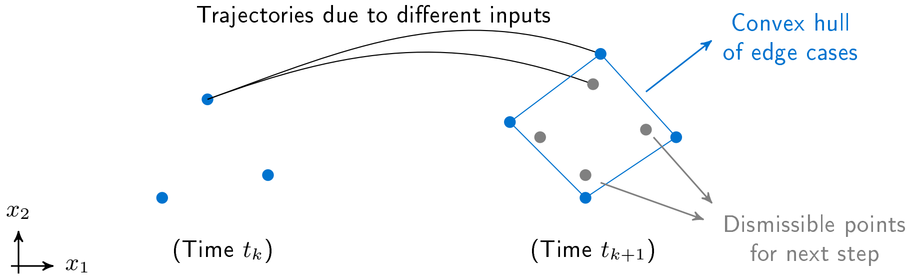
Edge-Case Simulations for Linear Systems with Uncertain Initial State and Input

Background

The application of cyber-physical systems in safety-critical environments requires formal verification techniques in order to ensure correct functionality. A contemporary example would be the launch of a rover to another planet, where even small failures are critical as they might lead to the failure of the mission. Reachability analysis is one of the main techniques to provide safety guarantees: Under the influence of uncertainty in the initial state and external input or disturbances, the reachable set of states encompassing all possible system behaviors over time is computed. If the reachable set of states does not intersect an unsafe set, which is determined by unwanted system behavior, safety is formally guaranteed. In general, only tight over-approximations of the exact reachable set of states can be computed. The tightness of reachable sets is often examined by visual comparison with a simulated trajectories. However, the number of possible trajectories is infinite and therefore, a visual comparison might give a wrong impression as edge cases could have been overlooked.


Trajectories due to different inputs
Convex hull of edge cases
x_2
x_1
(Time t_k)
(Time t_{k+1})
Dismissible points for next step

Description

In this thesis, we consider dynamical systems represented by linear ordinary differential equations (ODEs). The simulation of trajectories as well as reachability analysis for linear systems is implemented in the CORA toolbox [1]. By ODE theory, edge cases can only originate from the vertices of the uncertainty sets in the initial state and input. A naive albeit exhaustive approach, e.g., taking all combinations of the vertices of the initial set and the input set, scales exponentially, as every vertex of the input set has to be considered each time step. This becomes all the more severe with increasing state and input dimensions. Due to the uniqueness of ODE solutions, many trajectories of this impractical approach can be dismissed if they are contained in the convex hull of all other trajectories as depicted above. While the computation of the convex hull of a point cloud is theoretically feasible in any dimension, it may only serve as a ground truth since it substantially increases the computation time.

The goal of this thesis is to develop a strategy, which efficiently produces the most critical simulations such that we obtain accurate insight into the most critical possible system behavior. All programming will be done in MATLAB, and the final implementation should be integrated into the CORA toolbox to make it publicly available in a future CORA release.

Tasks

- Development and implementation of a strategy yielding edge-case simulations
- Evaluation of the performance on benchmark systems
- Integration of the final implementation into the CORA toolbox

References

[1] M. Althoff. An introduction to CORA 2015. In *Proc. of the Workshop on Applied Verification for Continuous and Hybrid Systems*, pages 120–151, 2015.

Technische Universität München

Fakultät für Informatik

Lehrstuhl für Echtzeitsysteme und Robotik

Supervisor:
Prof. Dr.-Ing. Matthias Althoff

Advisor:
Mark Wetzlinger, M.Sc.

Research project:
ConVeY

Type:
Bachelor's Thesis

Research area:
Reachability Analysis

Programming language:
MATLAB

Required skills:
Mathematical background in analysis/geometry, programming in MATLAB

Language:
English

Date of submission:
March 18, 2021

For more information please contact us:

Phone: +49.89.289.18144
(currently not available)

E-Mail: m.wetzlinger@tum.de

Internet:
https://www.in.tum.de/i06