Verifying the Safety of Lane Change Maneuvers of Self-driving Vehicles Based on Formalized Traffic Rules

Christian Pek[1], Peter Zahn[1], and Matthias Althoff[2]

***Abstract*— Validating the safety of self-driving vehicles requires an enormous amount of testing. By applying formal verification methods, we can prove the correctness of the vehicles' behavior, which at the same time reduces remaining risks and the need for extensive testing. However, current safety approaches do not consider liabilities of traffic participants if a collision occurs. Utilizing formalized traffic rules to verify motion plans allows this problem to be solved. We present a novel approach for verifying the safety of lane change maneuvers, using formalized traffic rules according to the Vienna Convention on Road Traffic. This allows us to provide additional guarantees that if a collision occurs, the self-driving vehicle is not responsible. Furthermore, we consider misbehavior of other traffic participants during lane changes and propose feasible solutions to avoid or mitigate a potential collision. The approach has been evaluated using real traffic data provided by the NGSIM project as well as simulated lane changes.**

I. Introduction

A. Motivation

Safety is the most important aspect in the success of self-driving vehicles. More specifically, the desired goal is that such vehicles drive more safely than humans, i. e. that fewer fatalities and crashes occur. For example, American drivers drove nearly 3 trillion miles in 2015 with 2.3 million reported injuries [1], corresponding to 0.77 injuries per 10^6 miles.

In order to be proven more reliable than humans, self-driving vehicles require a total of 3.9 million test miles to verify that their failure rate is at most the failure rate of human drivers according to [2]. Showing that the failure rate is significantly lower compared to humans demands about 161 million test miles, which would take a fleet of 100 self-driving vehicles 7.3 years of 24/7 driving. Note that these numbers are based on the total number of reported injuries and not the absolute number of fatalities.

As a consequence, sophisticated approaches are needed to verify the behavior of self-driving vehicles. For this purpose, formal verification methods can prove the correctness of the desired behavior of self-driving vehicles for a given model. Using such methods reduces the need for extensive testing, since certain aspects to be tested are provably correct with respect to the specification, Thus, testing would only be required to check whether the set of specifications is sufficient.

[1]Christian Pek and Peter Zahn are with BMW Group, D-85748 Garching, Germany, christian.pek@bmw.de and peter.zahn@bmw.de

[2]Matthias Althoff is with the Department of Computer Science, Technical University Munich, D-85748 Garching, Germany althoff@in.tum.de

B. Literature Review

Safety in the context of self-driving vehicles denotes the ability to respect road boundaries and to avoid collisions with obstacles and other traffic participants. In [3], three criteria to achieve safe motion plans are introduced: a robotic vehicle should consider "*its own dynamics*", the "*environment objects future behavior*", and "*reason over an infinite time horizon*". The last aspect in particular is computationally intense and hard to accomplish due to inaccuracies in the prediction of dynamic obstacles.

For this reason *Partial Motion Planning* [4] has been established, which is similar to a sliding window approach [5] over the planned path and allows one to use finite time horizons t_H. Common approaches, e. g. [6]–[8], involve planning trajectories, which are checked for intersections with obstacles within the horizon t_H. Still, the safety of the vehicle cannot be guaranteed for an infinite time horizon.

In [9], the concept of *Inevitable Collision States* (ICS) has been proposed. An ICS is an unsafe state in which the self-driving vehicle, no matter what trajectory it follows, eventually collides with an obstacle [10]–[12]. The motion plan of the ego vehicle is safe if it avoids ICS at any time.

Control Invariant Sets (CIS) [13] represent a contrary approach to ICS. By definition, for every state within a CIS there exists at least one feasible trajectory which keeps the system within the set indefinitely long; in [14] the concept has been applied to UAVs. ICS and CIS are computationally intense, since at worst every feasible trajectory must be checked. For that reason, most works focus on a discrete subset of trajectories, e. g. braking maneuvers.

Reachability Analysis can be applied to take any feasible future behavior of other traffic participants into account [15], [16]. Calculating the reachable set of each vehicle (including the ego vehicle) and comparing the intersection of the obtained sets allows possible future collisions to be identified [17]. Furthermore, reachability analysis enables one to assess the feasibility of planned maneuvers [18].

In [19], *Multi-lane Spatial Logic* (MLSL) is used to verify the safety of lane change maneuvers. They consider that vehicles reserve a certain space on the lane and evaluate whether the reserved spaces of all vehicles are disjoint at any time. Using MLSL allows them to verify the correctness of their developed lane change controller. Still, MLSL expressions are complex, and the vehicle must utilize the controller used in the verification.

