CTRLVERIF. Analysis of control systems

Lecture 4. Inner- and outer-approximation of general quantified expressions

Eric Goubault and Sylvie Putot

MPRI

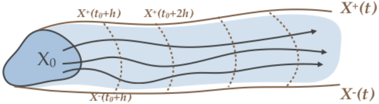
Outline

1. Taylor-based inner and outer reachability of continuous systems
   - A quick reminder on Taylor methods for nonlinear system reachability
   - Mean-value AE extensions for function image: the scalar case
   - Application to the solution of uncertain dynamical systems
2. Joint inner range and robust reachability
   - From range projection to joint inner range
   - Reachability problems for systems with inputs
   - Robust Mean Value theorem
3. Refining the approximations
   - Refinement by local quadrature
   - Higher-order AE extensions
4. Arbitrarily quantified reachability problems

Taylor-based inner and outer reachability of continuous systems

Remember: Taylor methods for nonlinear system reachability

Compute tubes of trajectories $[x](t)$, or flow-pipes, guaranteed to enclose all trajectories of system $\dot{x}(t) = f(x,t),\ x(t_0) \in [x_0]$



For $f \in C^k$, over-approximate the solution of $\dot{x}(t) = f(x(t)),\ x(t_0) \in [x_0]$ on $[t_0, T]$:

- Time grid $t_0 < t_1 < \ldots < t_N = T$
- Taylor-Lagrange expansion in t of the solution on each time slice $[t_j, t_{j+1}]$

$$x(t) = x(t_j) + \sum_{i=1}^{k-1} \frac{(t-t_j)^i}{i!} \frac{d^i x}{dt^i}(t_j) + \frac{(t-t_j)^k}{k!} \frac{d^k x}{dt^k}(t_j + \theta h),\ 0 < \theta < 1$$

- initial value $x(t_j) \in [x_j]$ given by Taylor expansion on previous time slice $[t_{j-1}, t_j]$, evaluated at time t_j
- coefficients of the expansion computed using that x is solution of $\dot{x}(t) = f(x,t)$

Set-valued computations: evaluation with intervals, *affine forms / zonotopes*, etc.

Taylor expansion based method for nonlinear ODE reachability

- Taylor-Lagrange expansion of the exact solution, valid for $t \in [t_j, t_j + h]$:

$$x(t) = x(t_j) + \sum_{i=1}^{k-1} \frac{(t-t_j)^i}{i!} \frac{d^i x}{dt^i}(t_j) + \frac{(t-t_j)^k}{k!} \frac{d^k x}{dt^k}(t_j + \theta h),\ 0 < \theta < 1$$

  with initial value given by Taylor expansion on previous time slice $[t_{j-1}, t_j]$, evaluated at time t_j: $x(t_j) \in [x_j] = [x]_{j-1}([x_{j-1}], t_j)$
- Coefficients are computed using that x is solution of $\dot{x}(t) = f(x, t)$:

$$\frac{dx}{dt}([x_j], t_j) = L_f^1([x_j], t_j) = \{f(x_j, t_j),\ x_j \in [x_j]\}$$

$$\frac{d^2x}{dt^2}([x_j], t_j) = L_f^2([x_j], t_j) = \{\frac{d}{dt}(f(x_j, t_j)),\ x_j \in [x_j]\} = \{\langle \frac{\partial f}{\partial x}.f\rangle(x_j, t_j),\ x_j \in [x_j]\}$$

$$\frac{d^i x}{dt^i}([x_j], t_j) = L_f^i([x_j], t_j) = \{\langle \frac{\partial L_f^{i-1}}{\partial x}.f\rangle(x_j, t_j),\ x_j \in [x_j]\}$$

  Defined inductively, can be computed efficiently by automatic differentiation

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

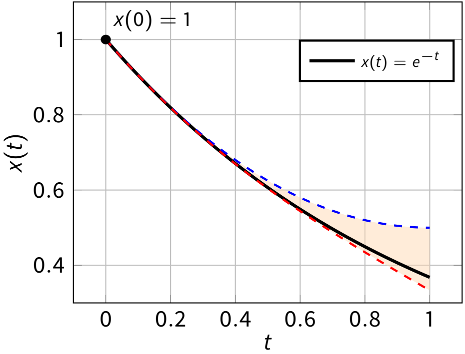
- Last coefficient a priori unknown: we need an a priori enclosure $[\boldsymbol{r}_{j+1}]$ of $x(t), t \in]t_j, t_j + h[$ (Lohner's method, based on Picard iteration).
- Initialization of next iterate $[\boldsymbol{x}_{j+1}] = [\boldsymbol{x}]_j([\boldsymbol{x}_j], t_{j+1})$

Example (exercise): $\dot{x} = -x$, with $x(0) = 1$

Compute Taylor Model of order 3 valid on t=[0,1] and deduce bounds for $x(1)$

Example (exercise): $\dot{x} = -x$, with $x(0) = 1$

Compute Taylor Model of order 3 valid on t=[0,1] and deduce bounds for $x(1)$



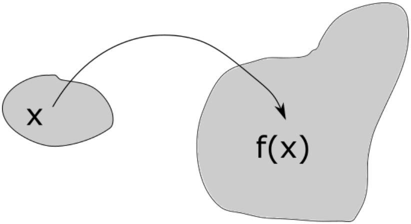
Remember: AE extensions for function image computation

Given

- $f : \mathbb{R}^m \to \mathbb{R}^n$
- a set $\boldsymbol{x}$ in $\mathcal{P}(\mathbb{R}^m)$

we want:

range$(f, \boldsymbol{x}) = \{f(x), x \in \boldsymbol{x}\}$.



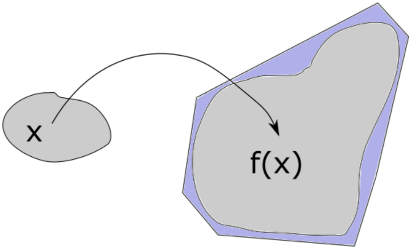
Remember: AE extensions for function image computation

Given

- $f : \mathbb{R}^m \to \mathbb{R}^n$
- a set $\boldsymbol{x}$ in $\mathcal{P}(\mathbb{R}^m)$

we want:

range$(f, \boldsymbol{x}) = \{f(x), x \in \boldsymbol{x}\}$.



