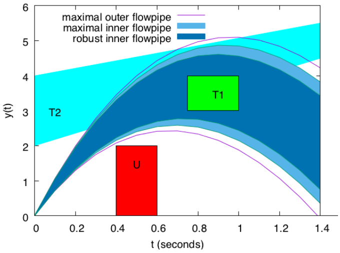
The mass m of the bullet is uncertain (a disturbance). The initial state is uncertain.
that should be able to reach targets T_1 and T_2, and avoid a wall L



Height $y(t)$

"Classical" properties for the verification of control systems

- 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

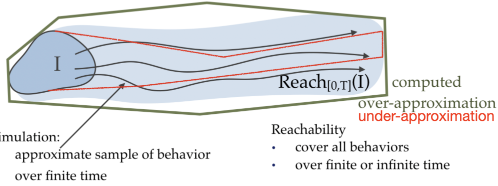


Height $y(t)$

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) $\varphi^f(s; x_0, u)$



Maximal reachability ("classical" reachability)

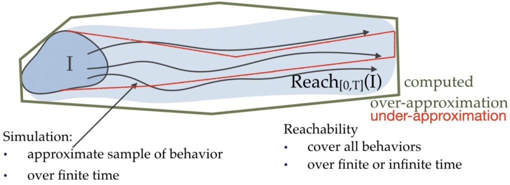
[I. M. Mitchell, HSCC 2007] Comparing Forward and Backward Reachability as Tools for Safety Analysis

- State x_f is (maximally) reachable at time s if
$$\exists x_0 \in \boldsymbol{Z}_0,\ \exists u : [0, s] \rightarrow \mathbb{U}, \text{ s.t. } \varphi^f(s; x_0, u) = x_f$$
- The (maximal) 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
$$R^f_{\mathcal{E}}([0, t]; \boldsymbol{Z}_0, \mathbb{U}) = \{x_f | x_f \text{ is reachable for some time } s \leq t\}$$

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) $\varphi^f(s;x_0,u)$



Minimal reachability

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

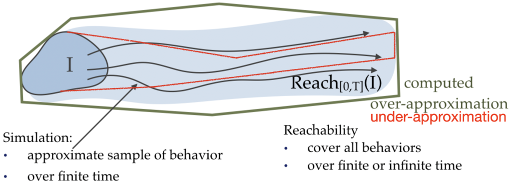
- State x_f is (minimally) reachable at time s if
$$\forall u:[0,s]\rightarrow\mathbb{U},\ \exists x_0\in\boldsymbol{Z}_0,\ \text{s.t. } \varphi^f(s;x_0,u)=x_f$$
- The (minimal) reachable set of system (S) is
$$R^f_{\mathcal{A}}(\boldsymbol{Z}_0,\mathbb{U})=\{x_f|x_f \text{ is reachable}\}$$

(but not often computed over infinite time)

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

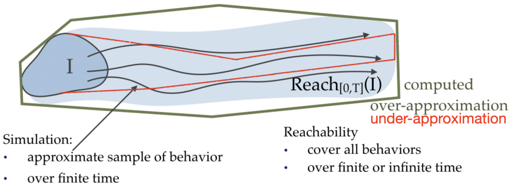
States that trajectories will reach whatever some components u_A of the input signal is, and for some other components u_E of the input signal

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

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

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

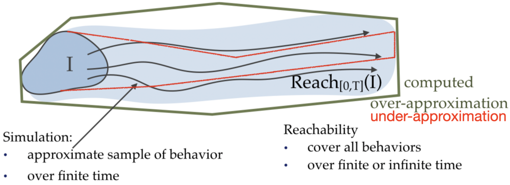
Think of disturbances for u_A, and controls for u_E; classical maximal reachability is for $\mathbb{U}_{\mathbb{A}} = \emptyset$, minimal reachability is for $\mathbb{U}_{\mathbb{E}} = \emptyset$ as defined in e.g.

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

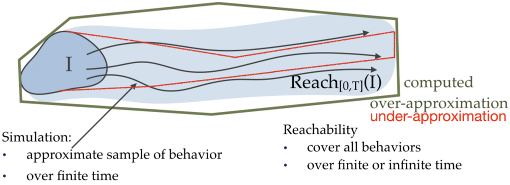
$$R^f_{\mathcal{AE}}(t; \boldsymbol{Z}_0, \mathbb{U}) = \{z \in \mathcal{D} \,|\, \forall u_A \in \mathbb{U}_{\mathbb{A}}, \exists u_E \in \mathbb{U}_{\mathbb{E}}, \exists z_0 \in \boldsymbol{Z}_0,\ z = \varphi^f(t; z_0, u_A, u_E)\}$$

We cover also time-dependent inputs - control - and disturbances ; other notion of robustness is $\exists u_E,\ \forall u_A$ see part II!

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

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

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

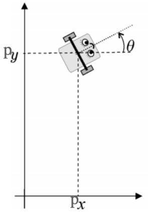
A simple example (1st part)

Dubbins vehicle

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

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

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)

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

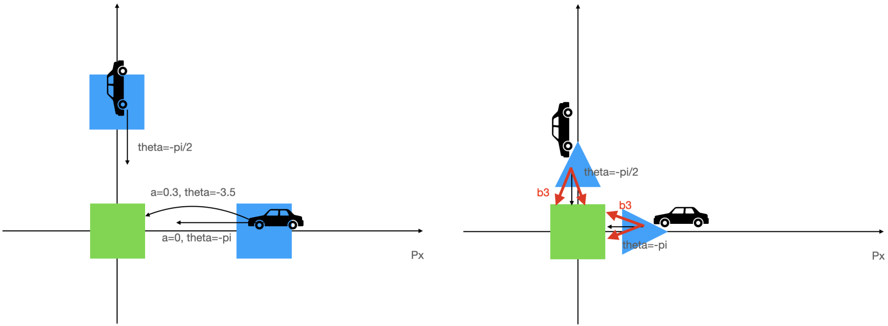
$$\mathcal{G}_0 = \{(p_x, p_y, \theta) || p_x| \leq 0.5, |p_y| \leq 0.5,\ 0 \leq \theta \leq 2\pi\}$$

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

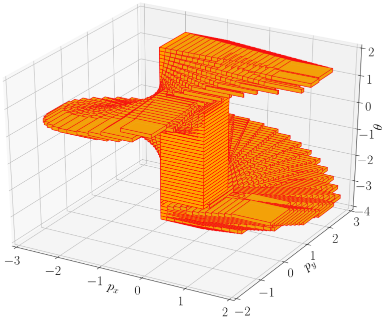


Without disturbance With disturbance

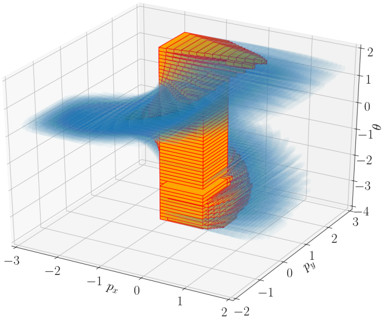
Robust approximation of BRS for the Dubbins vehicle

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

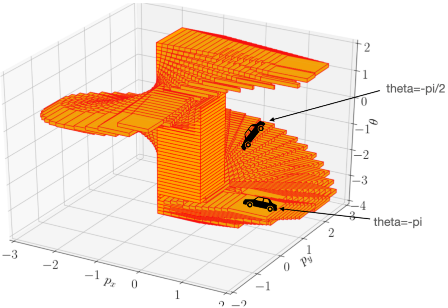


Robust inner (with disturbances), maximal inner (with disturbances)

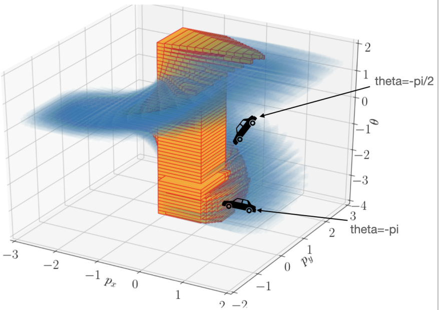
Joint p_x, p_y and θ for Dubbins, constant controls The results, also obtained in 2 seconds

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 The 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

Generalization (2nd part)

Dubbins vehicle again!

$$\begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{\theta} \end{pmatrix} = \begin{pmatrix} v cos(\theta) + b_1 \\ v sin(\theta) \\ a \end{pmatrix}$$