The verification of lane change maneuvers can also be done by applying game theory and logical reasoning [20]. The proposed control strategy allows the vehicle to safely

enter highways even under hard time constraints. However, the approach is only applicable if all vehicles are self-driving and able to communicate via *Car2Car* communication.

In addition to avoiding collisions, the aforementioned approaches do not consider the question of liability. Researchers apply formalized traffic regulations to solve this problem, e. g. in [21]. If a collision occurs and the ego vehicle has respected the traffic rules at all times, it can be deduced that another traffic participant must have violated the rules and thus caused the collision (assuming that collisions are impossible if everybody respects all traffic rules). The ego vehicle therefore is not responsible for the collision. Although traffic rules are more detailed than other laws, they are still abstract or inconsistent in some areas [22], which can be addressed by concretizing the rules.

C. Contribution

This work verifies the safety of lane change maneuvers. We therefore focus on the intended motion plan and assume redundant hardware, allowing us to ignore hardware faults for the subsequent discussion. Furthermore, we consider any kind of vehicle-operation. The verification is done by applying formalized traffic rules and determining safe states in vehicle convoys according to the Vienna Convention on Road Traffic.

The developed verification method not only allows one to assess the safety of maneuvers, but also provides accountability. Our approach guarantees that the self-driving vehicle is not responsible for the collision. Furthermore, we consider possible misbehavior of other traffic participants and propose feasible solutions to avoid or mitigate a potential collision.

II. Safety Derived From Traffic Rules

Concretized traffic rules can be used to determine if a self-driving vehicle is in a safe state or even if a planned lane change maneuver can be safely executed. For that purpose, we use the *Vienna Convention on Road Traffic* [23] adopted by 74 countries. The convention not only specifies abstract general rules, such as the existence of speed limits, but also detailed rules, e. g. requirements for safe overtaking or safe distances between vehicles. As traffic rules are formulated in natural language, they must be mathematically defined in a precise and sound way beforehand.

A. Models and Assumptions

Without loss of generality, we model lanes as paths. This means that the 2d-position $(x, y)^T \in \mathbb{R}^2$ of a vehicle will be described by the arc length $d \in \mathbb{R}$ (cf. Fig. 2). This abstraction can be made since the longitudinal occupancy of vehicles within a lane is sufficient for showing whether a lane change is safe or not. We use a curvilinear coordinate system that is aligned with the driving direction of the lane.

The indices l and f denote the leading or following vehicle of the ego vehicle inside a lane. To check for collisions, one has to consider the dimensions of vehicles. For the sake of clarity, we omit the usage of length/width offsets to a vehicle's position in order to describe its occupancy inside a lane. We assume that the initial time is $t_0 = 0$. Furthermore, we denote t_{lc} as the time required for the planned lane change and $T_{lc} = [t_0, t_{lc}]$ as the corresponding time interval. We use v to describe the velocity and a to describe the acceleration of a vehicle.

For our own planning, we assume that if the maneuver is proven formally safe w. r. t. [23] and a collision has occurred nonetheless, another vehicle must be liable. In addition, the following time-independent assumptions are made:

- A1) Only uni-directional multi-lane highways are considered, i. e. the velocity of vehicles is non negative $\forall t \geq 0 : v \geq 0$.
- A2) The maximum absolute acceleration a_{max} of each traffic participant is known a priori and is applicable throughout the duration of the lane change.
- A3) The initial state of the ego vehicle prior to the lane change is safe (cf. Sect. I-B).
- A4) The positions of vehicles that are safety-relevant during the lane change are fully observable.

For the future motion of other traffic participants, we make the following time-dependent assumptions (inspired by [24]):

- P1) The positive longitudinal acceleration of vehicles is stopped if a maximum velocity v_{max} is reached.
- P2) The limited engine power of a vehicle in driving direction is modeled as $a = a_{\text{max}} \frac{v_s}{v}$, where v_s is a parameterized switching velocity.
- P3) Vehicles may perform emergency brake maneuvers with $-a_{\text{max}}$ at any time.
- P4) Leading and following vehicles remain in their lane during the lane change of the ego vehicle (cf. [23]).

B. Formalizing Safe Distances

The Vienna Convention defines the safe distance between two vehicles as a *"sufficient distance [...] to avoid [a] collision if the vehicle in front should suddenly slow down or stop"* [23, §13]. Consequently, the safe distance $d_{\text{safe}} > 0$ to a leading vehicle B_l must be large enough for the ego vehicle to stop behind it if B_l, at worst, performs an *emergency brake* with $a_{\text{max},l}$ (cf. motion assumption P3) as formalized in [25].

