Distributed Controllers for Provably Live and Safe Car Manoeuvres on Freeways and in Urban Traffic

Maike Schwammberger[1]

1 Motivation

During the last years, driving assistance systems and fully autonomously driving cars are increasingly capturing the market worldwide. Consequently, it is of the utmost importance, to ensure certain functional properties of these autonomous systems, e.g. safety, meaning collision freedom with other traffic participants at any time. A first safety challenge is that it is not sufficient to consider one car isolated from its surroundings, but to consider a network of distributed mobile agents, possibly interacting with each other from time to time, e.g. via communication channels.

Reasoning about collision freedom involves car dynamics and spatial properties. An example for such a spatial property is 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 has elapsed, in general calculated as an integral of its speed.

One solution that uses purely logical reasoning on spatial aspects of traffic situations while being detached from the dynamics is the *Multi-lane Spatial Logic (MLSL)* approach [Hi11]. While [Hi11] focuses on safety of car manoeuvres in freeway traffic, extensions, e.g. to urban traffic [Sc17, Sc18a], have been proposed. Besides safety, recent work was done [Sc18b] on analysing safety and liveness aspects of the MLSL car controllers using the UPPAAL model checker [BDL04].

2 A short introduction to the Multi-lane Spatial Logic

The core of the MLSL approach is the logic itself, making it possible to have concise logical statements about traffic situations with a clear formal semantics. However, the overall approach can be divided into three central parts:

- **Abstraction:** An Abstract Model of real-world road structures, cars and their perception of other traffic participants. The abstract model includes a view, where only cars in an area around an active *ego car* are considered for reasoning about safety of that car. This significantly simplifies the state space that needs to be considered and is motivated by reality as only cars around the ego car might endanger its safety.

[1] University of Oldenburg, Department of Computing Science, Ammerländer Heerstraße 114–118, 26129 Oldenburg, Germany schwammberger@informatik.uni-oldenburg.de

- **Logic:** Reasoning about specific traffic situations in the Abstract Model, precisely in the view around the ego car. In MLSL, we formalise safety of ego by the formula

  $$Safe\,(ego) \;\equiv\; \neg\exists c\colon c \neq ego \wedge \langle re(ego) \wedge re(c)\rangle,$$

  where the atom $re(ego)$ formalises the *reservation* of the ego car, which is the space the car occupies on the road at one moment.
- **Application of the logic:** Extended timed automata controllers use the logic to implement protocols for traffic manoeuvres that are provably live and safe. The safety formula holds invariantly in our traffic manoeuvre controllers.

3 Conclusion, explainability and open questions

The strength of our approach is its concise formal semantics of both logic and controllers. While a network of the several controllers running in parallel can be very big and difficult to understand manually, wanted or unwanted behaviour of our controllers can be analysed and explained by using model checking tools, e.g. as done in [Sc18b] with UPPAAL. However, due to a huge state space only a limited number of cars is considered there.

Also, the purely formal approach comes at the cost of a high level of abstraction from the real world. While [ORW17] brings MLSL back together with the car dynamics, certainly, it needs to be considered whether our assumptions about the abstract model are reasonable and which steps we can take to weaken some of them without losing expressiveness.

For this and to increase analysability and thus explainability of our model and controllers, the work done in other topics around autonomous driving, but also from other diciplines is to be considered.

References

[BDL04] Behrmann, Gerd; David, Alexandre; Larsen, Kim G.: A Tutorial on Uppaal. In (Bernardo, Marcoand Corradini, Flavio, ed.): Formal Methods for the Design of Real-Time Systems. Springer, Berlin, Heidelberg, pp. 200–236, 2004.

[Hi11] Hilscher, Martin; Linker, Sven; Olderog, Ernst-Rüdiger; Ravn, Anders P.: An Abstract Model for Proving Safety of Multi-lane Traffic Manoeuvres. In (Qin, Shengchao; Qiu, Zongyan, eds): Formal Methods and Software Engineering: 13th ICFEM. Springer Berlin Heidelberg, pp. 404–419, 2011.

[ORW17] Olderog, Ernst-Rüdiger; Ravn, Anders P.; Wisniewski, Rafael: Linking spatial and dynamic models, applied to traffic maneuvers. In (Hinchey, Mike; Bowen, Jonathan P.; Olderog, Ernst-Rüdiger, eds): Provably Correct Systems, NASA Monographs in System and Software Engineering, pp. 95–120. Springer, 2017.

[Sc17] Schwammberger, Maike: Imperfect Knowledge in Autonomous Urban Traffic Manoeuvres. In: Proceedings First Workshop on Formal Verification of Autonomous Vehicles, FVAV@iFM 2017, Turin, Italy, 19th September 2017. pp. 59–74, 2017.

[Sc18a] Schwammberger, Maike: An abstract model for proving safety of autonomous urban traffic. Theoretical Computing Science, 744:143–169, 2018.

[Sc18b] Schwammberger, Maike: Introducing Liveness into Multi-lane Spatial Logic lane change controllers using UPPAAL. In (Gleirscher, Mario; Kugele, Stefan; Linker, Sven, eds): Proceedings SCAV@CPSWeek 2018. volume 269 of EPTCS, pp. 17–31, 2018.