Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

An abstract model for proving safety of autonomous urban traffic

Maike Schwammberger

Department of Computing Science, University of Oldenburg, Germany

ARTICLE INFO

Article history:
Received 13 April 2017
Received in revised form 11 May 2018
Accepted 22 May 2018
Available online xxxx

Keywords:
Multi-dimensional spatial logic
Urban traffic
Virtual lanes
Autonomous cars
Collision freedom
Timed automata

ABSTRACT

With *Multi-lane Spatial Logic* (MLSL), we can prove safety (collision freedom) on multi-lane motorways and country roads. In this work, we consider an extension of MLSL to deal with urban traffic scenarios, thereby focusing on crossing manoeuvres at intersections. To this end, we modify the existing abstract model by introducing a generic topology of urban traffic networks. We then show that even at intersections we can use purely spatial reasoning, detached from the underlying car dynamics, to prove safety of controllers modelled as extended timed automata.

1. Introduction

Traffic safety is a relevant topic as driving assistance systems and fully autonomously driving cars are increasingly capturing the market. In this context, safety means collision freedom and thus reasoning about car dynamics and spatial properties. An example for such a spatial property could be the information that two cars are positioned one behind the other, while an example for a dynamic property is the exact position of a car after some time elapsed, in general calculated as an integral of its speed. A lot of research approaches in the field of autonomous driving use hybrid automata to handle such dynamic aspects. But these complex hybrid models are hard to reason about and to verify.

An approach to separate the car dynamics from the spatial considerations and thereby to simplify reasoning, was introduced in [1] with the Multi-lane Spatial Logic (MLSL) for expressing spatial properties on multi-lane motorways with one driving direction for all cars. This logic and its dedicated abstract model was extended with length measurement in [2] for country roads to reason about the distance to oncoming traffic. The authors informally introduced respective controllers for lane change manoeuvres on motorways and country roads. These controllers use formulas of MLSL to reason about traffic situations and to decide if a car can safely change lanes.

Aside from highway traffic and country roads, safety in urban traffic scenarios is of high importance. In urban traffic, lane intersections are especially critical as cars enter them from various directions. Thus, our approach focuses on intersections. Since the purely spatial reasoning with MLSL is very convenient for verification, we reuse the approaches of [1] and [2] by extending them to our urban traffic manoeuvres. For this, we extend the abstract model and also the logic MLSL and

E-mail address: schwammberger@informatik.uni-oldenburg.de.

https://doi.org/10.1016/j.tcs.2018.05.028
0304-3975/© 2018 Published by Elsevier B.V.

additionally introduce extended timed automata [3] to construct controllers for turn manoeuvres at intersections. Finally, we prove the safety of these controllers.

The existing abstract model from [1] and [2] consists of adjacent lanes of infinite length. This is no longer sufficient for urban traffic, as we deal with intersecting lanes, where the intersections are critical parts of the model as traffic participants coming from different directions wish to enter them. We therefore consider finite lane segments and introduce special constructs for the intersection segments of the abstract model. We introduce a generic graph topology, comparable with the abstraction of a street map, capable of representing n-by-m intersections, where a road with n lane segments meets a road with m lane segments. For statements about the safety of one distinct car, we do not consider traffic situations throughout the whole topology, but focus on the local surroundings of that car by considering a dedicated *view*. For urban traffic with arbitrary sized intersections, we introduce virtually flattened views to cope with turning at intersections. We then extend MLSL by a formalism to express intersection segments with our *Urban Multi-lane Spatial Logic* (UMLSL). With this logic, we can reason about traffic situations in a view. We finally introduce syntax and semantics of *automotive-controlling timed automata* (ACTA) to construct a crossing controller which uses UMLSL formulas to determine if an intersection can safely be passed. Over the semantics of UMLSL and ACTA, we prove safety of our crossing controller.

The structure of this contribution is as follows. In Sect. 2 we discuss related work, including different approaches regarding the logical part and other traffic scenarios, some from automotive and some from other traffic domains. We introduce the extended abstract model and logic UMLSL in Sect. 3, followed by Sect. 4, where we introduce syntax and semantics of our extended timed automata and construct the crossing controller for turn manoeuvres. Finally, we prove safety of this crossing controller in Sect. 5. We conclude with a short summary and some notes on recent and future work in Sect. 6.

This paper extends the conference paper [4] by several new segments:

- We extend the abstract model to more complex intersections, which requires additional definitions and changes of several concepts from [4] throughout the paper. We use the Z specification language for the definitions [5].
- We add running examples in several subsections.
- *Sect. 2:* In a distinct related work section, we differentiate our own approach from existing formalisms for spatial and temporal logics and from other approaches on traffic safety.
- *Sect. 3 (Abstract model)*
  - *Sect. 3.1:* We extend the topology to more complex intersections, thus introducing definitions for a coarser version of the topology, a path definition and topological sanity conditions.
  - *Sect. 3.3:* The virtual view construction is completely redefined to cope for the more complex intersections from Subsect. 3.1. In contrast to [4], we give formal definitions for the concepts.
  - *Sect. 3.4:* We introduce a multi-view UMLSL semantics.
- *Sect. 4:* We add motivation and description.
- *Sect. 5:* The former proof sketch is extended to a formal mathematical proof.
- *Sect. 6:* We add more detailed future work concepts.

2. Related work

In this section, we first discuss related work on spatial logic. Then we present further approaches on different aspects of MLSL, like decidability and undecidability results and MLSL case studies. We continue with differing approaches to the safety of traffic manoeuvres, concentrating on formalisms for urban traffic manoeuvres at intersections, but also mentioning approaches for domains other than automotive.

Related work on temporal and spatial logics. Interval temporal logic (ITL) [6] and Duration Calculus (DC) [7] both allow for one-dimensional reasoning by specification of temporal intervals. With these intervals, one can e.g. specify system states happening one after the other. Shape Calculus [8] extends Duration Calculus by more dimensions as it allows an arbitrary amount of spatial and temporal dimensions.

Taking up this idea of a multidimensional logic, MLSL and its derivatives, including the here proposed urban logic, extend ITL and DC by a second dimension, whilst considering continuous (positions on lanes) and discrete components (the number of a lane). With these two-dimensional features we can, for instance, express that a car is occupying a certain space on a lane.

However, all versions of MLSL are not comparable to Shape Calculus, as they are created for a specific field of application: motorway traffic, country roads, or urban traffic. To this end, MLSL allows for quantification over cars, which is not implementable in Shape Calculus. Therefore, a reduction of MLSL to a decidable subset of Shape Calculus is not possible.

Other approaches with MLSL. While the MLSL approach profits from the fact that spatial aspects are considered detached from the car dynamics, it is of great interest to relate the purely spatial reasoning to car dynamics and thus link the approaches