- Control period of $t = 0.5$, linear velocity $v = 1$,
- Init: $\mathbb{X}_0 = \{(x, y, \theta) \mid x \in [-0.1, 0.1],\ y \in [-0.1, 0.1],\ \theta \in [-0.01, 0.01]\}$,
- Control a (angular velocity) in $\mathbb{U} = [-0.01, 0.01]$,
- disturbance b_1 in $\mathbb{W} = [-0.01, 0.01]$

We want to estimate:

$$R_{\exists\forall\exists}(\varphi) = \{z \in \mathbb{R}^m \mid \exists u \in \mathbb{U},\ \exists x_0 \in \mathbb{X}_0,\ \forall w \in \mathbb{W},\ \exists s \in [0, T],\ z = \varphi(s; x_0, u, w)\}$$

We will find (instantly using our `Julia` implementation):

$$[-0.0949993455, 0.5899993275] \times [-0.0925, 0.0925] \times [-0.01, 0.01] \subseteq R_{\exists\forall\exists}(\varphi)$$

(timeout using quantifier elimination under Mathematica)

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

Classical mean-value theorem

f smooth enough: $\frac{f(x)-f(x_0)}{x-x_0} = f'(\xi)$ for some $\xi \in [x_0, x]$

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 $\{|f_i'(c(\boldsymbol{x}_1), \dots, c(\boldsymbol{x}_{i-1}), x_i, \dots, x_m)|, x \in \boldsymbol{x}\} \subseteq \Delta_i$

Then:

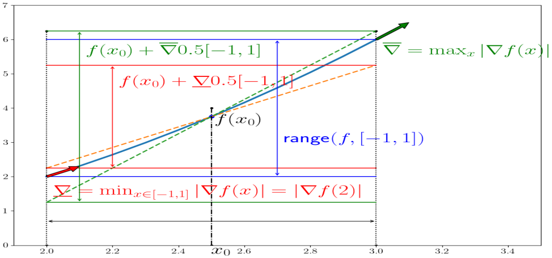
$$\mathrm{range}(f, \boldsymbol{x}) \subseteq [\underline{f_0}, \overline{f_0}] + \sum_{i=1}^{m} \overline{\Delta_i} r(\boldsymbol{x}_i)[-1, 1]$$

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

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 the CdC 2020 paper

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 $\{|\nabla_u f(w, u)|\ , w \in \boldsymbol{x}_{\mathcal{A}},\ u \in \boldsymbol{x}_{\mathcal{E}}\} \subseteq \boldsymbol{\nabla}_u$

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

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

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)

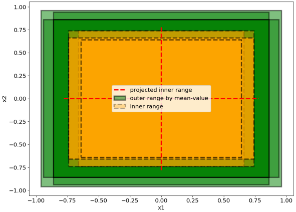
Compute 1-D inner range $\mathbf{z}_1$ of f_1 robust to x_1 and 1-D inner range $\mathbf{z}_2$ of f_2 robust to x_2:

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

Then

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

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



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

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

1-D under-approximations: $[-0.7, 0.7] \subseteq \text{range}(f_1, x)$, $[-0.68, 0.68] \subseteq \text{range}(f_2, x)$

2-D inner-approximation

- We obtain $[-0.64, 0.64]^2 \subseteq \text{range}(f_1, \boldsymbol{x}, 2)$ 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 we have 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-approximation (resp. over-approximation) of the robust range of g with respect to $x_{\mathcal{A}}$ and ξ, $\mathcal{I}_g \subseteq \text{range}(g, \mathrm{x} \times \mathrm{x}, I_{\mathcal{A}} \cup \{m+1, \ldots, 2m\}, I_{\mathcal{E}})$ is an under-approximation (resp. over-approximation) of the robust range of f with respect to $x_{\mathcal{A}}$, i.e. $\mathcal{I}_g \subseteq \text{range}(f, \mathrm{x}, I_{\mathcal{A}}, I_{\mathcal{E}})$

Hence

- 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 $\xi \in \mathrm{x}$.
- Let $\mathcal{I}_\alpha$ be an under-approximation of the robust range of α with respect to w, i.e. $\text{range}(\alpha, \mathrm{x}, I_{\mathcal{A}}, I_{\mathcal{E}})$, and $\mathcal{O}_\beta$ an over-approximation of the range of β, i.e. $\text{range}(\beta, \mathrm{x} \times \mathrm{x}, \emptyset, \{1, \ldots, 2m\})$.

The robust range of g with respect to $w \in \mathrm{x}_{\mathcal{A}}$ and $\xi \in \mathrm{x}$, i.e. $\text{range}(g, \mathrm{x} \times \mathrm{x}, I_{\mathcal{A}} \cup \{m+1, \ldots, 2m\}, I_{\mathcal{E}})$, is under-approximated by

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

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: $[0.875, 1.125]$.

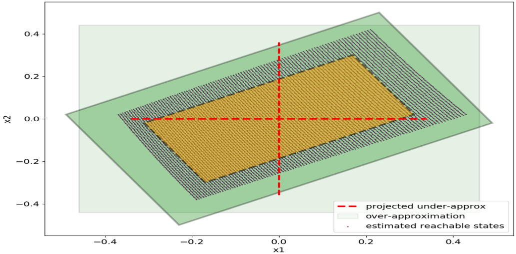
Skewing

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

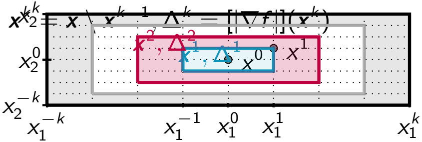
First idea: subdivision

- Partition each dimension $j = [1 \ldots m]$ of the m-dimensional input box $\boldsymbol{x} = \boldsymbol{x}_1 \times \ldots \times \boldsymbol{x}_m$ in $2k$ sub-intervals
- Define, for all $j = [1 \ldots m]$, $x_j^{-k} \leq x_j^{-(k-1)} \leq \ldots \leq x_j^0 \leq \ldots \leq x_j^k$, 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).

Quadrature

Partition: principle

- Note $\boldsymbol{x}^1 = [x_1^{-1}, x_1^1] \times [x_2^{-1}, x_2^1] \times \ldots \times [x_m^{-1}, x_m^1]$, and for all i between 2 and k, $\boldsymbol{x}^i = [x_1^{-i}, x_1^i] \times \ldots \times [x_m^{-i}, x_m^i] \setminus \mathring{\boldsymbol{x}}^{i-1}$,



- By mean-value,
  - $\forall x \in [x^{-1}, x^1]$, $\exists \xi^1 \in [x^{-1}, x^1]$, $f(x) = f(x^0) + \langle \nabla f(\xi^1), x - x^0 \rangle$. Let $\boldsymbol{f}^0 \supseteq f(x^0)$ and $\boldsymbol{\nabla}^i$ for i in $[1, k]$ such that $\{|\nabla f(x)|, x \in \boldsymbol{x}^i\} \subseteq \boldsymbol{\nabla}^i$.
  - So range$(f, \boldsymbol{x}^1) \subseteq \boldsymbol{f}^0 + \langle \overline{\nabla}^1, dx^1 \rangle [-1, 1]$, $[\overline{f^0} - \langle \underline{\nabla}^1, dx^1 \rangle, \underline{f^0} + \langle \underline{\nabla}^1, dx^1 \rangle] \subseteq$ range$(f, [x^{-1}, x^1])$.
  - Iterate on adjacent subdivisions: for $x \in \boldsymbol{x}^2$, there exist $x^1 \in \boldsymbol{x}^1 \cap \boldsymbol{x}^2$, $\xi^2 \in \boldsymbol{x}^2$ such that $f(x) = f(x^1) + \langle \nabla f(\xi^2), x - x^1 \rangle$ and $|x_1 - x_1^1| \leq dx_1^2$ and $|x_2 - x_2^1| \leq dx_2^2$.
  - range$(f, \boldsymbol{x}^1 \cup \boldsymbol{x}^2) \subseteq \boldsymbol{f}^0 + \langle \overline{\nabla}^1, dx^1 \rangle [-1, 1] + \langle \overline{\nabla}^2, dx^2 \rangle [-1, 1]$. There exists $(x, x^1) \in \boldsymbol{x}^2 \times \boldsymbol{x}^1$ s.t. $|x_1 - x_1^1| = dx_1^2$ and $|x_2 - x_2^1| = dx_2^2$ (take corners of boxes $\boldsymbol{x}^1$ and $\boldsymbol{x}^2$), so $[\overline{f^0} - \langle \underline{\nabla}^1, dx^1 \rangle - \langle \underline{\nabla}^2, dx^2 \rangle, \underline{f^0} + \langle \underline{\nabla}^1, dx^1 \rangle + \langle \underline{\nabla}^2, dx^2 \rangle] \subseteq$ range$(f, \boldsymbol{x}^1 \cup \boldsymbol{x}^2)$.
  - Generalizes to k subdivisions, i.e. under-approximation: $[\overline{f^0} - \sum_{i=1}^k \langle \underline{\nabla}^i, dx \rangle, \underline{f^0} + \sum_{i=1}^k \langle \underline{\nabla}^i, dx \rangle] \subseteq$ range$(f, \boldsymbol{x})$.