We briefly recall the results of [25]: The future position of a vehicle for a point in time $t \geq 0$ can be described by the general motion equation

$$d(t) = d_0 + vt + \frac{1}{2}at^2, \tag{1}$$

where $d_0 \in \mathbb{R}$ denotes the position of the vehicle at t_0. The ego vehicle collides with a leading vehicle B_l if their positions are equal for some $t \geq 0$:

$$\exists t \geq 0 : d_{\text{ego}}(t) = d_l(t). \tag{2}$$

In a subsequent work, the authors of [25] proposed an extension of the safe distance definitions, which takes reaction times $\delta \geq 0$ into account. According to that, the minimum required safe distance between the two vehicles depends on the condition

$$\begin{aligned} &d_l(\delta) \leq u_{\text{max,ego}} \wedge |a_{\text{max},l}| < |a_{\text{max,ego}}| \\ &\wedge\, v_l^* < v_{\text{ego}} \wedge t_{\text{stop,ego}} < t^*_{\text{stop},l}, \end{aligned} \tag{3}$$

where $u_{\max,\text{ego}}$ is the stopping distance of the ego vehicle including the reaction time δ, v_l^* is the velocity of B_l at time δ after starting emergency braking, and $t^*_{\text{stop},l} = v_l^*/|a_{\max,l}|$ and $t_{\text{stop,ego}} = v_{\text{ego}}/|a_{\max,\text{ego}}|$ are the stopping times of the vehicles. If condition (3) is true, one has to use the safe distance $d_{\text{safe},1}$ otherwise $d_{\text{safe},2}$:

$$\begin{aligned} d_{\text{safe},1} &= \frac{(v_l - |a_{\max,l}|\delta - v_{\text{ego}})^2}{-2(|a_{\max,l}| - |a_{\max,\text{ego}}|)} - v_l\delta + \frac{1}{2}|a_{\max,l}|\delta^2 \\ &\quad + v_{\text{ego}}\delta \\ d_{\text{safe},2} &= \frac{v_l^2}{-2|a_{\max,l}|} - \frac{v_{\text{ego}}^2}{-2|a_{\max,\text{ego}}|} + v_{\text{ego}}\delta \end{aligned} \tag{4}$$

The authors verified their results by using higher-order logic and the theorem prover *Isabelle* [26]. After introducing the relative distance $d_{\text{rel}} = d_l - d_{\text{ego}}$, we can conclude that the ego vehicle respects the safe distance to the leading vehicle B_l if the condition

$$\big((d_{\text{rel}} > d_{\text{safe},1} \wedge (3)) \vee (d_{\text{rel}} > d_{\text{safe},2} \wedge \neg(3))\big) \tag{5}$$

holds.

C. Determining Safe States

With respect to a leading vehicle B_l with position $d_l > d_{ego}$, a safe state of the ego vehicle with position $d_{\text{ego}}(t), t \geq 0$ is defined as

$$d_{\text{ego}}(t) < d_l(t) - d_{\text{safe},l}(t), \tag{6}$$

where $d_{\text{safe},l}$ corresponds to the safe distance to B_l. Similarly, a safe distance with respect to a following vehicle B_f with position $d_f < d_{\text{ego}}$ at time $t \geq 0$ is defined as

$$d_f(t) + d_{\text{safe},f}(t) < d_{\text{ego}}(t). \tag{7}$$

The safe distance $d_{\text{safe},f}$ in (7) is derived from the velocity v_{ego} of the ego vehicle, giving the following vehicle B_f the chance to brake without colliding with the ego vehicle. By combining (6) and (7), the safe free space $\mathcal{S}^t$ of the ego vehicle for a point in time $t \geq 0$ is defined as

$$\mathcal{S}^t = \{d \in \mathbb{R} \,|\, d_f(t) + d_{\text{safe},f}(t) < d < d_l(t) - d_{\text{safe},l}(t)\}. \tag{8}$$

If a following (or leading) vehicle does not exist (cf. assumption A4), we set $d_{\text{safe},f} \to -\infty$ (or $d_{\text{safe},l} \to \infty$, respectively). Fig. 1a visualizes the time-varying free space in (8) for an ego vehicle positioned between a leading and a following vehicle as a shaded area.