- Over-approximating extension of f (or inclusion function):
  $\boldsymbol{f}_o : \mathcal{P}(\mathbb{R}^m) \to \mathcal{P}(\mathbb{R}^n)$ such that $\forall \boldsymbol{x}$ in $\mathcal{P}(\mathbb{R}^m)$, range$(f, \boldsymbol{x}) \subseteq \boldsymbol{f}_o(\boldsymbol{x})$

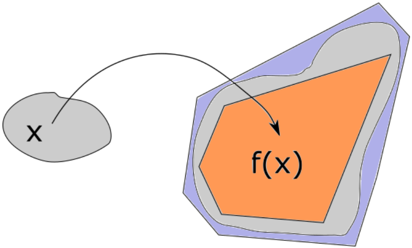
Remember: AE extensions for function image computation

Given

- $f : \mathbb{R}^m \to \mathbb{R}^n$
- a set $\boldsymbol{x}$ in $\mathcal{P}(\mathbb{R}^m)$

we want:

range$(f, \boldsymbol{x}) = \{f(x), x \in \boldsymbol{x}\}$.



- Over-approximating extension of f (or inclusion function):
  $\boldsymbol{f}_o : \mathcal{P}(\mathbb{R}^m) \to \mathcal{P}(\mathbb{R}^n)$ such that $\forall \boldsymbol{x}$ in $\mathcal{P}(\mathbb{R}^m)$, range$(f, \boldsymbol{x}) \subseteq \boldsymbol{f}_o(\boldsymbol{x})$
- Under-approximating extension of f:
  $\boldsymbol{f}_u : \mathcal{P}(\mathbb{R}^m) \to \mathcal{P}(\mathbb{R}^n)$ such that $\forall \boldsymbol{x}$ in $\mathcal{P}(\mathbb{R}^m)$, $\boldsymbol{f}_u(\boldsymbol{x}) \subseteq$ range$(f, \boldsymbol{x})$

Remember: AE extensions for function image computation

- Over-approximating extension of f (or inclusion function):
  $\boldsymbol{f}_o : \mathcal{P}(\mathbb{R}^m) \rightarrow \mathcal{P}(\mathbb{R}^n)$ such that $\forall \boldsymbol{x}$ in $\mathcal{P}(\mathbb{R}^m)$, $\text{range}(f, \boldsymbol{x}) \subseteq \boldsymbol{f}_o(\boldsymbol{x})$
- Under-approximating extension of f:
  $\boldsymbol{f}_u : \mathcal{P}(\mathbb{R}^m) \rightarrow \mathcal{P}(\mathbb{R}^n)$ such that $\forall \boldsymbol{x}$ in $\mathcal{P}(\mathbb{R}^m)$, $\boldsymbol{f}_u(\boldsymbol{x}) \subseteq \text{range}(f, \boldsymbol{x})$

Can be interpreted as AE propositions = quantified propositions where universal quantifiers (A) precede existential quantifiers (E)

$$\text{range}(f, \boldsymbol{x}) \subseteq \boldsymbol{z} = \boldsymbol{f}_o(\boldsymbol{x}) \Leftrightarrow \forall x \in \boldsymbol{x}, \exists z \in \boldsymbol{z}, f(x) = z$$

$$\boldsymbol{f}_u(\boldsymbol{x}) = \boldsymbol{z} \subseteq \text{range}(f, \boldsymbol{x}) \Leftrightarrow \forall z \in \boldsymbol{z}, \exists x \in \boldsymbol{x}, f(x) = z$$

Mean-Value AE extensions (scalar-valued function)

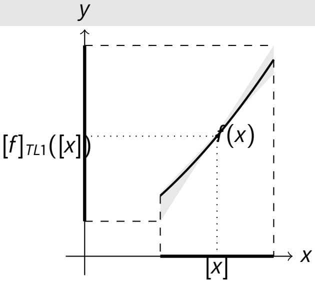
Theorem (Generalized Interval Mean-Value Theorem,Goldsztejn 2012)

- $f : \mathbb{R}^m \to \mathbb{R}$ *be a continuously differentiable function,* $\boldsymbol{x}$ *an initial box of* $\mathbb{R}^m$,
- $x_0 = mid(\boldsymbol{x})$ *the center of the box x,* $\boldsymbol{f}_0 = [\underline{f_0}, \overline{f_0}]$ *such that* $f(x_0) \in \boldsymbol{f}_0$
- $\Delta_i = [\underline{\Delta_i}, \overline{\Delta_i}]$ *such that* $\{|f_i'(x_{0,1}, \ldots, x_{0,i-1}, x_i, \ldots, x_m)|,\ x \in \boldsymbol{x}\} \subseteq \Delta_i$

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

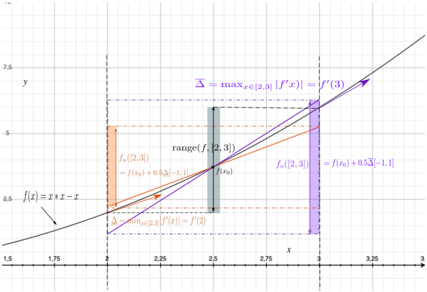
$$[\overline{f_0} - \sum_{i=1}^{m} \underline{\Delta_i} radius(\boldsymbol{x}_i), \underline{f_0} + \sum_{i=1}^{m} \underline{\Delta_i} radius(\boldsymbol{x}_i)] \subseteq range(f, \boldsymbol{x})$$

- Interval abstractions of $f(x) = f(x_0) + \int_{x_0}^{x} f'(x)dx,\ x \in \boldsymbol{x}$
- For over-approximation = centered mean-value extension



Example

- $f(x) = x^2 - x$ over $\boldsymbol{x} = [2, 3]$
- $f(2.5) = 3.75$
- $|\boldsymbol{f}'([2, 3])| \subseteq [3, 5] = [\underline{\Delta}, \overline{\Delta}]$.



Then,

$$3.75 + 0.5 * 3 * [-1, 1] \subseteq \text{range}(f, [2, 3]) \subseteq 3.75 + 0.5 * 5 * [-1, 1]$$

from which we deduce $[2.25, 5.25] \subseteq \text{range}(f, [2, 3]) \subseteq [1.25, 6.25]$.