(similarly for robust range)

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 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.

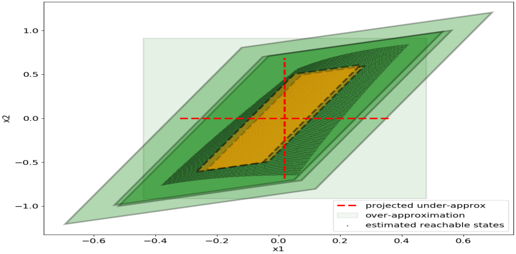


Table of Contents

Application to reachability of discrete systems

Principles

- Based on range estimation
- Two methods:
  - Method 1: propagate 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)

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 $\boldsymbol{z}^k$):

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

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 $\pi : [1 \dots n] \mapsto [1 \dots n]$
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

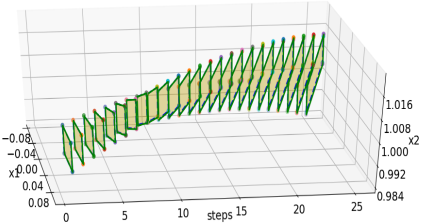
- Compute the sensitivity to initial states
- At each step k, compute under/over-approximation of range$(f^k, \boldsymbol{z}^0)$, i.e. the loop body f iterated k times, starting from $\boldsymbol{z}^0$.

for k from 0 to $K-1$ **do**
  $I^{k+1} := \mathcal{I}(f^{k+1}, \boldsymbol{z}^0, \pi)$, $O^{k+1} := \mathcal{O}(f^{k+1}, \boldsymbol{z}^O, \pi)$
end for

Test model

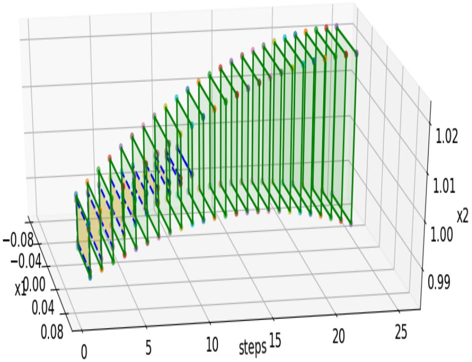
$$x_1^{k+1} = x_1^k + (0.5(x_1^k)^2 - 0.5(x_2^k)^2)\Delta$$
$$x_2^{k+1} = x_2^k + 2x_1^k x_2^k \Delta$$

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)

Test model



Box under and over-approximations for 25 steps of the test model

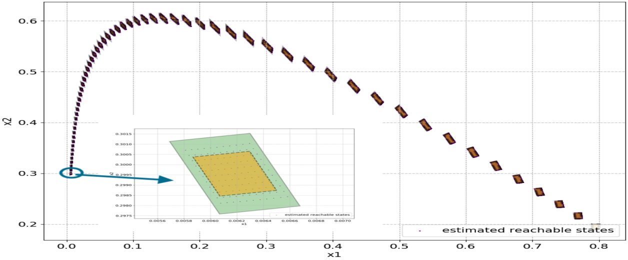
SIR Epidemic Model

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).



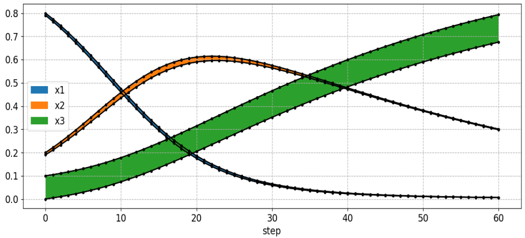
SIR Epidemic Model

Model

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

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

Algorithm 2 finds non-empty, tight approx (in 0.05s, init. $x_3 \in [0, 0.1]$)



Projections of under and over-approximations for 60 steps

Honeybees Site Choice Model

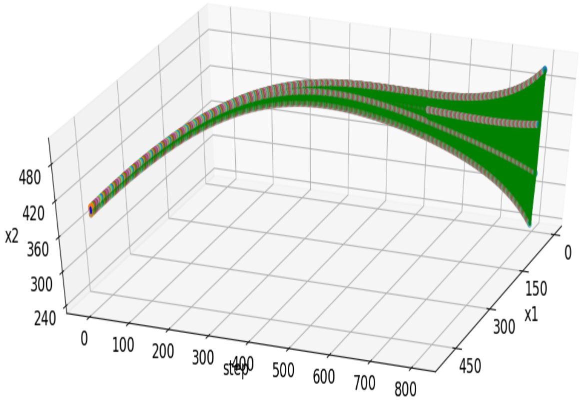
Model

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

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

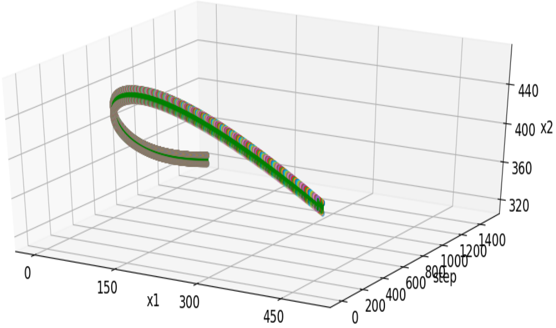
Honeybees Site Choice Model

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.

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

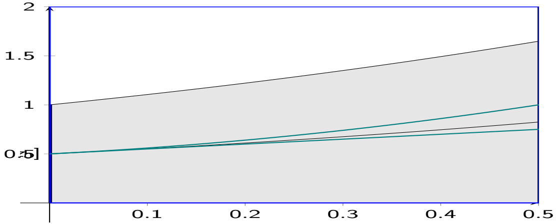
Algorithm (Init: $j = 0,\ t_j = t_0,\ [\boldsymbol{z}_j] = [\boldsymbol{z}_0],\ [\tilde{z}_j] = \tilde{z}_0 \in [\boldsymbol{z}_0],\ [\boldsymbol{J}_j] = Id$)

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

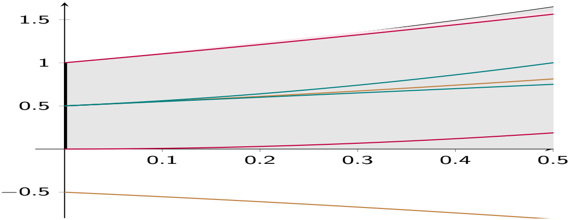
$$\begin{aligned} z(t, z_0) &= z(0, z_0) + z(0, z_0)t + \frac{z(\xi, z_0)}{2} t^2, \quad \xi \in [0, 0.5] \\ [z](t, \tilde{z}_0) &= \tilde{z}_0 + \tilde{z}_0 t + [0,1] t^2 \end{aligned}$$

  - 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 $\tilde{z}_0 = \mathrm{mid}([z_0]) = 0.5$ for inner tube:

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

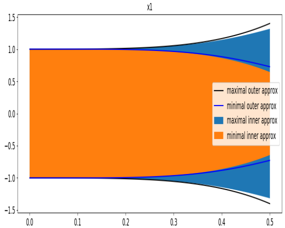


6D quadrotor

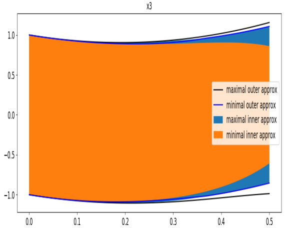
6 dim simplified quadcopter : coordinates (p_x, p_y), pitch ϕ

