Data-driven System Adaptation and Motion-Primitive Updating for Formally Safe Control

Technical University of Munich

Department of Informatics

Chair of Robotics, Artificial Intelligence and Real-time Systems

Background

Formally verified controllers can guarantee safety, but the guarantees rely on a model and uncertainty description that adequately cover real system behavior. In practice, disturbances, unmodeled dynamics, and time-varying effects can cause mismatches that may invalidate previously verified properties.

A standard correctness notion is *reachset conformance* [2]: observed trajectories should be consistent with model-based set predictions. While uncertainty descriptions can be calibrated from data, new behaviors may appear during operation, motivating runtime mechanisms to maintain safety assurances.

Motion primitives (MPs) [1] and maneuver automata offer an efficient safety framework via an offline verified maneuver library for fast online switching. A key challenge is keeping such safety certificates valid as uncertainty or operating conditions evolve.

Description

This project investigates a runtime adaptation concept that combines: (i) revising an uncertainty description based on newly available operational data, and (ii) maintaining formally justified safety guarantees for a motion-primitive-based controller library under such revisions.

Starting from a simplified baseline model (e.g., linear dynamics), the project will explore how to (a) identify and characterize mismatches between model-based set predictions and observed behavior, (b) adjust the uncertainty representation in a principled manner, and (c) ensure that the motion-primitive library remains valid with respect to constraints and terminal conditions. The emphasis is on designing an end-to-end workflow that is efficient enough for online use while preserving formal safety arguments.

Tasks

- Literature review on reachability-based safety verification, reachset conformance, and motion-primitive/maneuver-automaton safety frameworks.
- Design and implement a motion-primitive library under changing uncertainty/operating conditions.
- Experimental evaluation on representative scenarios.
- Document methodology, experiments, and results.

Contact

Main contact: yongkuan.zhang@tum.de.

References

[1] D. Heß, M. Althoff, and T. Sattel. Formal verification of maneuver automata for parameterized motion primitives. In *2014 IEEE/RSJ International Conference on Intelligent Robots and Systems*, pages 1474–1481, 2014.

[2] L. Lützow and M. Althoff. Scalable reachset-conformant identification of linear systems. *IEEE Control Systems Letters*, 8:520–525, 2024.

Supervisor:
Prof. Dr.-Ing. Matthias Althoff

Advisor:
Yongkuan Zhang

Research project:
Formal Safety & Data-Driven Online Adaptation

Type:
GR/MA

Research area:
Formal Methods / Reachability / Safety Verification / Motion Planning and Control

Programming language:
Matlab, Python

Required skills:
Good math background; good programming skills; Matlab and/or Python; ability to work independently. Prior exposure to reachability analysis and set-based methods (e.g., zonotopes) is a plus but not mandatory.

Language:
English

Date of submission:
Start as soon as possible

For more information please contact us:

Phone: +49 015225283555

E-Mail: yongkuan.zhang@tum.de

Website: