

Robustness-Guided Falsification (of Autonomous Vehicles)

Florian Finkeldei

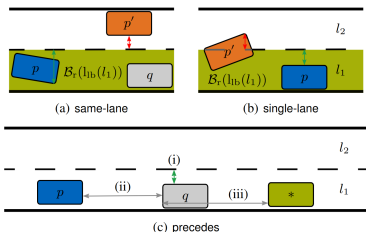
Prof. Dr.-Ing. Matthias Althoff
Cyber-Physical Systems Group
Technische Universität München

January 16, 2024

Robustness-Guided Falsification

Motivation

- Autonomous vehicles must obey traffic rules.
- Express traffic rules as temporal logic.
- STL for robustness degree of rule satisfaction.



Gressenbuch et al.: Predictive Monitoring of Traffic Rules.

Falsification

Find counter example that exposes traffic rule violations of AV by minimizing its robustness value in an optimization problem. We steer all surrounding vehicles (aka 'attackers').

Tasks

- Literature review on robustness guided falsification with
- Focus on autonomous driving use-case.
- Comparison to other falsification strategies in terms of
 - Success rate,
 - Computational performance → real-time capability,
 - Restrictions to the system model.

Qualifications

- Familiar with concept of temporal logics,
- Ideally some background / interest in numerical optimization.

Interested? Contact me!

Florian Finkeldei

florian.finkeldei@tum.de

Relevant papers

- Corso et al. (2022): A Survey of Algorithms for Black-Box Safety Validation of Cyber-Physical Systems
- Waga (2020): Falsification of Cyber-Physical Systems with Robustness-Guided Black-Box Checking
- Klischat et al. (2023): Falsifying Motion Plans of Autonomous Vehicles With Abstractly Specified Traffic Scenarios
- Dreossi et al. (2019): VERIFAI: A Toolkit for the Formal Design and Analysis of Artificial Intelligence-Based Systems