Inner-approx. for ODEs with uncertain initial condition

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 $\tilde{z}_0 \in [z_0]$ and

$\left\{ |\frac{\partial z}{\partial z_{0,i}}|(t, z_0),\ z_0 \in [z_0] \right\} \subseteq [\boldsymbol{J}_i]$: Taylor models

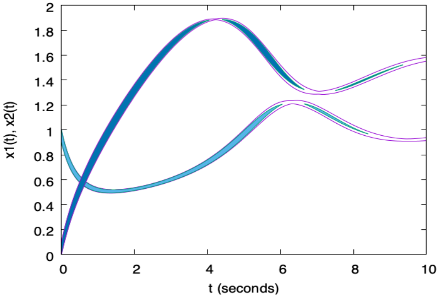
Algorithm (Init: $j = 0$, $t_j = t_0$, $[\boldsymbol{z}_j] = [\boldsymbol{z}_0]$, $[\tilde{z}_j] = \tilde{z}_0 \in [\boldsymbol{z}_0]$, $[\boldsymbol{J}_j] = Id$)

- 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 $|\frac{\partial z}{\partial z_0}|(t, [z_0])$
- Deduce an inner-approximation valid for t in $[t_j, t_{j+1}]$ if the following is non-empty :

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

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

Brusselator system (Taylor Models order 4)



$$\begin{cases} \dot{x}_1 = 1 + x_1^2 x_2 - 2.5x_1 \\ \dot{x}_2 = 1.5x_1 - x_1^2 x_2 \end{cases}$$

$$x_1(0) \in [0.9, 1], x_2(0) \in [0, 0.1]$$

The inner-approximation is deduced at each time instant from outer-approximations:

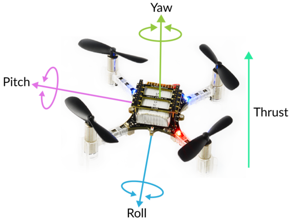
- Any outer-approximating method can be used to bound the flow and its Jacobian
- The outer-approximations can be safely evaluated with outward rounding (the larger these bounds, the smaller the inner-approximation)
- The conservativeness in the inner-approximation does not propagate

Application: Quadcopter Dynamics (nominal mode)

Model

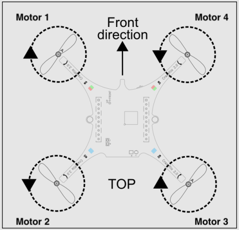
$$\begin{cases} \dot{z} = -s_\theta u + c_\theta s_\phi v + c_\theta c_\phi w & \dot{\theta} = c_\phi q - s_\phi r \\ \dot{u} = rv - qw + s_\theta g & \dot{\psi} = \frac{c_\phi}{c_\theta} r + \frac{s_\phi}{c_\theta} q \\ \dot{v} = -ru + pw - c_\theta s_\phi g & \dot{p} = \frac{I_y - I_z}{I_x} qr + \frac{1}{I_x} M_x \\ \dot{w} = qu - pv - c_\theta c_\phi g + \frac{F}{m} & \dot{q} = \frac{I_z - I_x}{I_y} pr + \frac{1}{I_y} M_y \\ \dot{\phi} = p + c_\phi t_\theta r + t_\theta s_\phi q & \dot{r} = \frac{I_x - I_y}{I_z} pq + \frac{1}{I_z} M_z \end{cases}$$

- z: vertical position in the world frame,
- (u, v, w): linear velocity of CoG in body-fixed frame wrt inertial frame
- (ϕ, θ, ψ): angular orientation (roll, pitch, yaw),
- (p, q, r): roll, pitch and yaw rate wrt body frame
- F: sum of individual motor thrusts, I_x, I_y, I_z: quadcopter's inertial moments around x, y, z.



Modelling and control

- four commands *thrust*, cmd_ϕ, cmd_ψ and cmd_θ instead of PWM.
- From which we deduce the input force and moments from the squared rotation rates, with force and momentum equations equal to:

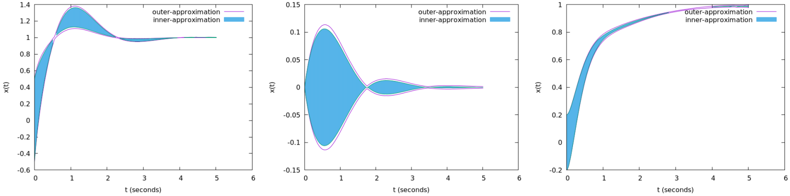


Motors' controls

$$\begin{bmatrix} F \\ M_x \\ M_y \\ M_z \end{bmatrix} = \begin{bmatrix} C_T\left(C_1^2(cmd_\theta^2 + cmd_\phi^2 + 4cmd_\psi^2 + 4thrust^2) + 8C_1C_2thrust + 4C_2^2\right) \\ 4C_Td\left(C_1^2(cmd_\phi thrust - cmd_\theta cmd_\psi) + C_1C_2cmd_\phi\right) \\ 4C_Td\left(C_1^2(cmd_\theta thrust - cmd_\phi cmd_\psi) + C_1C_2cmd_\theta\right) \\ 2C_D\left(C_1^2(4cmd_\psi thrust - cmd_\phi cmd_\theta) + 4C_1C_2cmd_\psi\right) \end{bmatrix}$$

Reachability results on the quadcopter

Takes 6.3 seconds with Taylor models of order 5

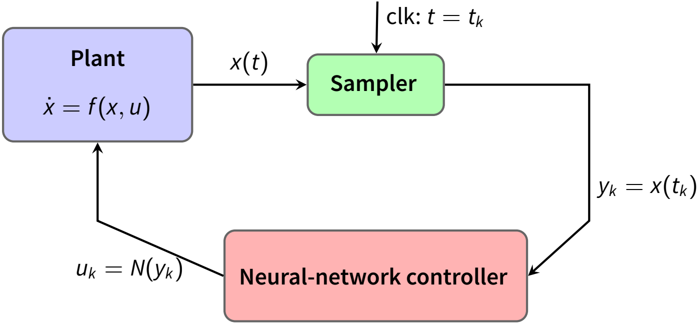


(a) Roll rate p **(b)** Roll ϕ **(c)** Altitude z

Neural network controlled systems

$$\dot{x}(t) = f(x(t), u(t), w(t))$$
$$x(t_0) = x_0 \in \mathcal{X}_0$$
$$u(t) = u_k = h(y(x(\tau_k))), \text{ for } t \in [\tau_k, \tau_{k+1}), \text{ with } \tau_k = t_0 + k\Delta t_u, \ \forall k \geq 0$$

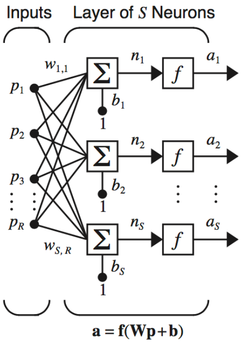
Taylor model (zonotope coeff)

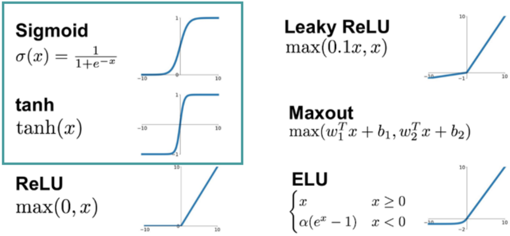


Zonotope

Feedforward neural network controlled system

Each layer consists in a linear transform followed by a non linear activation function:





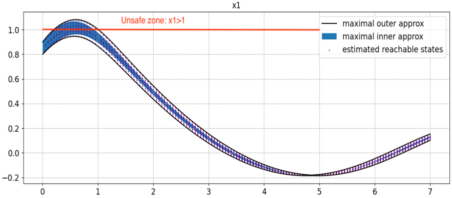
We focus on differentiable activation functions (needed for inner-approximations)

Taylor expansions in time for vector field $f(x(t), h(x(\tau_k)))$ and its Jacobian wrt initial states and uncertainties: implies differentiating h, using $tanh'(x) = 1.0 - tanh(x)^2$ and $sig'(x) = sig(x)(1 - sig(x))$.