If the ego vehicle is continuously driving within this free space, i. e. $\forall t \geq 0 : d_{\text{ego}}(t) \in \mathcal{S}^t$, safety is guaranteed for an infinite time horizon $t \to \infty$ (cf. [27], [28]). Additionally, the question of liability of the ego vehicle can be answered. If a collision occurs, at least one vehicle must have violated the safe distance and hence caused the collision. As driving in $\mathcal{S}^t$ implies keeping safe distances, the ego vehicle is not responsible for the collision.

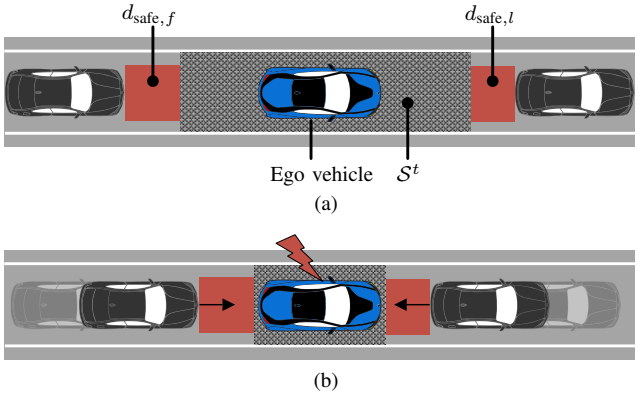

Fig. 1. Visualization of safe free space $\mathcal{S}^t$: (a) the *safe* free space (shaded area) and the safe distances (red area) of a leading and following vehicle and (b) collisions might be inevitable if the leading vehicle brakes and the following vehicle accelerates.

D. Liability Trade-offs

There are situations in which maintaining the safety of the passengers involves a liability trade-off. For instance, if B_l is continuously braking and B_f is continuously accelerating (cf. Fig. 1b), a collision might be inevitable. This scenario can be found e. g. at the end of a tailback on motorways. If the ego vehicle adjusts its velocity to respect the safe distance to B_l in this situation, and B_f would crash into the ego vehicle, B_f is legally speaking at fault for the collision.

But, in order to protect passengers, the goal for the ego vehicle might be to mitigate a collision by decreasing the relative velocity to B_f and B_l. This can be done by adjusting its own velocity v_{ego} to $v^*_{ego} = (v_f + v_l)/2$ as soon as the situation has been detected. In case $v^*_{ego} > v_{ego}$, the necessary safe distance $d_{\text{safe},l}$ to B_l has to be increased (cf. (4)). However, the ego vehicle may no longer be able to respect $d_{\text{safe},l}$, as the deceleration of B_l decreases the relative distance (cf. Fig. 1b and (5)). Thus, there is a risk of a collision with the leading vehicle during the mitigation maneuver.

We recommend that the ego vehicle has the option to lower the total arising damage of the rear-collision by risking a collision with its leading vehicle. This particular problem requires the legislative power to refine the traffic rules for autonomous vehicles.

III. Safety of Lane Change Maneuvers

During lane change maneuvers, two adjacent lanes l_c (current) and l_d (desired) have to be considered. We introduce $T_c \subset T_{lc}$ and $T_d \subset T_{lc}$ as the time intervals during which the occupancy of the ego vehicle is located in lane l_c and l_d, respectively. In order to verify the safety, we have to show that the ego vehicle is driving within the respective safe spaces, $\mathcal{S}^t_c$ in l_c and $\mathcal{S}^t_d$ in l_d, at any time $t \in T_{lc}$ during the lane change (cf. Fig. 2), i. e.

$$\forall t \in T_c : d_{\text{ego}}(t) \in \mathcal{S}^t_c \wedge \forall t \in T_d : d_{\text{ego}}(t) \in \mathcal{S}^t_d. \tag{9}$$