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

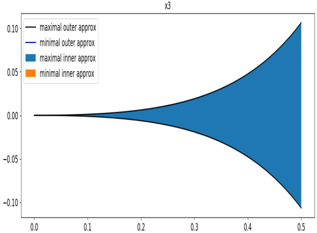
Model

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

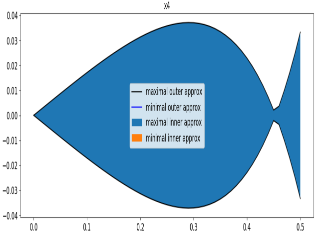
- defining position (p_x, p_y, p_z); velocities (v_x, v_y, v_z); pitch, roll (θ_x, θ_y); pitch, roll rates (ω_x, ω_y); $-\frac{\pi}{18} \leq S_x \leq \frac{\pi}{18}$, $-\frac{\pi}{18} \leq S_y \leq \frac{\pi}{18}$, $0 \leq T_z \leq 2g = 19.62$.
- Wind disturbances (d_x, d_y, d_z); $n_0 = 10$, $d_1 = 8$, $d_0 = 10$, $k_T = 0.91$
- 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

No disturbances, constant controls (1.28s comp. time, order 4, horizon 0.5s, step 0.01s)



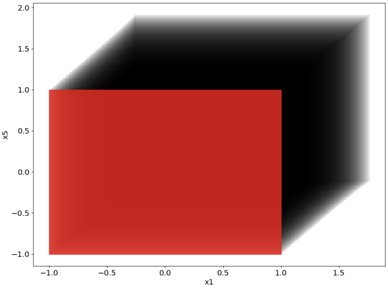
θ_x as a function of time



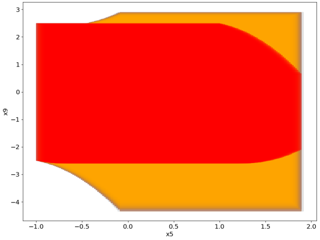
ω_x as a function of time

10D quadrotor

No disturbances, constant controls (1.28s comp. time, order 4, horizon 0.5s, step 0.01s)



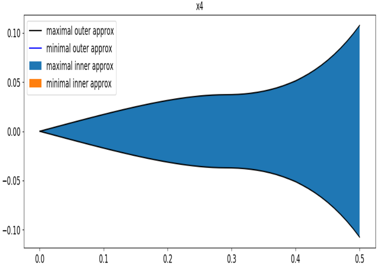
Joint range for p_x and p_y



Joint p_y and p_z

10D quadrotor

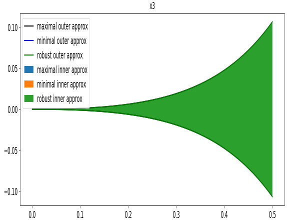
Time-varying controls (step 0.01s), no disturbance - analysis time 6.49s



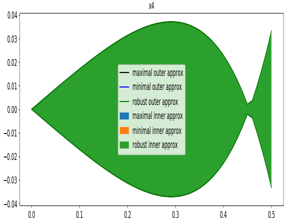
ω_x

10D quadrotor

Disturbances d_x, d_y, d_z in [-0.5, 0.5] - analysis time 1.22s)



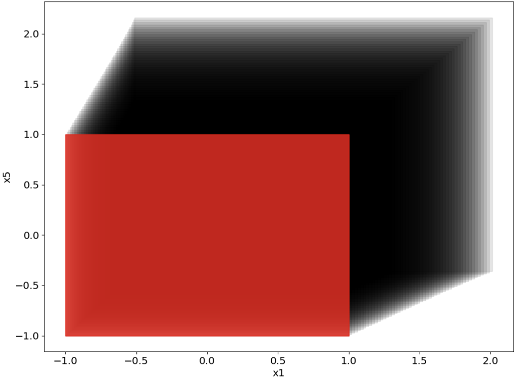
θ_x



ω_x

10D quadrotor

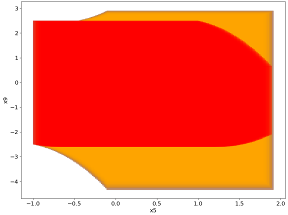
Disturbances d_x, d_y, d_z in [-0.5, 0.5] - analysis time 1.22s)



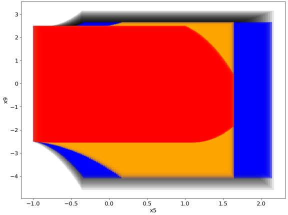
Joint range for p_x and p_y

10D quadrotor

No disturbance, time-varying



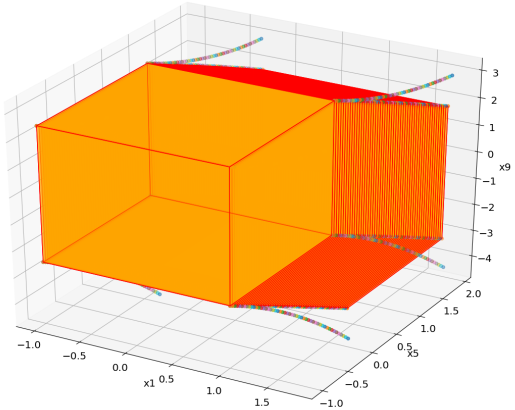
Joint p_y, p_z



Joint p_y and p_z

10D quadrotor

No disturbance, time-varying



Joint p_x, p_y and p_z

Efficiency

ODE	dim	$param$	$t\ hor$	$stepsize$	$order$	$disturb$	$time-var$	$subd$	$time\ s$
Bru	2	2	4	0.02	4				1.26
$B24$	2	1	1	0.1	3	✓	✓		0.02
Dub	3	4	1	0.01	3				0.14
–	–	–	–	–	–			100	11.58
–	–	–	–	–	–	✓	✓	100	428.1
$6D$	6	2	1	0.01	4				0.87
–	–	–	–	–	–		✓		15.56
–	–	–	–	–	–	✓	✓		30.52
$L-L$	7	0	20	0.1	3				24.04
$10D$	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.

Table of Contents

Motivation

Robust reachability - given $\phi(t; x_0, u, v)$ the flow of an ODE at time t from x_0 with control u and disturbance w

For time $t \in [0, T]$, compute:

$$R_{\forall\exists}(\varphi)(t) = \{z \ | \ \forall w \in \mathbb{W}, \ \exists x_0 \in \mathbb{X}_0, \ \exists u \in \mathbb{U}, z = \varphi(t; x_0, u, w)\}$$

(can a controller compensate disturbances or change of values of parameters that are known to the controller?)

"Even more" robust (but needs some time and/or space relaxation)

Can a controller not knowing the disturbance still reach the target, up to some (time) relaxation?

$$R_{\exists\forall\exists}(\varphi) = \{z \in \mathbb{R}^m \mid \exists u \in \mathbb{U}, \ \exists x_0 \in \mathbb{X}_0, \ \forall w \in \mathbb{W}, \ \exists s \in [0, T], \ z = \varphi(s; x_0, u, w)\}$$

But also

Motion planning

Go through regions S_j between times T_{j-1} and T_j, $j = 1, \dots, k$, final states z_k?

$$\begin{aligned}\{z_k \in \mathbb{R}^m \mid \exists u_1 \in \mathbb{U},\ \forall x_0 \in \mathbb{X}_0,\ \forall w_1 \in \mathbb{W},\ \exists t_1 \in [0, T_1],\ \exists z_1 \in S_1 \\ \exists u_2 \in \mathbb{U},\ \forall w_2 \in \mathbb{W},\ \exists t_2 \in [T_1, T_2],\ \exists z_2 \in S_2,\ \dots \\ \exists u_k \in \mathbb{U},\ \forall w_k \in \mathbb{W},\ \exists t_k \in [T_{k-1}, T], \\ \begin{pmatrix} z_1 \\ z_2 \\ \dots \\ z_k \end{pmatrix} = \begin{pmatrix} \varphi(t_1; u_1, x_0, w_1) \\ \varphi(t_2 - t_1; u_2, z_1, w_2) \\ \dots \\ \varphi(t_k - t_{k_1}; u_k, z_{k-1}, w_k) \end{pmatrix}\end{aligned}$$

General temporal logics formulas, and hyperproperties

E.g. behavioral robustness, or comparisons of controllers:

$$\begin{aligned}R_{\exists\forall\exists\forall\exists}(\varphi) = \{z \ \mid\ \exists x_0 \in \mathbb{X}_0,\ \exists \delta \in [-\epsilon, \epsilon]^i, \\ \forall u \in \mathbb{U},\ \exists u' \in \mathbb{U},\ \forall w \in \mathbb{W},\ \exists t \in [T_1, T_2], \\ z = \|\varphi(t; x_0, u, w) - \varphi(t; x_0 + \delta, u', w)\|\}\end{aligned}$$