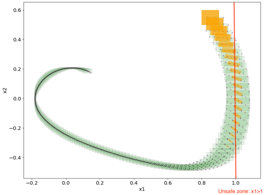
Example: sampling (purple dots) and inner/outer-approximations

$$\dot{x}_1 = x_2$$
$$\dot{x}_2 = u x_2^2 - x_1$$

where control u given by NN 3×20 nodes with sigmoid activation



(a) x_1 as function of time



(b) Joint range (x_1, x_2)

- Over-approximation is very tight
- Samples show $(x1, x2)$ becomes almost a 1-dim curve: inner-approx difficult!
- N-dim inner-approximation more difficult and imprecise than 1-dim inner-approx

Property $x_1 < 1$ (red line):

- over-approx raises an alarm
- under-approx proves falsification

Joint inner range and robust reachability

Vector-valued functions: from range projection to joint inner range

Product of 1-dim approximations as n-dim approximation?

- Products of 1-dim over-approx. are n-dim over-approx.
- Generally false for under-approximations! Take $(z_1, z_2) = (f_1(x_1, x_2), f_2(x_1, x_2))$ and

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

Problem: does not imply $\forall z_1 \in \boldsymbol{z}_1$ and $\forall z_2 \in \boldsymbol{z}_2, \exists x_1 \in \boldsymbol{x}_1$ and $\exists x_2 \in \boldsymbol{x}_2$ such that $z = f(x)$.
The reason is that a witness for $\exists x_i$ may not be the same for each component of f

Vector-valued functions: from range projection to joint inner range

Product of 1-dim approximations as n-dim approximation?

- Products of 1-dim over-approx. are n-dim over-approx.
- Generally false for under-approximations! Take $(z_1, z_2) = (f_1(x_1, x_2), f_2(x_1, x_2))$ and

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

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

Problem: does not imply $\forall z_1 \in \boldsymbol{z}_1$ and $\forall z_2 \in \boldsymbol{z}_2, \exists x_1 \in \boldsymbol{x}_1$ and $\exists x_2 \in \boldsymbol{x}_2$ such that $z = f(x)$.
The reason is that a witness for $\exists x_i$ may not be the same for each component of f

A simple relaxation:

- such that no variable is existentially quantified in several components
- strengthen the quantified formula: robust inner-approximations

Suppose we can compute $\boldsymbol{z}_1$ and $\boldsymbol{z}_2$ with continuous selections x_2 and x_1 such that

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

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

By Brouwer fixpoint thm: $\boxed{\boldsymbol{z}_1 \times \boldsymbol{z}_2 \subseteq range(f, \boldsymbol{x}_1 \times \boldsymbol{x}_2)}$
(an inner box $\rightarrow$ parallelepiped by preconditioning)

Reachability with Inputs

Reachability questions for hybrid systems with inputs:

1. Viability
   - does there exist a choice for the inputs u such that the executions of the system remain in a given set?
   - inputs as controls that can be used to steer the system in the set
2. Invariance
   - do the executions of the system remain in a given set for all choices of u?
   - inputs as uncontrollable disturbances that can steer the system outside the desired set
3. Gaming.
   - does there exist a choice for the controls, such that despite the action of the disturbances the execution of the system remain is a given set?
   - some of the input variables are controls, while others are disturbances.

Reachability problems for systems with inputs

- Maximal reachability: looking for input signals u that maximize the reachable set

$$I_{\mathcal{E}}(t) \subseteq R^{f,h}_{\mathcal{E}}(t; \mathbb{X}_0, \mathbb{U}) = \{x \mid \exists u \in \mathbb{U}, \exists x_0 \in \mathbb{X}_0,\ x = \varphi^{f,h}(t; x_0, u)\} \subseteq O_{\mathcal{E}}(t)$$

- Minimal reachability: states that trajectories will reach for any input signal w

$$I_{\mathcal{A}}(t) \subseteq R^{f,h}_{\mathcal{A}}(t; \mathbb{X}_0, \mathbb{W}) = \{x \mid \forall w \in \mathbb{W}, \exists x_0 \in \mathbb{X}_0,\ x = \varphi^{f,h}(t; x_0, w)\} \subseteq O_{\mathcal{A}}(t)$$

- Robust reachability: states reachable robustly to disturbances on components w:

$$R^{f}_{\mathcal{A}\mathcal{E}}(t; \mathbb{X}_0, \mathbb{W}, \mathbb{U}) = \{x \in \mathcal{D} \mid \forall w \in \mathbb{W}, \exists u \in \mathbb{U}, \exists x_0 \in \boldsymbol{x}_0,\ x = \varphi^{f}(t; x_0, w, u)\}$$

We have: $R^{f,h}_{\mathcal{A}}(t; \mathbb{X}_0, \mathbb{W}) \subseteq R^{f,h}_{\mathcal{A}\mathcal{E}}(t; \mathbb{X}_0, \mathbb{W}) \subseteq R^{f,h}_{\mathcal{E}}(t; \mathbb{X}_0, \mathbb{W})$

Robustly reachable sets

Robust range: states reachable whatever the disturbances on components $w \in \boldsymbol{x}_A$

$$\text{range}_{\mathcal{A}\mathcal{E}}(f, \boldsymbol{x}_{\mathcal{A}}, \boldsymbol{x}_{\mathcal{E}}) = \{z \,|\, \forall w \in \boldsymbol{x}_{\mathcal{A}}, \exists u \in \boldsymbol{x}_{\mathcal{E}},\ z = f(w, u)\} \subseteq \text{range}(f, \boldsymbol{x})$$

