Inner and Outer Approximating Flowpipes for Delay Differential Equations

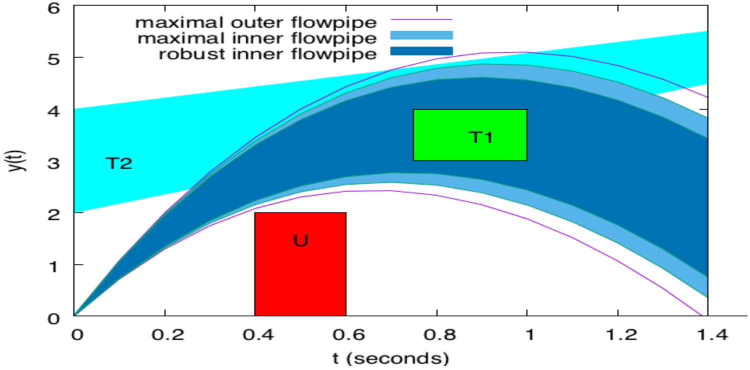
Eric Goubault Sylvie Putot Lorenz Sahlmann

LIX, Ecole Polytechnique - CNRS, Université Paris-Saclay

CAV, Oxford, July 17, 2018

Motivation: bounded-time reachable sets for uncertain dynamical systems

- Over-approximating flowpipes = overapproximation of the reachable sets
  - provide safety proof but conservative ("false alarms")
- Under-approximating flowpipes = states guaranteed to be reached
  - falsification of safety properties
  - precision estimates
  - verification of new properties (robustness to some parameters, sweep-avoid, etc)



- ... and for Delay Differential Equations!

Delay Differential Systems

Delay Differential Equations, with known constant delay τ (communication time in CPS) and uncertain initial conditions and parameters β

$$\begin{cases} \dot{z}(t) = f(z(t), z(t-\tau), \beta) & \text{if } t \in [t_0+\tau, T] \\ z(t) = z_0(t, \beta) & \text{if } t \in [t_0, t_0+\tau] \end{cases}$$

Example (Basic PD-controller for a self-driving car)

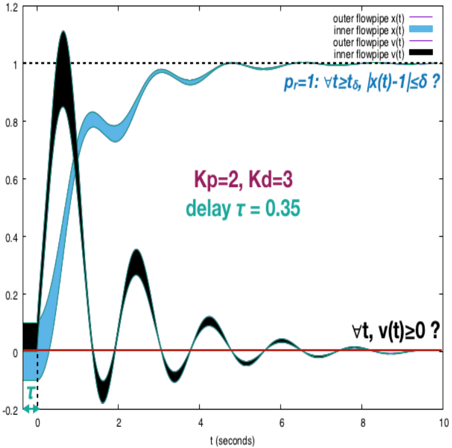
- controlling the car's position x and velocity v by adjusting its acceleration depending on the current distance to a reference position p_r.
- delay τ to transfer the data to the controller, due to sensing or transmission time
- possibly uncertain (but constant) coefficients K_p and K_d

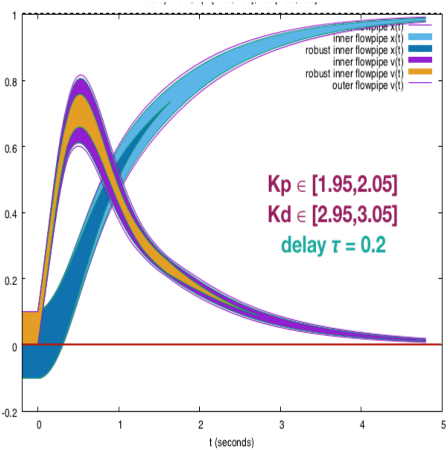
$$\begin{cases} \dot{x}(t) = v(t) \\ \dot{v}(t) = -K_p\big(x(t-\tau) - p_r\big) - K_d\, v(t-\tau) \end{cases}$$

- uncertain initial state $(x_0, v_0) \in [-0.1, 0.1] \times [0, 0.1]$, constant on time interval $[-\tau, 0]$.