Problem statement

Notations

- $f : \mathbb{R}^p \to \mathbb{R}^m$ (e.g. flow function etc.)
- the p arguments of f partitioned into consecutive j_i arguments $i = 1, \ldots, 2n$ corresponding to the alternations of quantifiers, with $p = \sum_{i=1}^{2n} j_i$.
- partition identified with sequence $(j_1, \ldots, j_{2n})$, denoted by $\boldsymbol{p}$.
- we note: $\boldsymbol{x}_i = (x_{k_i+1}, \ldots, x_{k_{i+1}})$ where $k_i = \sum_{l=1}^{i-1} j_l$, $i = 1, \ldots, 2n+1$, and

$$f(x_1, x_2, \ldots, x_{k_{2n}}) = f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{2n})$$

General quantified problems

n alternations of quantifiers $\forall\exists$ reachability problem:

$$R_{\boldsymbol{p}}(f) = \Big\{ z \in \mathbb{R}^m \mid \forall \boldsymbol{x}_1 \in [-1,1]^{j_1},\ \exists \boldsymbol{x}_2 \in [-1,1]^{j_2},\ \ldots,$$
$$\forall \boldsymbol{x}_{2n-1} \in [-1,1]^{j_{2n-1}}, \exists \boldsymbol{x}_{2\boldsymbol{n}} \in [-1,1]^{j_{2n}},\ z = f(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{2n}) \Big\}$$

On the generality of these quantified problems

Remarks

- Add dummy existential quantifier (resp. universal quantifier) at the beginning (resp. end) for getting all quantified formulas
- Up to reparametrization, quantified problems with other boxes than $[-1, 1]^{j_i}$
- Also possible to consider more general sets over which to quantify variables x_i by suitable outer and inner approximations as boxes
- Can consider e.g. control u and disturbance w as piecewise constant signals over a bounded time horizon.

Example

Dubbins vehicle

$$\begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{\theta} \end{pmatrix} = \begin{pmatrix} v cos(\theta) + b_1 \\ v sin(\theta) \\ a \end{pmatrix}$$

- Control period of $t = 0.5$, linear velocity $v = 1$,
- Initial conditions:
  $\mathbb{X}_0 = \{(x, y, \theta) \mid x \in [-0.1, 0.1], \; y \in [-0.1, 0.1], \; \theta \in [-0.01, 0.01]\}$,
- Control a (angular velocity) in $\mathbb{U} = [-0.01, 0.01]$,
- disturbance b_1 in $\mathbb{W} = [-0.01, 0.01]$

We want to estimate:

$$R_{\exists\forall\exists}(\varphi) = \{z \in \mathbb{R}^m \mid \exists u \in \mathbb{U}, \; \exists x_0 \in \mathbb{X}_0, \; \forall w \in \mathbb{W}, \; \exists s \in [0, T], \; z = \varphi(s; x_0, u, w)\}$$

First step: scalar affine functions

Notations

f is the affine function:

$$f(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{2n}) = \delta_0 + \langle \Delta_1, \boldsymbol{x}_1 \rangle + \langle \Delta_2, \boldsymbol{x}_2 \rangle + \ldots + \langle \Delta_{2n}, \boldsymbol{x}_{2n} \rangle$$

with $\Delta_i = (\delta_{k_i+1}, \ldots, \delta_{k_{i+1}}) \in \mathbb{R}^{j_i}$, $i = 1, \ldots, 2n$, where $k_i = \sum_{l=1}^{i-1} j_l$.

Exact characterization

$$R_{\boldsymbol{p}}(f) = \delta_0 + \left[\sum_{k=1}^{n} (||\Delta_{2k-1}|| - ||\Delta_{2k}||) \, , \, \sum_{k=1}^{n} (||\Delta_{2k}|| - ||\Delta_{2k-1}||) \right]$$

if $||\Delta_{2l-1}|| \leq ||\Delta_{2l}|| + \sum_{k=l+1}^{n} (||\Delta_{2k}|| - ||\Delta_{2k-1}||)$ for $l = 1, \ldots, n$, otherwise $R_{\boldsymbol{p}}(f) = \emptyset$

The non-vacuity condition is paramount

Notations

Function f from $\mathbb{R}^2$ to $\mathbb{R}$, consider:

$$\begin{array}{rcl} R_{\forall\exists}(f) & = & \{z \mid \forall x_2,\ \exists x_1,\ z = f(x_1, x_2)\} \\ R_{\exists\forall}(f) & = & \{z \mid \exists x_1,\ \forall x_2,\ z = f(x_1, x_2)\} \end{array}$$

Difference between $\forall, \exists$ and $\exists, \forall$

We always have $R_{\exists\forall}(f) \subseteq R_{\forall\exists}(f)$, but, for any affine function $f(x_1, x_2) = a + bx_1 + cx_2$:

- If $c \neq 0$, $R_{\exists\forall}(f) = \emptyset$
- If $c = 0$, $R_{\exists\forall}(f) = [a - |b|, a + |b|] = R_{\forall\exists}(f)$,

The case of non-linear scalar functions

Notations

- Function $f: \mathbb{R}^p \to \mathbb{R}$, $\boldsymbol{p} = (j_1, \ldots, j_{2n})$ partition of the p arguments of f, $k_l = \sum_{i=1}^{l-1} j_i$, for $l = 1, \ldots, 2n+1$.
- Suppose we have p intervals $A_1, \ldots, A_p$, write $\boldsymbol{A}_i = (A_{k_i+1}, \ldots, A_{k_{i+1}}),\ i = 1, \ldots, 2n$ for the corresponding boxes in $\mathbb{R}^{j_i}$,
- Consider the set:

$$\mathcal{C}(\boldsymbol{A}_1, \ldots, \boldsymbol{A}_{2n}) = \{z \mid \forall \alpha_1 \in \boldsymbol{A}_1,\ \exists \alpha_2 \in \boldsymbol{A}_2, \ldots,$$

$$\forall \alpha_{2n-1} \in \boldsymbol{A}_{2n-1},\ \exists \alpha_{2n} \in \boldsymbol{A}_{2n},\ z = \sum_{j=1}^{2n} \alpha_j\}.$$

- And functions, for $j = 1, \ldots, p$:

$$h^{x_1, \ldots, x_{j-1}}(x_j) = f(x_1, \ldots, x_{j-1}, x_j, 0, \ldots, 0) - f(x_1, \ldots, x_{j-1}, 0, \ldots, 0)$$

The case of non-linear scalar functions

Characterization of $R_{\mathrm{p}}(f)$ through linearizations

Given inner and outer-approximations of the images of functions $h^{x_1,\dots,x_{j-1}}$, for $j = 1, \dots, p.$:

$$I_j \subseteq range(h^{x_1,\dots,x_{j-1}}) \subseteq O_j$$

Then, writing $\boldsymbol{I}_i = \prod_{j=k_i+1}^{k_{i+1}} [\underline{I}_j, \overline{I}_j]$, $\boldsymbol{O}_i = \prod_{j=k_i+1}^{k_{i+1}} [\underline{O}_j, \overline{O}_j]$, $i = 1, \dots, 2n$:

$$f(0,\dots,0)+\mathcal{C}(\boldsymbol{O}_1, \boldsymbol{I}_2, \dots, \boldsymbol{O}_{2n-1}, \boldsymbol{I}_{2n}) \subseteq R_{\boldsymbol{p}}(f) \subseteq f(0,\dots,0)+C(\boldsymbol{I}_1, \boldsymbol{O}_2, \dots, \boldsymbol{I}_{2n-1}, \boldsymbol{O}_{2n})$$

How do we find simple inner and outer-approximations of functions?