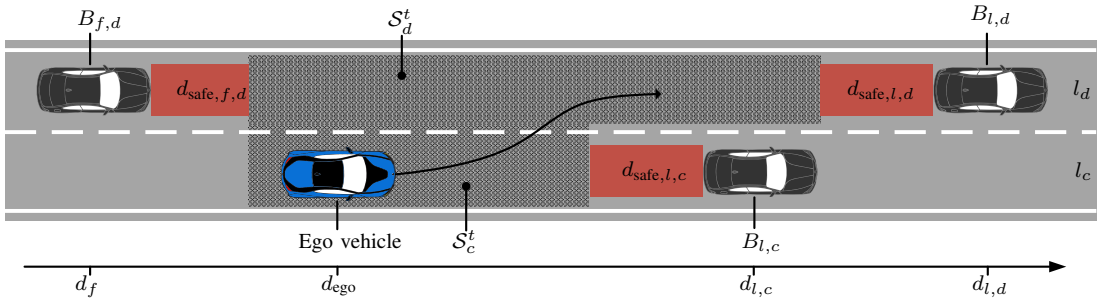

Fig. 2. Visualization of a lane change maneuver: The ego vehicle with position d_{ego} driving in lane l_c with a leading vehicle $B_{l,c}$ wants to change to lane l_d. This lane contains two vehicles, $B_{f,d}$ and $B_{l,d}$. The safe distances are illustrated in red and the safe free spaces as shaded area.

Other traffic participants may accelerate or decelerate during the lane change of the ego vehicle. However, regarding the safety verification, we only have to consider future motions, which reduce the safe free space $\mathcal{S}^t$ during the maneuver, i. e. decelerations of leading vehicles and accelerations of following vehicles (cf. Fig. 2). In the first case, it is sufficient to respect the safe distance to leading vehicles as this implies that the ego vehicle can adjust its speed to compensate for a sudden deceleration (per definition even for emergency braking).

In the case of accelerating following vehicles, we have to calculate with a full longitudinal acceleration of the following vehicle. As there are no regulations about when and how a following vehicle has to react to a merging (leading) vehicle, one has to assume that in the worst case it first reacts to the ego vehicle if it has completed the lane change. Based on motion assumptions P1 and P2, the positive longitudinal acceleration (decelerating and emergency braking are not touched by this) of a vehicle is defined as a function of their current velocity

$$a(v) = \begin{cases} \gamma a_{\max} & \text{if } 0 \leq v < v_s \\ \gamma a_{\max} \frac{v_s}{v} & \text{if } v_s \leq v < v_{\max} \\ 0 & \text{if } v_{\max} \leq v \end{cases} \tag{10}$$

where v_s is a parameterized switching velocity as described in [29] (e. g. v_s=4.755 m/s), $a_{\max}$ corresponds to the maximal feasible acceleration of the vehicle and $\gamma \in [0, 1]$ is a user-defined parameter to adjust the resulting acceleration. By setting $\gamma < 1$, one can incorporate the assumption, that the following vehicle is only allowed to accelerate to a limited extent. If the following vehicle violates assumption P1, we set its acceleration to $a_{\max}$. The velocity $v_{\max}$ corresponds to the speed limit multiplied by a speeding factor $\alpha > 1$. We use $\overline{v}_f$ as an over-approximation of the vehicles' velocity to account for sensor inaccuracies.

As soon as the ego vehicle has fully entered a lane, the following vehicle in this lane has to respect a safe distance to the ego vehicle according to the Vienna Convention on Road Traffic [23]. Nevertheless, the ego vehicle has to consider this safe distance to $B_{f,d}$ while changing lanes in order to not directly merge in front of vehicle $B_{f,d}$.

A. Enabling Dynamic Driving Behavior

The driving behavior of the ego vehicle during the lane change is limited to the size of $(\mathcal{S}_c^t \cup \mathcal{S}_d^t)$. This means that a larger free space allows the ego vehicle to drive more dynamically, i. e. by applying higher lateral accelerations a_y as well as longitudinal accelerations a_x. The size of $\mathcal{S}_c^t$ may be enlarged by enabling the vehicle to cut the safe distance $d_{\text{safe},l,c}$ to $B_{l,c}$ (cf. Fig. 3).

Instead of braking, the ego vehicle can perform an evasive maneuver to l_d if $B_{l,c}$ performs an emergency brake maneuver. However, the free space required by the evasive maneuver to l_d must not be occupied by other vehicles during the maneuver. The safe distances in (4) are based on the assumption that $B_{l,c}$ may suddenly perform an emergency brake maneuver (cf. motion assumption P3). $B_{l,c}$ requires the time $t_{\text{stop},l,c} = \underline{v}_{l,c}/|a_{\max,l,c}|$ to come to a full stop after starting the emergency brake maneuver.

We denote $y_{\text{eva}} > 0$ as the lateral distance needed to fully enter l_d, i. e. the distance between the center of l_d and the center of l_c (coordinate system depicted in Fig. 3). The required time t_{eva} to perform a steering maneuver using the maximum feasible lateral acceleration $a_{\max,y}$ of the ego vehicle corresponds to

$$t_{\text{eva}} = \sqrt{\frac{2y_{\text{eva}}}{a_{\max,y}}} + \delta_{\text{steer}}, \tag{11}$$

where $\delta_{\text{steer}} \geq 0$ is the reaction time needed to execute steering. Note that $a_{\max,y}$ depends on the road friction coefficient μ as well as *Kamm's circle* $a_{\max}^2 = a_{\max,x}^2 + a_{\max,y}^2$.