Delays can induce instabilities or weird behaviors!

- Asymptotic stability guaranteed for $K_p = 2$ and $K_d = 3$ when no delay $\tau = 0$.
- Even small delays can have a huge impact on the dynamics and possibly safety
  - safety condition example: $\forall t,\ v(t) \geq 0$ (true for $\tau = 0.2$, false for $\tau = 0.35$)
  - robustness to uncertainty in Kp and Kd (in right figure)





Velocity $v(t)$ and position $x(t)$ (left $\tau = 0.35$, right $\tau = 0.2$)

The method of steps for solving DDEs (constant delay)

Example (method of steps)

$$\begin{cases} \dot{z}(t) = -z(t) \cdot z(t-\tau) =: f\left(z(t), z(t-\tau), \beta\right) & t \in [0, T] \\ z(t) = (1+\beta t)^2 =: z_0(t, \beta) & t \in [-\tau, 0] \end{cases} \tag{1}$$

- On $t \in [0, \tau]$ the solution of the DDE (1) is the solution of the ODE (2)

$$\dot{z}(t) = -z(t)(1+\beta(t-\tau))^2, \; t \in [0, \tau] \tag{2}$$

  with initial value $z(0) = z_0(0, \beta) = 1$.
- We iterate the process: we plug the solution of (2) for $t \in [0, \tau]$ in DDE (1) and obtain $z(t)$ for $t \in [\tau, 2\tau]$ as solution of a new ODE, etc.

It is a general method for DDEs

- On each time interval $[t_0 + i\tau, t_0 + (i+1)\tau]$, for $i \geq 1$, the function $z(t-\tau)$ is a known history function, computed as the solution of the DDE on the previous time interval $[t_0 + (i-1)\tau, t_0 + i\tau]$
- Plugging the solution of the previous ODE into the DDE yields a new ODE on the next tile interval

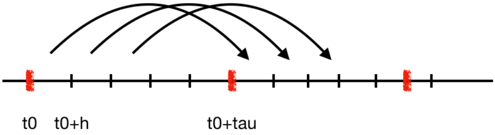
Reachability analysis for DDEs

An extension of Taylor model approaches to compute flowpipes

- We use existing Taylor approaches to compute flowpipes for each ODE derived from the DDE, on each $[t_0 + i\tau, t_0 + (i+1)\tau]$
- The main difficulty is to over-approximate functions (for initial condition and solution of the previous ODE) efficiently: Taylor models with zonotopic coefficients

Building flowpipes

- Two level of grids: at each step of the coarse grid of step size τ, we build the Taylor models for the solution of the new ODE on a finer grid of step size $h = \tau/p$.



Building the Taylor model for over-approximating flowpipes

Taylor expansion on $[t_{ij}, t_{i(j+1)}]$ (with i the coarse grid step, j the fine grid step)

$$[z](t, t_{ij}, [z_{ij}]) = [z_{ij}] + \sum_{l=1}^{k-1} (t - t_{ij})^l [f_{ij}]^{[l]} + (t - t_{ij})^k [\overline{f_{ij}}]^{[k]},$$

- The coefficients are defined inductively, and computed by automatic differentiation:

$$\begin{array}{rcl} [f_{ij}]^{[1]} & = & [f]\left([z_{ij}], [z_{(i-1)j}]\right) \\ [f_{1j}]^{[l+1]} & = & \frac{1}{l+1}\left(\left[\frac{\partial f^{[l]}}{\partial z}\right][f_{1j}]^{[1]} + [z_{0j}]\,[f_{0j}]^{[1]}\right) \\ [f_{ij}]^{[l+1]} & = & \frac{1}{l+1}\left(\left[\frac{\partial f^{[l]}}{\partial z}\right][f_{ij}]^{[1]} + \left[\frac{\partial f^{[l]}}{\partial z^{\tau}}\right]\left[f_{(i-1)j}\right]^{[1]}\right) \quad \text{if } i \geq 2 \end{array}$$