Generalized mean-value theorem

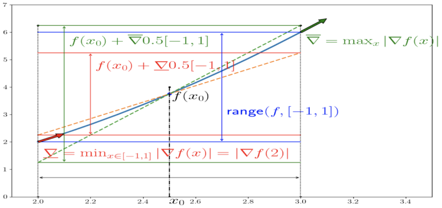
If we have, for all $i = 1, \ldots, 2n$ and all $j = k_i + 1, \ldots, k_{i+1}$, $\nabla_j = [\underline{\nabla}_j, \overline{\nabla}_j]$ such that:

$$\left\{ \left| \frac{\partial f}{\partial x_j}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_i, 0, \ldots, 0) \right| \mid \boldsymbol{x}_l \in [-1, 1]^{j_l},\ l = 1, \ldots, i \right\} \subseteq \nabla_j$$

then, for all $j = 1, \ldots, 2n$:

$$I_i = \underline{\nabla}_j[-1, 1], \quad O_j = \overline{\nabla}_j[-1, 1]$$

give inner and outer-approximations of $range(h^{x_1, \cdots, x_{j-1}})$



(other approximation methods, higher-order in particular, see e.g. Eric Goubault Sylvie Putot, "Tractable higher-order under-approximating AE extensions for non-linear systems" ADHS 2021)

Finally

General formula for scalar, general functions

$$f(0,\ldots,0) + \left[\sum_{k=1}^{n} \sum \left(\overline{\boldsymbol{O}}_{2k-1} + \underline{\boldsymbol{I}}_{2k}\right),\ \sum_{k=1}^{n} \sum \left(\overline{\boldsymbol{I}}_{2k} + \underline{\boldsymbol{O}}_{2k-1}\right)\right] \subseteq R_{\boldsymbol{p}}(f)$$

if $\sum \overline{\boldsymbol{O}}_{2l-1} - \sum \underline{\boldsymbol{O}}_{2l-1} \leq \sum_{k=l}^{n} \sum \left(\overline{\boldsymbol{I}}_{2k} - \underline{\boldsymbol{I}}_{2k}\right) - \sum_{k=l+1}^{n} \sum \left(\overline{\boldsymbol{O}}_{2k-1} - \underline{\boldsymbol{O}}_{2k-1}\right)$ for $l = 1, \ldots, n$, otherwise the inner-approximation is empty, and:

$$R_{\boldsymbol{p}}(f) \subseteq f(0,\ldots,0) + \left[\sum_{k=1}^{n} \sum \left(\overline{\boldsymbol{I}}_{2k-1} + \underline{\boldsymbol{O}}_{2k}\right),\ \sum_{k=1}^{n} \sum \left(\overline{\boldsymbol{O}}_{2k} + \underline{\boldsymbol{I}}_{2k-1}\right)\right]$$

if $\sum \overline{\boldsymbol{I}}_{2l-1} - \sum \underline{\boldsymbol{I}}_{2l-1} \leq \sum_{k=l}^{n} \sum \left(\overline{\boldsymbol{O}}_{2k} - \underline{\boldsymbol{O}}_{2k}\right) - \sum_{k=l+1}^{n} \sum \left(\overline{\boldsymbol{I}}_{2k-1} - \underline{\boldsymbol{I}}_{2k-1}\right)$ for $l = 1, \ldots, n$, otherwise the outer-approximation is empty.

Looks a bit intimidating...

Example, function $g : \mathbb{R}^3 \to \mathbb{R}$ on $[-1,1]^3$

$$g(x_1,x_2,x_3) = \frac{x_1^2}{4} + (x_2+1)(x_3+2) + (x_3+3)^2.$$

Compute $R_{\exists\forall\exists}(g) = \{z \mid \exists x_1 \in [-1,1],\ \forall x_2 \in [-1,1],\ \exists x_3 \in [-1,1], z = g(x_1,x_2,x_3)\}$

"Individual contributions" of each argument

- $\nabla_1 = |\frac{\partial g}{\partial x_1}| = |\frac{x_1}{2}| \in \left[0, \frac{1}{2}\right]$, $\nabla_2 = |\frac{\partial g}{\partial x_2}| = |x_3+2| \in [1,3]$, $\nabla_3 = |\frac{\partial g}{\partial x_3}| = |x_2+1+2(x_3+3)| \in [4,10]$, and $c = g(0,0,0) = 11$.
- Therefore, outer and inner approximations: $O_1 = \left[-\frac{1}{2}, \frac{1}{2}\right]$, $I_1 = 0$, $O_2 = [-3,3]$, $I_2 = [-1,1]$ and $O_3 = [-10,10]$, $I_3 = [-4,4]$.

Outer-approximation of $R_{\exists\forall\exists}(g)$

$$\begin{array}{ccccccccccc} [& c & +\underline{O}_1 & +\overline{I}_2 & +\underline{O}_3, & c & +\overline{O}_1 & +\underline{I}_2 & +\overline{O}_3 &] & \\ =[& 11 & -\frac{1}{2} & +1 & -10, & 11 & +\frac{1}{2} & -1 & +10 &] & = [1.5, 20.5] \end{array}$$

(in comparison, the sampling based estimation is $[6.25, 16.25]$)

Looks a bit intimidating...

Example, function $g : \mathbb{R}^3 \to \mathbb{R}$ on $[-1,1]^3$

Compute $R_{\exists\forall\exists}(g) = \{z \mid \exists x_1 \in [-1,1],\ \forall x_2 \in [-1,1],\ \exists x_3 \in [-1,1], z = g(x_1,x_2,x_3)\}$.

"Individual contributions" of each argument

- $\nabla_1 = |\frac{\partial g}{\partial x_1}| = |\frac{x_1}{2}| \in \left[0, \frac{1}{2}\right]$, $\nabla_2 = |\frac{\partial g}{\partial x_2}| = |x_3 + 2| \in [1,3]$, $\nabla_3 = |\frac{\partial g}{\partial x_3}| = |x_2 + 1 + 2(x_3+3)| \in [4,10]$, and $c = g(0,0,0) = 11$.
- Therefore, outer and inner approximations: $O_1 = \left[-\frac{1}{2}, \frac{1}{2}\right]$, $I_1 = 0$, $O_2 = [-3,3]$, $I_2 = [-1,1]$ and $O_3 = [-10,10]$, $I_3 = [-4,4]$.

Inner-approximation of $R_{\exists\forall\exists}(g)$

As $\overline{I}_3 + \underline{O}_2 = 1 \geq \underline{I}_3 + \overline{O}_2 = -1$:

$$\begin{array}{rcccccccccl} [& c & +\underline{I}_1 & +\overline{O}_2 & +\underline{I}_3, & c & +\overline{I}_1 & +\underline{O}_2 & +\overline{I}_3 &] & \\ =[& 11 & 0 & +3 & -4, & 11 & +0 & -3 & +4 &] & = [10,12] \end{array}$$

(in comparison, the sampling based estimation is $[6.25, 16.25]$)

Difference between ∀∃ and ∃∀ (II)

For function f from $\mathbb{R}^2$ to $\mathbb{R}$

$$\begin{aligned} R_{\forall\exists}(f) &= \{z \mid \forall x_2,\ \exists x_1,\ z = f(x_1, x_2)\} \\ R_{\exists\forall}(f) &= \{z \mid \exists x_1,\ \forall x_2,\ z = f(x_1, x_2)\} \end{aligned}$$

Recall, in any case, $R_{\exists\forall}(f) \subseteq R_{\forall\exists}(f)$

When f is non-linear, an example

- $f(x_1, x_2) = (x_1^2 - 1)x_2 + x_1$ for $x_1 \in [-1, 1]$ and $x_2 \in [-1, 1]$
- We have: $R_{\forall\exists}(f) = [-1, 1]$, which is a strict superset of $R_{\exists\forall}(f) = \{-1, 1\}$

(different than the linear case, where $R_{\forall\exists}(f)$ and $R_{\exists\forall}(f)$ would not agree only in the case when the latter is empty)

Dubbins example (II)

Direct computation from the ODE (no need for Taylor approximant)

- Outer-approximation of a "central trajectory" (x_c, y_c, θ_c) starting at $x = 0$, $y = 0$, $\theta = 0$, $b_1 = 0$ and $a = 0$: $x_c = t$, $y_c = 0$ and $\theta_c = 0$,
- $\frac{\partial x}{\partial t} = cos(\theta) + b_1 \in [0.989999965, 1.01]$ hence $I_{x,t} = [0, 0.494999982]$, $O_{x,t} = [0, 0.505]$,
- Similarly for the other variables: $I_{y,t} = 0$, $O_{y,t} = [-sin(0.015)/2, sin(0.015)/2] = [-1.309\ 10^{-4}, 1.309\ 10^{-4}]$ and $I_{\theta,t} = 0$, $O_{\theta,t} = [-0.005, 0.005]$,
- The Jacobian of φ with respect to x_0, y_0, θ_0, b_1 and a, satisfies a variational equation, we find:
  - $I_{x,a} = 0$, $O_{x,a} = [-6.545\ 10^{-7}, 6.545\ 10^{-7}]$, $I_{x,x_0} = O_{x,x_0} = [-0.1, 0.1]$, $I_{x,\theta_0} = 0$, $O_{x,\theta_0} = [-1.309\ 10^{-6}, 1.309\ 10^{-6}]$, $I_{x,b_1} = 0$, $O_{x,b_1} = [-0.005, 0.005]$,
  - $I_{y,a} = 0$, $O_{y,a} = [-0, 0025,\ 0.0025]$, $I_{y,y_0} = O_{y,y_0} = [-0.1, 0.1]$, $I_{y,\theta_0} = 0$, $O_{y,\theta_0} = [-0, 005, 0.005]$,
  - $I_{\theta,\theta_0} = O_{\theta,\theta_0} = [-0.01, 0.01]$, $I_{\theta,a} = 0$, $O_{\theta,a} = [0, 0.005]$,