Using (1), we are able to determine a minimum relative distance necessary for a collision-free evasive maneuver to l_d. The traveled distance of $B_{l,c}$ during the time interval $[0, t_{\text{eva}}]$ after starting emergency braking corresponds to

$$\Delta x_{l,c}(t) = \begin{cases} \underline{v}_{l,c} t_{\text{eva}} - \frac{1}{2}|a_{\max,l,c}| t_{\text{eva}}^2 & \text{if } t_{\text{eva}} \leq t_{\text{stop},l,c} \\ \underline{v}_{l,c} t_{\text{stop},l,c} - \frac{1}{2}|a_{\max,l,c}| t_{\text{stop},l,c}^2 & \text{if } t_{\text{stop},l,c} < t_{\text{eva}}, \end{cases}$$

where $\underline{v}_{l,c}$ is an under-approximation of the vehicle's velocity at time t to account for sensor inaccuracies. During the same time interval, the ego vehicle travels $\Delta x_{\text{ego}} = \overline{v}_{\text{ego}} t_{\text{eva}}$, where $\overline{v}_{\text{ego}}$ is an over-approximation of the ego vehicles' velocity during the evasive-maneuver.

If $\Delta x_{\text{ego}} > \Delta x_{l,c}$ holds, the ego vehicle has to respect a safe evasive distance $d_{\text{rel,eva}} = \Delta x_{\text{ego}} - \Delta x_{l,c}$ to $B_{l,c}$. Otherwise, $d_{\text{rel,eva}} = 0$ as the traveled distance of $B_{l,c}$ is higher than the required distance of the evasive maneuver

$$d_{\text{rel,eva}}(t) = \begin{cases} \Delta x_{\text{ego}} - \Delta x_{l,c}(t) & \text{if } \Delta x_{\text{ego}} > \Delta x_{l,c} \\ 0 & \text{if } \Delta x_{\text{ego}} \leq \Delta x_{l,c}. \end{cases} \quad (12)$$

Hence, the ego vehicle has to fulfill

$$\forall t \in T_c : d_{\text{ego}}(t) < d_{l,c}(t) - d_{\text{rel,eva}}(t) \quad (13)$$

while it is driving in l_c. The ego vehicle has to start the dynamic lane change to l_d at latest when it can no longer respect the safe evasive distance $d_{\text{rel,eva}}$.

Fig. 3 visualizes the safe evasive distance for an ego vehicle positioned behind a leading vehicle. Note that braking (cf. Sect. II-B) is preferred if one cannot assure that the free space required by the evasive maneuver is not occupied during the time of the maneuver or if $d_{\text{rel,eva}} > d_{\text{safe},l,c}$ as braking can be executed at a later point in time than evading (cf. similar discussion in [30]). Whereas evading is advantageous if it can be executed at a later point in time or if the ego vehicle is not able to respect the required safe distance, e. g. a vehicle merges in front of the ego vehicle as regarded in Sect. III-B.

B. Misbehavior of Traffic Participants

The presented verification assumes that leading and following vehicles remain in their lane during the lane change of the ego vehicle (cf. motion assumption P4 and [23]). However, if traffic participants violate this assumption, (9) becomes invalid. This may be the case in the following scenarios:

- M1) A leading or following vehicle performs a lane change after the ego vehicle has started its lane change (cf. situations (a) in Fig. 4).
- M2) Vehicles, neither located on l_c or l_d, merge into the safe space during the lane change and become the new leading or following vehicle in this lane (cf. situations (b) in Fig. 4).
- M3) A following vehicle fully accelerates and thus closes the gap on its lane during the lane change (cf. situation (c) in Fig. 4).