- Remainder term :
  - compute an enclosure $[\overline{z_{ij}}]$ of solution $z(t, z_0)$ on $[t_{ij}, t_{i(j+1)}]$ by the Picard-Lindelöf iteration: find $[\overline{z_{ij}}]$ such that

$$[z_{ij}] + [t_{ij}, t_{i(j+1)}][f]([\overline{z_{ij}}], [\overline{z_{i-1j}}]) \subseteq [\overline{z_{ij}}]$$

  - then evaluate $[f]$ over $[\overline{z_{ij}}]$:

$$[\overline{f_{ij}}]^{[1]} = [f]([\overline{z_{ij}}], [\overline{z_{(i-1)j}}]), \quad \text{and inductively } [\overline{f_{ij}}]^{[l+1]} = \ldots$$

Initialization of the next iterate: $[z_{i(j+1)}] = [z](t_{i(j+1)}, t_{ij}, [z_{ij}])$

Inner-approximating flowpipes

Inner-approximation

Given uncertain (constant) parameters $\beta \in \boldsymbol{\beta}$, an inner-approximation at time t of the reachable set, is $]z[(t, \boldsymbol{\beta}) \subseteq z(t, \boldsymbol{\beta})$ such that $(\forall z \in]z[(t, \boldsymbol{\beta}))\,(\exists \beta \in \boldsymbol{\beta})\,(\varphi(t, \beta) = z)$.

Robust inner-approximation

Given uncertain (constant) parameters $\beta = (\beta_{\mathcal{A}}, \beta_{\mathcal{E}}) \in \boldsymbol{\beta}$, an inner-approximation of the reachable set $z(t, \boldsymbol{\beta})$ at time t, robust with respect to $\beta_{\mathcal{A}}$, is a set $]z[_{\mathcal{A}}(t, \boldsymbol{\beta}_{\mathcal{A}}, \boldsymbol{\beta}_{\mathcal{E}})$ such that $(\forall z \in]z[_{\mathcal{A}}(t, \boldsymbol{\beta}_{\mathcal{A}}, \boldsymbol{\beta}_{\mathcal{E}}))\,(\forall \beta_{\mathcal{A}} \in \boldsymbol{\beta}_{\mathcal{A}})\,(\exists \beta_{\mathcal{E}} \in \boldsymbol{\beta}_{\mathcal{E}})\,(\varphi(t, \beta_{\mathcal{A}}, \beta_{\mathcal{E}}) = z)$.

General principle of our algorithm (extending [HSCC 2017])

1. Compute outer-approximating flowpipes, on each time interval $[t_{ij}, t_{i(j+1)}]$, of:
   - the solution $z(t, \tilde{\beta})$ for some $\tilde{\beta} \in \boldsymbol{\beta}$
   - the entries $J_{ij}(t) = \frac{\partial z_i}{\partial \beta_j}(t)$ of the Jacobian matrix $J(t, \beta)$ of the solution with respect to the parameters β, for all $\beta \in \boldsymbol{\beta}$: they also satisfy a DDE (the variational equations)
2. Use a generalized Mean-Value Theorem to derive an inner-approximation

Computing inner-approximating flowpipes

Generalized intervals

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

Theorem (Generalized Mean-Value Theorem (builds on [Goldsztejn 2005], [HSCC'17]))