Robustly reachable sets

Robust range: states reachable whatever the disturbances on components $w \in \boldsymbol{x}_A$

$$\text{range}_{\mathcal{A}\mathcal{E}}(f, \boldsymbol{x}_{\mathcal{A}}, \boldsymbol{x}_{\mathcal{E}}) = \{z \mid \forall w \in \boldsymbol{x}_{\mathcal{A}}, \exists u \in \boldsymbol{x}_{\mathcal{E}},\ z = f(w,u)\} \subseteq \text{range}(f, \boldsymbol{x})$$

A particular case of robust reachability for dynamical systems with disturbances/inputs

$$(S_c) \begin{cases} \dot{x}(t) = f(x(t), u(t)) \\ x(0) \in \boldsymbol{x}_0, u(t) \in \mathbb{U} \subseteq \mathbb{R}^p \end{cases} \qquad (S_d) \begin{cases} x^{k+1} = f(x^k, u^k) \\ x^0 \in \boldsymbol{x}^0, u(k) \in \mathbb{U} \subseteq \mathbb{R}^p \end{cases}$$

flow $\varphi^f(t; x_0, u)$

Sets reachable robustly to disturbances on components u_A:

$$R^f_{\mathcal{A}\mathcal{E}}(t; \boldsymbol{x}_0, \mathbb{U}) = \{x \in \mathcal{D} \mid \forall u_A \in \mathbb{U}_{\mathbb{A}}, \exists u_E \in \mathbb{U}_{\mathbb{E}}, \exists x_0 \in \boldsymbol{x}_0,\ x = \varphi^f(t; x_0, u_A, u_E)\}$$

- u_A can be seen as disturbance, u_E as control
- (classical) maximal reachability for $\mathbb{U}_{\mathbb{A}} = \emptyset$, minimal reachability for $\mathbb{U}_{\mathbb{E}} = \emptyset$

Robust Mean Value theorem

$$\mathrm{range}_{\mathcal{AE}}(f, \boldsymbol{x}_{\mathcal{A}}, \boldsymbol{x}_{\mathcal{E}}) = \{z \mid \forall w \in \boldsymbol{x}_{\mathcal{A}}, \exists u \in \boldsymbol{x}_{\mathcal{E}},\ z = f(w,u)\} \subseteq \mathrm{range}(f, \boldsymbol{x})$$

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

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

Then:

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

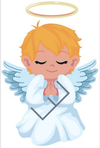
$$[\overline{f^0} - \langle \underline{\nabla}_u, r(\boldsymbol{x}_{\mathcal{E}})\rangle + \langle \overline{\nabla}_w, r(\boldsymbol{x}_{\mathcal{A}})\rangle, \underline{f^0} + \langle \underline{\nabla}_u, r(\boldsymbol{x}_{\mathcal{E}})\rangle - \langle \overline{\nabla}_w, r(\boldsymbol{x}_{\mathcal{A}})\rangle]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

Intuition:

- Control $u \in \boldsymbol{x}_{\mathcal{E}}$ acts positively on the (exact) range width : widens the over (resp. under) approximation by $\langle \overline{\nabla}_u, r(\boldsymbol{x}_{\mathcal{E}})\rangle)[-1,1]$ (resp. $\langle \underline{\nabla}_u, r(\boldsymbol{x}_{\mathcal{E}})\rangle)[-1,1]$)
- Disturbance $w \in \boldsymbol{x}_{\mathcal{A}}$ acts as an adversary: shrinks down the over (resp. under) approximation by $\langle \underline{\nabla}_w, r(\boldsymbol{x}_{\mathcal{A}})\rangle)[-1,1]$ (resp. by $\langle \overline{\nabla}_w, r(\boldsymbol{x}_{\mathcal{A}})\rangle)[-1,1]$)

Intuitively: a simple two-player game!

The players

 ($\exists$-player)

 ($\forall$-player)

Rules of outer-approximation game for $f(x_1, \ldots, x_p)$: for each quantifier Q_i, $i \in [1, p]$

- if $Q_i = \exists$,  widens by the maximal contribution $\overline{\nabla}_u$
- if $Q_i = \forall$,  shrinks by the minimal contribution $\underline{\nabla}_w$

Rules of inner-approximation game for $f(x_1, \ldots, x_p)$: for each quantifier Q_i, $i \in [1, p]$

- if $Q_i = \exists$,  widens by the minimal contribution $\underline{\nabla}_u$
- if $Q_i = \forall$,  shrinks by the maximal contribution $\overline{\nabla}_w$

Example in 2-D

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

$$f(1,1) = 0; \quad \mid \nabla f(\boldsymbol{x}) \mid \subseteq \begin{pmatrix} [6.8, 9.2] & [0, 0.4] \\ [0, 0.4] & [6.8, 9.2] \end{pmatrix}$$

- 1-D mean-value approximations:
- 2-D under-approximation by robust range:

Example in 2-D

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

$$f(1,1) = 0; \quad |\nabla f(\boldsymbol{x})| \subseteq \begin{pmatrix} [6.8, 9.2] & [0, 0.4] \\ [0, 0.4] & [6.8, 9.2] \end{pmatrix}$$

- 1-D mean-value approximations:
- 2-D under-approximation by robust range:

Application to reachability of discrete-time systems

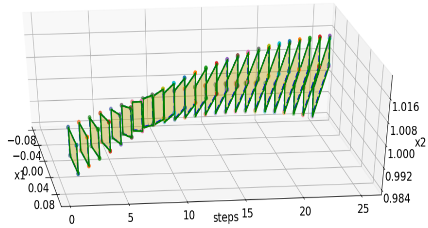
Iteratively compute function image, with as input, the previously computed approximations (under and over-approximations I^k and O^k of the reachable set $\boldsymbol{z}^k$):

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

Test model

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

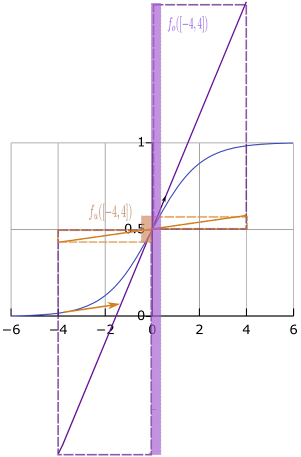
with $x_1^0 \in [0.05, 0.1], x_2^0 \in [0.99, 1.00]$ and $\Delta = 0.01$.