Dubbins example (II)

Compute $R_{\exists\forall\exists}$:

$$\exists a \in [-0.01, 0.01],\ \exists x_0 \in [-0.1, 0.1],\ \exists y_0 \in [-0.1, 0.1],\\ \exists \theta_0 \in [-0.01, 0.01],\ \forall b_1 \in [-0.01, 0.01],\ \exists t \in [0, 0.5],\\ z = \varphi(t; x_0, y_0, \theta_0, a, b_1)$$

Hence, inner-approximation

Lower bound inner-approximation for x:

$$\begin{array}{ccccccc} x_c & +\underline{I}_{x,a} & +\underline{I}_{x,x_0} & +\underline{I}_{x,y_0} & +\underline{I}_{x,\theta_0} & +\overline{O}_{x,b_1} & +\underline{I}_{x,t} \\ = 0 & -0 & -0.1 & +0 & -0 & +0.005 & +0 \end{array}$$

which is equal to -0.095, and its upper bound:

$$\begin{array}{ccccccc} x_c & +\overline{I}_{x,a} & +\overline{I}_{x,x_0} & +\overline{I}_{x,y_0} & +\overline{I}_{x,\theta_0} & +\underline{O}_{x,b_1} & +\overline{I}_{x,t} \\ 0 & +0 & +0.1 & +0 & +0 & -0.005 & +0.494999982 \end{array}$$

which is equal to 0.589999982. Therefore the inner-approximation for x is equal to $[-0.095, 0.589999982]$.

Dubbins example (II)

Compute $R_{\exists\forall\exists}$:

$$\exists a \in [-0.01, 0.01],\ \exists x_0 \in [-0.1, 0.1],\ \exists y_0 \in [-0.1, 0.1],\\ \exists \theta_0 \in [-0.01, 0.01],\ \forall b_1 \in [-0.01, 0.01],\ \exists t \in [0, 0.5],\\ z = \varphi(t; x_0, y_0, \theta_0, a, b_1)$$

Hence, outer-approximation

Lower bound outer-approximation for the x:

$$\begin{array}{ccccccc} x_c & +\underline{O}_{x,a} & +\underline{O}_{x,x_0} & +\underline{O}_{x,y_0} & +\underline{O}_{x,\theta_0} & +\overline{I}_{x,b_1} & +\underline{O}_{x,t} \\ = 0 & -6.545\ 10^{-7} & -0.1 & +0 & -1.309\ 10^{-6} & +0 & +0 \end{array}$$

which is equal to -0.1000019635, and its upper bound:

$$\begin{array}{ccccccc} x_c & +\overline{O}_{x,a} & +\overline{O}_{x,x_0} & +\overline{O}_{x,y_0} & +\overline{O}_{x,\theta_0} & +\underline{I}_{x,b_1} & +\overline{O}_{x,t} \\ = 0 & +6.545\ 10^{-7} & +0.1 & 0 & +1.309\ 10^{-6} & -0 & +0.505 \end{array}$$

which is equal to 0.6050019635. Therefore the outer-approximation for x is equal to $[-0.1000019635, 0.6050019635]$.

Dubbins example (II)

Compute $R_{\exists\forall\exists}$:

$$\exists a \in [-0.01, 0.01],\ \exists x_0 \in [-0.1, 0.1],\ \exists y_0 \in [-0.1, 0.1],\\ \exists \theta_0 \in [-0.01, 0.01],\ \forall b_1 \in [-0.01, 0.01],\ \exists t \in [0, 0.5],\\ z = \varphi(t; x_0, y_0, \theta_0, a, b_1)$$

And...

- for y the inner-approximation $[-0.1, 0.1]$ and over-approximation $[0.1076309, 0.1076309]$,
- and for θ the inner-approximation $[-0.01,\ 0.01]$ and over-approximation $[-0.02, 0.02]$.

Very close to results obtained by quantifier elimination (Mathematica), here with a much smaller complexity.

Problematic

Example

Inner approximate $R_{\forall\exists\forall\exists}(f) = \{z \mid \forall x_1,\ \exists x_2,\ \exists x_3,\ \forall x_4,\ \exists x_5,\ \exists x_6, z = f(x)\}$?

- Outer-approximation of each component, separately, will give an outer-approximation of $R_{\forall\exists\forall\exists}(f)$
- But not for the inner-approximation!

Idea, for "joint" inner-approximation

- Conjunction of quantified formulas for each component if no variable is existentially quantified for several components.
- Transform the quantified formula by strengthening them for that objective

For example:

$$\forall x_1,\ \forall x_2,\ \boxed{\exists x_3},\ \forall x_4,\ \forall x_5,\ \boxed{\exists x_6},\ z_1 = f_1(x_1, x_2, x_3, x_4, x_5, x_6)$$
$$\forall x_1,\ \forall x_3,\ \boxed{\exists x_2},\ \forall x_4,\ \forall x_6,\ \boxed{\exists x_5},\ z_2 = f_2(x_1, x_2, x_3, x_4, x_5, x_6)$$

General theorem

More formally... and I am not going to go through this!

Let $f : \mathbb{R}^u \to \mathbb{R}^m$ be an elementary function and $\pi^i : \{k_{2i}+1, \ldots, k_{2i+1}\} \to \{1, \ldots, m\}$ for $i = 1, \ldots, n$. Let us note, for all $i \in \{1, \ldots n\}$, $j \in \{1, \ldots, m\}$ $J^i_{E,z_j} = \{l \in \{k_{2i}+1, \ldots, k_{2i+1}\},\ \pi^i(l) = j\}$ and $J^i_{A,z_j} = \{k_{2i-1}+1, \ldots, k_{2i}\} \setminus J_{E,z_i}$. Consider the following m quantified problems, $j \in \{1, \ldots, m\}$:

$$\forall z_j \in \boldsymbol{z}_j,\ (\forall \boldsymbol{x}_l \in [-1,1])_{l \in J^1_{A,z_j}},\ (\exists \boldsymbol{x}_l \in [-1,1])_{l \in J^1_{E,z_j}}, \ldots$$
$$(\forall \boldsymbol{x}_l \in [-1,1])_{l \in J^n_{A,z_j}},\ (\exists x_j \in [-1,1])_{l \in J^n_{E,z_j}},\ z_i = f_i(x_1, \ldots, x_{k_{2n}})$$

Then $\boldsymbol{z} = \boldsymbol{z}_1 \times \boldsymbol{z}_2 \times \ldots \times \boldsymbol{z}_n$, if non-empty, is an inner-approximation of $R_{\boldsymbol{p}}(f)$.

Example

Consider $f = (f_1, f_2) : \mathbb{R}^4 \to \mathbb{R}^2$:

$$\begin{array}{rcl} f_1(x_1, x_2, x_3, x_4) & = & 2 + 2x_1 + x_2 + 3x_3 + x_4 \\ f_2(x_1, x_2, x_3, x_4) & = & -1 - x_1 - x_2 + x_3 + 5x_4 \end{array}$$

And compute:

$$R_{\exists\forall\exists}(f) = \{z \in \mathbb{R}^2 | \exists x_1 \in [-1,1],\ \forall x_2 \in [-1,1],\ \exists x_3 \in [-1,1],\ \exists x_4 \in [-1,1],\ z = f(x_1, x_2, x_3, x_4)\}$$

Same calculation as before, 1 component at a time: $R_{\exists\forall\exists}(f) \subseteq [-3,7] \times [-7,5]$.