Scenario M1 to M3 consider leading and following vehicles on any lane that is relevant for the lane change maneuver, i. e. have an influence on the ego vehicle's maneuver by modifying the safe free space $(\mathcal{S}_c^t \cup \mathcal{S}_d^t)$. For the solutions to M1 and M2, we will focus on leading vehicles. However, the presented solutions can be applied to following vehicles in a similar manner. In this case, one must calculate with a positive acceleration.

a) Misbehavior M1: In terms of misbehavior M1, the roles of vehicles (leading or following) may vary during the lane change, e. g. $B_{l,c}$ becomes $B_{l,d}$. We denote t_d as the time of detecting the misbehavior and Δt as the maximum time in which the ego vehicle must have entered the safe space again. We determine if the ego vehicle is able to regain safety by applying a *feasible* and *collision-free* trajectory with a braking profile $a_{\text{ego}} : [t_d, t_d + \Delta t] \rightarrow [-a_{\text{max,ego}}, 0]$, such that $\forall t \geq (t_d + \Delta t)$ (9) holds. Larger values of Δt allow the motion planner to determine more comfortable braking profiles.

In case we cannot determine a feasible a_{ego}, a potential collision might be imminent. If lane l_c is no longer occupied due to the lane change of $B_{l,c}$, the ego vehicle can execute a combined braking and steering maneuver back to l_c while considering safe distances to vehicles in l_c. However, if the required free space for the evasive maneuver on l_c is already occupied by another vehicle (e. g. $B_{f,c}$), the ego vehicle must execute an emergency brake maneuver with $-a_{\text{max,ego}}$ in order to avoid or mitigate a collision.

b) Misbehavior M2: In terms of misbehavior M2, the ego vehicle executes the aforementioned solutions. However, it is also able to determine a positive acceleration to overtake the merging vehicle, so that it can merge behind the ego vehicle. Furthermore, based on $d_{\text{ego}}(t_d)$, the evasive maneuver can be modified as follows: Considering a vehicle merging to l_d, if the ego vehicle is still driving on l_c (i. e. $t_d \notin T_d$), it cancels the lane change and remains in l_c. Otherwise, if it is driving in l_d (i. e. $t_d \in T_d$), the ego vehicle determines a feasible a_{ego} such that it returns to l_c and remains in l_c.

The safety of the evasive maneuver can be further enhanced if the ego vehicle imitates the lateral motion of the merging vehicle, i. e. the lateral distance between both vehicles is not decreasing over time. We recommend that the ego vehicle is allowed to disrespect safe distances during emergency situations to avoid a collision. For a vehicle merging to l_c, the ego vehicle may perform a lane change to

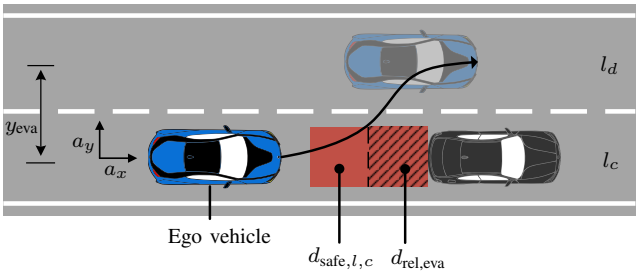

Fig. 3. The ego vehicle may cut the safe distance $d_{\text{safe},l,c}$ in order to execute a more dynamical lane change.

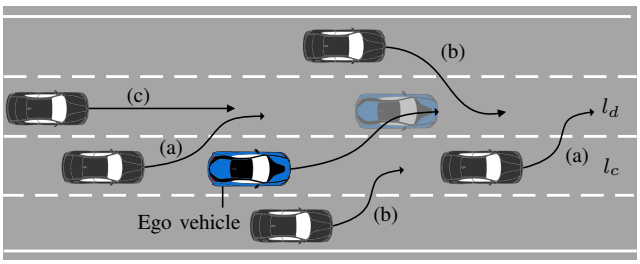

Fig. 4. Possible misbehavior: (a) following or leading vehicles change lanes directly after the ego vehicle, (b) vehicles, neither located on l_c or l_d, merge into the safe space, or (c) the following vehicle fully accelerates.

TABLE I

PERCENTAGE OF SAFE LANE CHANGES FOR VARIOUS REACTION TIMES

Data-set	n	t_{lc}	$\delta = 0.0\,\mathrm{s}$	$\delta = 0.3\,\mathrm{s}$	$\delta = 1.0\,\mathrm{s}$
$7^{50} - 8^{05}$	195	$4.03s$	62.6%	60.0%	39.0%
$8^{05} - 8^{20}$	192	$3.57s$	62.5%	60.9%	47.4%
$8^{20} - 8^{35}$	169	$4.81s$	45.0%	43.8%	33.1%

l_d rather than an uncomfortable emergency brake maneuver. Still, this requires the legislative power to refine traffic rules.

c) Misbehavior M3: Considering misbehavior M3, the ego vehicle determines a positive and collision-free acceleration profile a_{ego} to maintain the safe distance. If there is no feasible profile or if a collision is imminent, the ego vehicle performs an evasive maneuver depending on the lane of the following vehicle: If it is driving in l_c, the ego vehicle performs an evasive maneuver to l_d, otherwise to l_c.