Under- (yellow) and over-approximated (green) reachable sets over time up to 25 steps (0.02 sec)

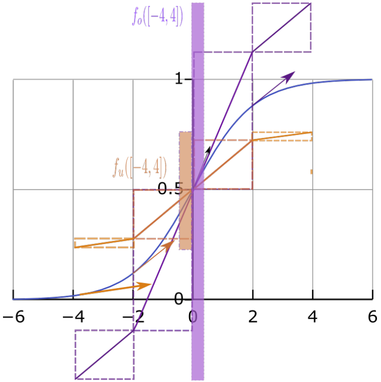
Refining the approximations

Example: the sigmoid function



- Not so accurate/satisfying...
- First natural idea: input domain partition? Costly and convex union of the under-approximating boxes is in general not an under-approximation of range(f, $\boldsymbol{x}$)

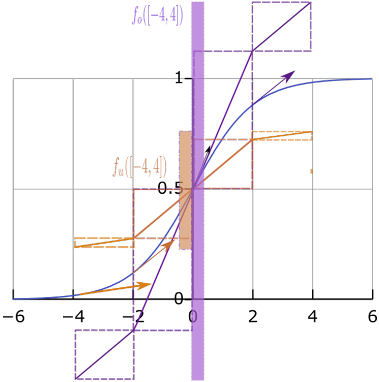
Refinement by local quadrature



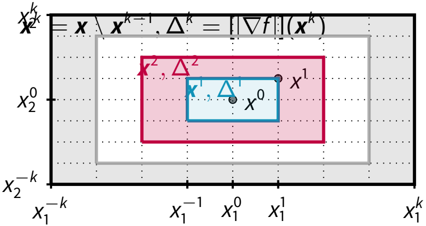
Mean-value extension is an interval abstraction of $f(x) = f(x_0) + \int_{x_0}^{x} f'(x)dx$: use a partition $\boldsymbol{x} = \boldsymbol{x}_1 \cup \boldsymbol{x}_2$ to refine:

$$f^0 + \langle \underline{\nabla}^1, dx^1 \rangle [-1, 1] + \langle \underline{\nabla}^2, dx^2 \rangle [-1, 1] \subseteq \text{range}(f, \boldsymbol{x}^1 \cup \boldsymbol{x}^2)$$
$$\text{range}(f, \boldsymbol{x}^1 \cup \boldsymbol{x}^2) \subseteq f^0 + \langle \overline{\nabla}^1, dx^1 \rangle [-1, 1] + \langle \overline{\nabla}^2, dx^2 \rangle [-1, 1]$$

Refinement by local quadrature



Generalizes to more partitions and n dimensions.



Higher-order AE extensions

Theorem

Let g be an elementary (compositions of +, -, $\times$, /, sine, cosine, log, exp in particular) approximation function for f, s.t.

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

Then any under-approx $\mathcal{I}_g$ (resp. over-approx $\mathcal{O}_g$) of the range of g robust to $x_{\mathcal{A}}$ and ξ is an under-approx (resp. over-approx) of the range of f robust to $x_{\mathcal{A}}$, i.e.

$$\mathcal{I}_g \subseteq range_{\mathcal{AE}}(f, \mathbf{x}_{\mathcal{A}}, \mathbf{x}_{\mathcal{E}}) \subseteq \mathcal{O}_g$$

If g can be separated, i.e. $g(w,u,\xi) = \alpha(w,u) + \beta(w,u,\xi)$, with $\mathcal{I}_\alpha$ under-approx of the range of α robust to w, $\mathcal{O}_\beta$ over-approx of the range of β then

$$\mathcal{I}_g = [\underline{\mathcal{I}_\alpha} + \overline{\mathcal{O}_\beta}, \overline{\mathcal{I}_\alpha} + \underline{\mathcal{O}_\beta}] \subseteq range_{\mathcal{AE}}(f, \mathbf{x}_{\mathcal{A}}, \mathbf{x}_{\mathcal{E}})u$$

Typically, $g(w,u,\xi)$ Taylor expansion of f (with $x = (w,u)$ and ξ from Lagrange remainder):

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

Easily applicable for $n = 1$ (linear expression can be exactly evaluated)

Arbitrarily quantified reachability problems

A more general notion of robustness of a control loop

Reminder: robust reachability until now

Given $\varphi(t; x_0, u, w)$ the flow of an ODE at time t from x_0 with control u and disturbance w, for time $t \in [0, T]$, compute:

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

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

Alternative problem (control is not aware of perturbations)

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

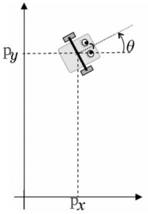
$$R_{\exists\forall\exists}(\varphi) = \{z \in \mathbb{R}^m \mid [\exists u \in [0,s] \to \mathbb{U}],\ \exists x_0 \in \mathbb{X}_0,\ \forall w \in [0,s] \to \mathbb{W},\ \exists s \in [0,T],\ z = \varphi(s; x_0, u, w)\}$$

where $[\exists u]$ optional if we know the controller,

Example: Dubins vehicle

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

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



- Init: $\mathbb{X}_0 = \{(p_x, p_y, \theta) \mid p_x \in [-0.1, 0.1],\ p_y \in [-0.1, 0.1],\ \theta \in [-0.01, 0.01]\}$,
- Control a (angular velocity) in $\mathbb{U} = [-0.01, 0.01]$, disturbance b_1 in $\mathbb{W} = [-0.01, 0.01]$

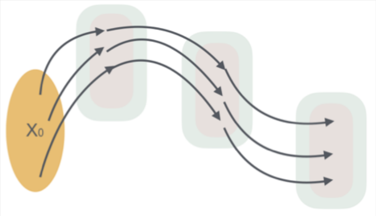
We want to estimate:

$$R_{\exists\forall\exists}(\varphi) = \{z \in \mathbb{R}^m \mid \exists a \in \mathbb{U},\ \exists x_0 \in \mathbb{X}_0,\ \forall b_1 \in \mathbb{W},\ \exists s \in [0, T],\ z = \varphi(s; x_0, u, w)\}$$

But also

Motion planning

- Find possible waypoints and final state, for a controller that takes *k* constrained actions
- Gives *k* alternations of ∀∃ quantifiers, for *k* waypoints



General temporal logics formulas, and hyperproperties

- behavioral robustness,
- comparisons of controllers

Etc.

Extension to the general case of arbitrary order of quantifiers

$$R_{\boldsymbol{p}}(f) = \{z \in \mathbb{R}^m \mid Q_1 x_1 \in [-1,1], Q_2 x_2 \in [-1,1], \ldots Q_p x_p \in [-1,1], \boldsymbol{z} = f(x_1, x_2, \ldots, x_p)\}$$

Rules of outer-approximation game:

Rounds for i from p to 1:

- if $Q_i = \exists$,  widens range by the maximal contribution $\overline{\nabla}_u$
- if $Q_i = \forall$,  shrinks range by the minimal contribution $\underline{\nabla}_w$
- if empty range, stop: daemon wins

Rules of inner-approximation game:

Rounds for i from p to 1:

- if $Q_i = \exists$,  widens range by the minimal contribution $\underline{\nabla}_u$
- if $Q_i = \forall$,  shrinks range by the maximal contribution $\overline{\nabla}_w$

An outer-approximation game

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 $c = g(0,0,0) = 11$.
- $O_1 = \left[-\frac{1}{2}, \frac{1}{2}\right]$, $I_1 = 0$, $O_2 = [-3,3]$, $I_2 = [-1,1]$ and $O_3 = [-10,10]$, $I_3 = [-4,4]$.