- *For $\beta = (\beta_{\mathcal{A}}, \beta_{\mathcal{E}})$, we note $J_{\mathcal{A}}$ the sub-matrix of the Jacobian corresponding to the partial derivatives with respect to $\beta_{\mathcal{A}}$ and $J_{\mathcal{E}}$ the remaining columns*
- *If for t in $[t_{ij}, t_{i(j+1)}]$, the following, evaluated with Kaucher arithmetic [Kaucher 1980] on generalized intervals, is an improper interval*

$$
]z[_{\mathcal{A}}(t, t_{ij}, \boldsymbol{\beta}_{\mathcal{A}}, \boldsymbol{\beta}_{\mathcal{E}}) = [z](t, t_{ij}, [\tilde{z}_{ij}]) + [J]_{\mathcal{A}}(t, t_{ij}, [J_{ij}])(\boldsymbol{\beta}_{\mathcal{A}} - \tilde{\beta}_{\mathcal{A}}) + [J]_{\mathcal{E}}(t, t_{ij}, [J_{ij}])(\mathit{dual}\ \boldsymbol{\beta}_{\mathcal{E}} - \tilde{\beta}_{\mathcal{E}})
$$

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

Implementation and Experiments

Protoype in C++

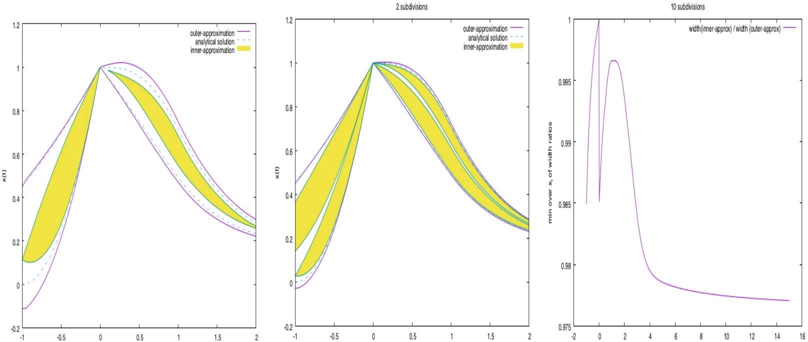
Using :

- `FILIB++` C++ library for interval computation
- `FADBAD++` package for automatic differentiation
- and (a slightly modified version of) `aaflib` library for affine arithmetic

Extends a previous prototype for ODEs [HSCC2017], and is available from
`http://www.lix.polytechnique.fr/Labo/Sylvie.Putot/software.html`

Simple running example: efficiency and accuracy of the analysis

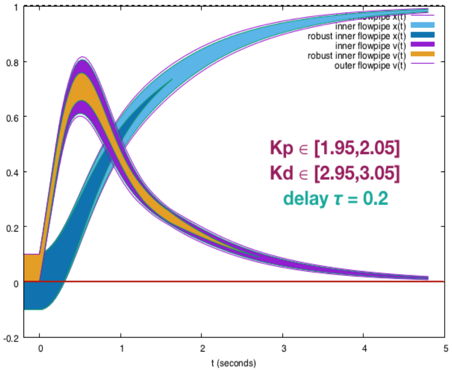
- Order 2 Taylor models, integration step size 0.05 sec, until $T_{\max} = 2$
- Left (results obtained in 0.03 seconds) and center figures:
  - dashed lines: analytical solution
  - solid external lines: outer-approximating flowpipe
  - filled yellow region = inner-approximating flowpipe
- Subdivision of range of initial conditions to improve accuracy (left no subdiv, center 2 subdiv, right 10 subdiv)
- Right figure: quality measure γ = width of inner-approx over width of outer-approx (stabilizes here over 0.975)



Robustness to the constant PD-controller parameters for self-driving car

- Outer-approximating flowpipe $O(t)$:
  $\forall t, \forall x_0 \in X_0, \forall (K_p, K_d) \in [1.95, 2.05] \times [2.95, 3.05], \exists x \in O(t), x = x(t, x_0, K_p, K_d)$
- Inner-approximating flowpipe $I(t)$ (purple / light blue filled region):
  $\forall t, \forall x \in I(t), \exists x_0 \in X_0, \exists (K_p, K_d) \in [1.95, 2.05] \times [2.95, 3.05], x = x(t, x_0, K_p, K_d)$
- Robust inner-approximating flowpipe $I_A(t)$ (orange / dark blue filled region):
  $\forall t, \forall x \in I_A(t), \forall (K_p, K_d) \in [1.95, 2.05] \times [2.95, 3.05], \exists x_0 \in X_0, x = x(t, x_0, K_p, K_d)$