For the joint inner-approximation, interpret:

$$\boxed{\exists x_1},\ \forall x_2,\ \forall x_3,\ \boxed{\exists x_4},\ z_1 = f_1(x_1, x_2, x_3, x_4)$$
$$\forall x_1,\ \forall x_2,\ \forall x_4,\ \boxed{\exists x_3},\ z_2 = f_2(x_1, x_2, x_3, x_4)$$

Empty set for z_1 already: contribution of the existentially quantified x_4 is $[-1,1]$ whereas the universally quantified x_2 and x_3 account for $[-4,4]$, which thus cannot be fully compensated

Example

Consider $f = (f_1, f_2) : \mathbb{R}^4 \to \mathbb{R}^2$:

$$\begin{aligned} f_1(x_1, x_2, x_3, x_4) &= 2 + 2x_1 + x_2 + 3x_3 + x_4 \\ f_2(x_1, x_2, x_3, x_4) &= -1 - x_1 - x_2 + x_3 + 5x_4 \end{aligned}$$

And compute:

$$R_{\exists\forall\exists}(f) = \{z \in \mathbb{R}^2 | \exists x_1 \in [-1,1],\ \forall x_2 \in [-1,1],\ \exists x_3 \in [-1,1], \\ \exists x_4 \in [-1,1],\ z = f(x_1, x_2, x_3, x_4)\}$$

For the joint inner-approximation, interpret:

$$\boxed{\exists x_1},\ \forall x_2,\ \forall x_4,\ \boxed{\exists x_3},\ z_1 = f_1(x_1, x_2, x_3, x_4)$$

$$\forall x_1,\ \forall x_2,\ \forall x_3,\ \boxed{\exists x_4},\ z_2 = f_2(x_1, x_2, x_3, x_4)$$

$$\begin{aligned} z_1 &= [\, z_1^c - ||\Delta_{x_1}|| + ||\Delta_{x_2,x_4}|| - ||\Delta_{x_3}||,\ z_1^c + ||\Delta_{x_1}|| - ||\Delta_{x_2,x_4}|| + ||\Delta_{x_3}||] \\ &= [\ 2 \quad -2 \quad +1+1 \quad -3,\quad 2 \quad +2 \quad -1-1 \quad +3] = [-1, 5] \end{aligned}$$

Example

Consider $f = (f_1, f_2) : \mathbb{R}^4 \to \mathbb{R}^2$:

$$\begin{array}{rcl} f_1(x_1, x_2, x_3, x_4) & = & 2 + 2x_1 + x_2 + 3x_3 + x_4 \\ f_2(x_1, x_2, x_3, x_4) & = & -1 - x_1 - x_2 + x_3 + 5x_4 \end{array}$$

And compute:

$$R_{\exists\forall\exists}(f) = \{z \in \mathbb{R}^2 | \exists x_1 \in [-1,1],\ \forall x_2 \in [-1,1],\ \exists x_3 \in [-1,1],\ \exists x_4 \in [-1,1],\ z = f(x_1, x_2, x_3, x_4)\}$$

For the joint inner-approximation, interpret:

$$\boxed{\exists x_1},\ \forall x_2,\ \forall x_4,\ \boxed{\exists x_3},\ z_1 = f_1(x_1, x_2, x_3, x_4)$$
$$\forall x_1,\ \forall x_2,\ \forall x_3,\ \boxed{\exists x_4},\ z_2 = f_2(x_1, x_2, x_3, x_4)$$

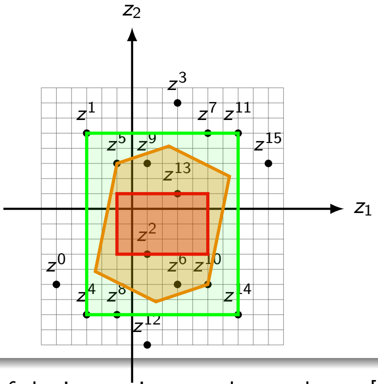
$$\begin{array}{rl} z_2 = & [\ z_2^c\ + \|\Delta_{x_1,x_2,x_4}\| - \|\Delta_{x_3}\|,\ z_1^c\ - \|\Delta_{x_1,x_2,x_4}\| \quad + \|\Delta_{x_3}\|] \\ = & [\ \ -1\ \ +1+1+1 \quad -5, \quad -1\ \ -1-1-1\ \ +5] = [-3,1] \end{array}$$

Hence $[-1,5] \times [-3,1] \subseteq R_{\exists\forall\exists}(f) \subseteq [-3,7] \times [-7,5]$.

Example, in picture

$$
\begin{aligned}
f_1(x_1,x_2,x_3,x_4) &= 2+2x_1+x_2+3x_3+x_4\\
f_2(x_1,x_2,x_3,x_4) &= -1-x_1-x_2+x_3+5x_4
\end{aligned}
$$

$$R_{\exists\forall\exists}(f)=\{z\in\mathbb{R}^2|\exists x_1,\ \forall x_2,\ \exists x_3,\exists x_4,\ z=f(x_1,x_2,x_3,x_4)\}$$



(some particular points of the image; inner and outer boxes $[-1,5]\times[-3,1]$ and $[-3,7]\times[-7,5]$; polyhedron lying in between is the exact robust image)

Last application: Dubbins!

Space relaxation

$$R_{\exists\forall\exists}(\varphi) = \{(x, y, \theta) \mid \exists a \in [-0.01, 0.01],\ \exists x_0 \in [-0.1, 0.1],\\ \exists y_0 \in [-0.1, 0.1],\ \exists \theta_0 \in [-0.01, 0.01],\ \forall b_1 \in [-0.01, 0.01],\\ \exists t \in [0, 0.5],\ \exists \delta_2 \in [-1.309\ 10^{-4}, 1.309\ 10^{-4}],\ \exists \delta_3 \in [-0.005, 0.005],\\ (x, y, \theta) = \varphi(t; x_0, y_0, \theta_0, a, b_1) + (0, \delta_2, \delta_3)\}$$

Outer-approximation

$$R_{\exists\forall\exists}(\varphi) \subseteq [-0.1000019635, 0.6050019635] \times\\ [0.1077618, 0.1077618] \times [-0.025, 0.025]$$

Last application: Dubbins!

$$R_{\exists\forall\exists}(\varphi) = \{(x, y, \theta) \mid \exists a \in [-0.01, 0.01],\ \exists x_0 \in [-0.1, 0.1],\ \exists y_0 \in [-0.1, 0.1],\ \exists \theta_0 \in [-0.01, 0.01],\ \forall b_1 \in [-0.01, 0.01],\ \exists t \in [0, 0.5],\ \exists \delta_2 \in [-1.309\ 10^{-4}, 1.309\ 10^{-4}],\ \exists \delta_3 \in [-0.005, 0.005],\ (x, y, \theta) = \varphi(t; x_0, y_0, \theta_0, a, b_1) + (0, \delta_2, \delta_3)\}$$

For the inner-approximation, interpret:

$$\forall a,\ \forall y_0, \forall \theta_0,\ \boxed{\exists x_0},\ \forall b_1,\ \forall \delta_2,\ \forall \delta_3,\ \boxed{\exists t},\ x = \varphi_x(t; x_0, y_0, \theta_0, a, b_1)$$

$$\forall a,\ \forall x_0, \forall \theta_0,\ \boxed{\exists y_0},\ \forall b_1,\ \forall \delta_3,\ \forall t,\ \boxed{\exists \delta_2},\ y = \varphi_y(t; x_0, y_0, \theta_0, a, b_1) + \delta_2$$

$$\forall x_0,\ \forall y_0, \boxed{\exists \theta_0,\ \exists a},\ \forall b_1,\ \forall \delta_2,\ \forall t,\ \boxed{\exists \delta_3},\ \theta = \varphi_\theta(t; x_0, y_0, \theta_0, a, b_1) + \delta_3$$

$$[-0.0949993455, 0.5899993275] \times [-0.0925, 0.0925] \times [-0.01, 0.01] \subseteq R_{\exists\forall\exists}(\varphi)$$

(timeout using quantifier elimination under Mathematica)

Table of Contents

Conclusion and future work

- Higher-order approximations for generalized quantified problems (there is already an order 1 method, generalizing the order 0 method we presented)
- Full application of generalized quantified problems to STL
- General quantified problems and applications to viability
- Larger classes of systems (hybrid/switched, DDEs as in CAV 2018, neural net controllers as in CAV 2022 etc.)

Check out `https://github.com/cosynus-lix/RINO` !

Any questions?

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