Outer-approximation of $R_{\exists\forall\exists}(g)$ - round 3

$$\begin{aligned} & [\ c + \underline{O}_3,\ c + \overline{O}_3\ ] \\ = & [\ 11 - 10,\ 11 + 10\ ] \end{aligned}$$

An outer-approximation game

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 $c = g(0,0,0) = 11$.
- $O_1 = \left[-\frac{1}{2}, \frac{1}{2}\right]$, $I_1 = 0$, $O_2 = [-3,3]$, $I_2 = [-1,1]$ and $O_3 = [-10,10]$, $I_3 = [-4,4]$.

Outer-approximation of $R_{\exists\forall\exists}(g)$ - round 2

$$\begin{array}{lcccccc} [& c & +\overline{I}_2 & +\underline{O}_3, & c & +\underline{I}_2 & +\overline{O}_3 &] \\ = [& 11 & +1 & -10, & 11 & -1 & +10 &] \end{array}$$

An outer-approximation game

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 $c = g(0,0,0) = 11$.
- $O_1 = \left[-\frac{1}{2}, \frac{1}{2}\right]$, $I_1 = 0$, $O_2 = [-3,3]$, $I_2 = [-1,1]$ and $O_3 = [-10,10]$, $I_3 = [-4,4]$.

Outer-approximation of $R_{\exists\forall\exists}(g)$ - round 1, Angel wins

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

An outer-approximation game

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 $c = g(0,0,0) = 11$.
- $O_1 = \left[-\frac{1}{2}, \frac{1}{2}\right]$, $I_1 = 0$, $O_2 = [-3,3]$, $I_2 = [-1,1]$ and $O_3 = [-10,10]$, $I_3 = [-4,4]$.

Outer-approximation of $R_{\exists\forall\exists}(g)$ - round 1, Angel wins






$$[\ c\ + \underline{O}_1\ + \overline{I}_2\ + \underline{O}_3,\ c\ + \overline{O}_1\ + \underline{I}_2\ + \overline{O}_3\ ]$$
$$= [\ 11\ - \tfrac{1}{2}\ + 1\ - 10,\ 11\ + \tfrac{1}{2}\ - 1\ + 10\ ] = [1.5, 20.5]$$

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

An inner-approximation game

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 $c = g(0, 0, 0) = 11$.
- $O_1 = \left[-\frac{1}{2}, \frac{1}{2}\right]$, $I_1 = 0$, $O_2 = [-3, 3]$, $I_2 = [-1, 1]$ and $O_3 = [-10, 10]$, $I_3 = [-4, 4]$.

Inner-approximation of $R_{\exists\forall\exists}(g)$ - round 3

$$[\ c + \underline{I}_3,\ c + \overline{I}_3\ ]$$
$$= [\ 11 - 4,\ 11 + 4\ ]$$

An inner-approximation game

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 $c = g(0,0,0) = 11$.
- $O_1 = \left[-\frac{1}{2}, \frac{1}{2}\right]$, $I_1 = 0$, $O_2 = [-3, 3]$, $I_2 = [-1, 1]$ and $O_3 = [-10, 10]$, $I_3 = [-4, 4]$.

Inner-approximation of $R_{\exists\forall\exists}(g)$ - round 2

$$[\ c \quad +\overline{O}_2 \quad +\underline{I}_3,\quad c \quad +\underline{O}_2 \quad +\overline{I}_3\ ]$$
$$= [\ 11 \quad +3 \quad -4,\quad 11 \quad -3 \quad +4\ ]$$

An inner-approximation game

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 $c = g(0,0,0) = 11$.
- $O_1 = \left[-\frac{1}{2}, \frac{1}{2}\right]$, $I_1 = 0$, $O_2 = [-3,3]$, $I_2 = [-1,1]$ and $O_3 = [-10,10]$, $I_3 = [-4,4]$.

Inner-approximation of $R_{\exists\forall\exists}(g)$ - round 1, Angel wins

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

An inner-approximation game

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 $c = g(0,0,0) = 11$.
- $O_1 = \left[-\frac{1}{2}, \frac{1}{2}\right]$, $I_1 = 0$, $O_2 = [-3,3]$, $I_2 = [-1,1]$ and $O_3 = [-10,10]$, $I_3 = [-4,4]$.

Inner-approximation of $R_{\exists\forall\exists}(g)$ - round 1, Angel wins

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

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

The problem with joint inner-approximations

A simple example

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

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

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

Problem?

- Outer-approximation of each component $\Rightarrow$ outer-approximation of $R_{\exists\forall\exists}(f)$: Same calculation as before, 1 component at a time: $R_{\exists\forall\exists}(f) \subseteq [-3,7] \times [-7,5]$.
- Would find here also$[-3,7] \times [-7,5] \subseteq R_{\exists\forall\exists}(f)$, wrong!

Reason: a witness for $\exists x_i$ may not be the same for each component of f!

A solution for joint inner-approximations

A simple relaxation

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

For example ($\underline{\forall}$ as relaxations of $\exists$):

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

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

(for each i, $\boxed{\exists x_i}$ appears in only one component of f)

Reminder: we wanted to compute, originally:

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

Example

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

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

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

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 (we already did the first component!):

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

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

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

Example

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

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

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

For the joint inner-approximation, interpret (2nd component):

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

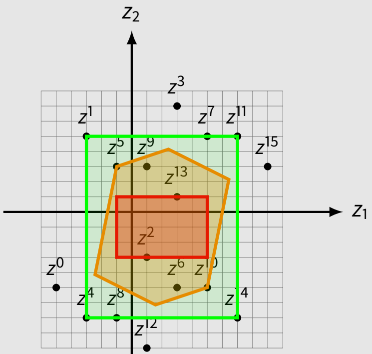
$$\forall x_1,\ \forall x_2,\ \forall x_3,\ \boxed{\exists x_4},\ z_2 = f_2(x_1,x_2,x_3,x_4)$$

$$\begin{aligned} z_2 &= [\ z_2^c\ + \delta_{x_1} + \delta_{x_2} + \delta_{x_4} - \delta_{x_3},\ z_1^c\ - \delta_{x_1} - \delta_{x_2} - \delta_{x_4} + \delta_{x_3}] \\ &= [\ -1\ \ +1 + 1 + 1\ \ -5,\ -1\ \ -1 - 1 - 1\ \ +5]\ = [-3, 1] \end{aligned}$$

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

Example, in picture

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



- Samples $z^0, \ldots, z^{15}$ of $f([-1, 1]^4)$
- Outer-approximation (our method)
- Exact set $R_{\exists\forall\exists}(f)$
- Inner-approximation (our method)

Dubins example

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

- 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:

$$\dot{\left(\frac{\partial x}{\partial x_0}\right)} = -vsin(\theta)\frac{\partial \theta}{\partial x_0} + \frac{\partial b_1}{\partial x_0}$$

with $\frac{\partial x}{\partial x_0}(t = 0) = 1$, $\frac{\partial \theta}{\partial x_0}(t = 0) = 0$ etc.