- Results obtained in 0.24s with order 3 Taylor models and time step = 0.04
- The outer-approximation proves safety (the velocity never becomes negative)
- The inner-approximation provides falsification when relevant, and an accuracy measure γ
- The robust inner-approximation provides robustness to uncertainty in K_p and K_d



Velocity $v(t)$ and position $x(t)$

Platoon of autonomous vehicles (adapted from [Erneux 2009])

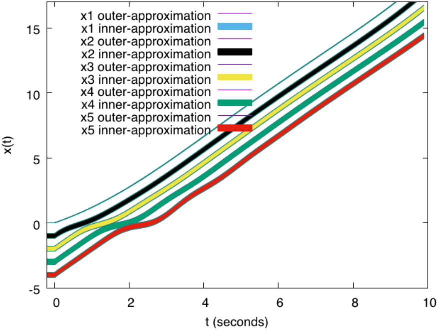
- Vehicles C_1 (leading),...,C_n, adapting their current velocity v_i, with delay $\tau = 0.3$
- Vehicles have sensors to measure speed of vehicle ahead
- Polynomial ODE of order 3 for x_1 and v_2, positions x_i and velocities v_{i+1} such that

$$\begin{array}{rcll} \dot{x}_i(t) & = & v_i(t) & i = 2, \cdots, n \\ \dot{v}_{i+1}(t) & = & 2.5(v_i(t-\tau) - v_{i+1}(t-\tau)) & i = 2, \cdots, n-1 \end{array}$$

- Cars have uncertain initial position and speed

Results

- For 5 cars (9-dimensional system), until time 10, with time step 0.1 and order 3 Taylor models (obtained in 2.13 sec)
- Inner-approximations of positions intersect: we have proven there are unsafe initial conditions.
- For 10 cars (19-dimension system), results obtained in 6.5 sec



A seven-dimensional benchmark from [Franzle et al. FORMATS 2017]

Example

$$f(x(t), x(t-\tau) = \begin{cases} 1.4x_3(t) - 0.9x_1(t-\tau) \\ 2.5x_5(t) - 1.5x_2(t) \\ 0.6x_7(t) - 0.8x_3(t)x_2(t) \\ 2 - 1.3x_4(t)x_3(t) \\ 0.7x_1(t) - x_4(t)x_5(t) \\ 0.3x_1(t) - 3.1x_6(t) \\ 1.8x_6(t) - 1.5x_7(t)x_2(t)) \end{cases}$$

and the initial function is constant on $[-\tau, 0]$ with values in
$[1.0, 1.2] \times [0.95, 1.15] \times [1.4, 1.6] \times [2.3, 2.5] \times [0.9, 1.1] \times [0.0, 0.2] \times [0.35, 0.55]$

(Unfair) comparison wrt [Franzle et al. FORMATS 2017]

Reachable sets of the DDE computed until $t = 0.1$, and quality measure $\gamma()$ (ratio of the width of projection on each x_i of inner-approx over outer-approx):

	time (sec)	accuracy measure $\gamma(x_1), \ldots, \gamma(x_7)$
our work (order 2)	0.13	0.998, 0.996, 0.978, 0.964, 0.97, 0.9997, 0.961
Franzle et al.	505	0.575, 0.525, 0.527, 0.543, 0.477, 0.366, 0.523

Future work

- Uncertain and variable delays (extension to uncertain but constant delay is reasonably easy, variable delay is much more intricate)
- Hybrid systems with delays
- From uncertain parameters to uncertain controls (defined as a class of functions with e.g. bounds on values and certain derivatives)