Dubins example

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

- 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:
  - $I_{x,a} = 0$, $O_{x,a} = [-6.545\ 10^{-7}, 6.545\ 10^{-7}]$, $I_{x,x_0} = O_{x,x_0} = [-0.1, 0.1]$, $I_{x,\theta_0} = 0$, $O_{x,\theta_0} = [-1.309\ 10^{-6}, 1.309\ 10^{-6}]$, $I_{x,b_1} = 0$, $O_{x,b_1} = [-0.005, 0.005]$,
  - $I_{y,a} = 0$, $O_{y,a} = [-0, 0025, 0.0025]$, $I_{y,y_0} = O_{y,y_0} = [-0.1, 0.1]$, $I_{y,\theta_0} = 0$, $O_{y,\theta_0} = [-0, 005, 0.005]$,
  - $I_{\theta,\theta_0} = O_{\theta,\theta_0} = [-0.01, 0.01]$, $I_{\theta,a} = 0$, $O_{\theta,a} = [0, 0.005]$,

Dubins example

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,

Dubins example

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

and its upper bound:

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

which is equal to 0.589999982. Therefore inner-approx $[-0.095, 0.589999982]$.

Dubins example

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:

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

which is equal to -0.1000019635,

Dubins example

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

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. Outer-approx $[-0.1000019635, 0.6050019635]$.

Dubins example

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.

Last application: Dubins!

Space relaxation

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

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)

Vector-valued functions: back to the example

Consider again:

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

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

Using the Fourier-Motzkin elimination procedure for x_4:

$$\exists x_1 \in [-1, 1],\ \forall x_2 \in [-1, 1],\ \exists x_3 \in [-1, 1],$$
$$z_1 \geq 1 + 2x_1 + x_2 + 3x_3 \ \wedge\ z_1 \leq 3 + 2x_1 + x_2 + 3x_3$$
$$z_2 \geq -6 - x_1 - x_2 + x_3 \ \wedge\ z_2 \leq 4 - x_1 - x_2 + x_3$$
$$\wedge\ 11 + 11x_1 + 6x_2 + 16x_3 = 5z_1 - z_2$$

Example

Then eliminating x_3 gives:

$$\frac{1}{3}z_1 - z_2 - 9 - \frac{5}{3}x_1 - \frac{4}{3}x_2 \leq 0 \ \wedge \ z_2 - \frac{1}{3}z_1 + \frac{13}{3} + \frac{5}{3}x_1 + \frac{4}{3}x_2 \leq 0$$
$$\wedge \ z_1 - 6 - 2x_1 - x_2 \leq 0 \ \wedge \ z_1 + 2 - 2x_1 - x_2 \geq 0$$
$$\wedge \ z_2 - 5 + x_1 + x_2 \leq 0 \ \wedge \ z_2 + 7 + x_1 + x_2 \geq 0$$
$$\wedge \frac{1}{16}(5z_1 - z_2 - 11 - 11x_1 - 6x_2) \leq 3 + 2x_1 + x_2 + 3x_3 \wedge \frac{1}{16}(5z_1 - z_2 - 11 - 11x_1 - 6x_2) \leq 4 - x_1 - x_2 + x_3$$
$$\wedge 1 + 2x_1 + x_2 + 3x_3 \leq \frac{1}{16}(5z_1 - z_2 - 11 - 11x_1 - 6x_2) \wedge -6 - x_1 - x_2 + x_3 \leq \frac{1}{16}(5z_1 - z_2 - 11 - 11x_1 - 6x_2)$$

And after lengthy calculations for eliminating x_2 and x_1 in turn, and simplifications, we obtain exactly the zonotope which is the exact set $R_{\mathbf{p}}(\mathbf{f})$.

Too complex: use zonotope approximations

Zonotopes: a quick recap

A zonotope is the Minkowski sum of the line segments $[-1, 1]g_i$ in $\mathbb{R}^n$.

Definition

Let X and Y be two subsets of $\mathbb{R}^n$. The Minkowski sum $X \oplus Y$ is the subset of $\mathbb{R}^n$ given by:

$$X \oplus Y = \{x + y \,|\, x \in X,\ y \in Y\}$$

Zonotopes are obviously closed under Minkowski sum. Are they closed under the Minkowski difference, a pseudo-inverse of the operation of the Minkowski sum ?

Definition

Let X and Y be two subsets of $\mathbb{R}^n$. The Minkowski difference $X \ominus Y$ is the subset of $\mathbb{R}^n$ given by:

$$X \ominus Y = \{x \in \mathbb{R}^n \mid \{x\} \oplus Y \subseteq X\}$$

As shown in [Althoff2015], zonotopes are not closed under the Minkowski difference, unless in dimensions less or equal to 2, but there are algorithmic ways to inner and outer-approximate the Minkowski difference of two zonotopes as a zonotope.

Order 1 method

Intuitively, in the two-player game, replace interval computations for each component on f by computation on polyhedras:

- widening with an interval is now Minkowski sum with a zonotope
- shrinking with an interval is now Minkowski difference with a zonotope

Theoretical complexity

- Minkowski sums and differences of general polyhedra can be doubly exponential
- Keeping things within zonotopes, as is the case in dimension 2, or with further inner and outer-approximations such as the ones given in [Althoff15], makes computations polynomial time.

Next

For next week: paper reading

- *Inner and outer approximate quantifier elimination for general reachability problems, E. Goubault and S. Putot, 2024*
- longer version if details neeeded *Inner and outer approximations of arbitrarily quantified reachability problems, E. Goubault and S. Putot, 2026*
- Who is presenting ?

Next week (Eric Goubault): From Sets to Geometry, Application to unbounded-time reachability and controllability