IV. EVALUATION

The presented method has been evaluated on a data-set of recorded traffic from the *NGSIM* project [31] to investigate the safety of human driven lane changes. The data-set contains the position, speed, acceleration, and respective lane of vehicles driving on US Highway 101. It was obtained between 7:50 am and 8:35 am with a granularity of $\Delta t = 0.1\,\mathrm{s}$. The study area is $640\,\mathrm{m}$ long and consists of five lanes.

We assumed a maximum absolute acceleration of $a_{\text{max}} = 8\,\mathrm{m/s^2}$ per vehicle, a maximum velocity of $v_{\text{max}} = 16.67\,\mathrm{m/s}$, and a switching velocity $v_s = 4.755\,\mathrm{m/s}$ for the evaluation. The velocities of following and leading vehicles are over- and under-approximated by $5\,\%$, respectively. Furthermore, we make use of the safe distance extension to take reaction times into account, assuming $\delta_{\text{human}} = 1.0\,\mathrm{s}$ for humans and $\delta_{\text{machine}} = 0.3\,\mathrm{s}$ for self-driving vehicles [32]. The lane change duration t_{lc} has been determined by looking at the time that the ego vehicle requires to fully cross the lane marking based on its width. The lane changes considered in the evaluation comply with the following criteria:

1) Lane changes on the main lanes 1-5 (6,7,8 are ramps).
2) Only one lane change of the ego vehicle.
3) Complete lane change has been recorded.

The safety evaluation has been implemented using forward simulation of the vehicles' initial state. Tab. I highlights the evaluation results of $N = 556$ total lane changes for different reaction times. In terms of $\delta = 0.0\,\mathrm{s}$, an average of $56.7\,\%$ of the lane changes are classified as safe. This number will decrease to $54.9\,\%$ if δ_{machine} is used. Considering that the vehicles in the data-set were controlled by humans, only $39.83\,\%$ of the lane changes are classified as safe.

Two main reasons for an evaluation classified as *unsafe* have been identified: the ego vehicle was not able to respect the safe distance to the following vehicle $B_{f,d}$, or due to the full acceleration of $B_{f,d}$ the desired gap on l_d vanished during the lane change. We validated the correctness of our approach and implementation by simulating random emergency braking of the vehicles based on the velocity considered in the verification. Every *safe* lane change was collision-free, whereas every *unsafe* lane change resulted in a collision.

We used simulations to validate the proposed solutions to misbehaving traffic participants. Therefore, $N = 10^8$ random lane changes have been generated, including random initial states of the vehicles. Afterwards, we extracted the subset of $N_{\text{safe}} \approx 60.2 \times 10^6$ safe lane changes, classified using our approach. We applied random misbehavior according to Sec. III-B to one of the traffic participant in each scenario within the subset of safe lane changes in order to produce sudden unsafe lane changes.

Using $\Delta t = 2\,\mathrm{s}$, $\delta = \delta_{\text{human}}$, and $a_{\text{max,ego}} = 8\,\mathrm{m/s^2}$, we checked if the ego vehicle is able to regain safety in each of the scenarios. The generated misbehavior led to a number of unsafe lane changes $N_{\text{unsafe}} \approx 20.0 \times 10^6$, where $1.8\,\%$ of them were caused by M1, $73.6\,\%$ by M2, and $24.6\,\%$ by M3. Using the proposed solutions in Sec. III-B, the ego vehicle was able to avoid collisions in every situation. In $99.9\,\%$ of the cases, the ego vehicle was able to regain safety by executing a braking profile a_{ego} combined with an evasive maneuver. Thus, in only $0.1\,\%$ of the unsafe lane changes, the ego vehicle had to perform an emergency brake. We repeated our simulation multiple times to validate our findings.

V. DISCUSSION

This paper presents a novel and pragmatic approach for verifying the safety of lane change maneuvers of autonomous vehicles by incorporating formalized traffic rules. The assessment is particularly based on safe distances, allowing the ego vehicle to drive safely for an infinite time horizon. Using the developed approach and the proposed solutions to misbehavior of traffic participants, the autonomous vehicle can verify its decision to change lanes and recover if the lane change becomes unsafe during the maneuver.

Compared to other research in the area of formal verification, such as [12], [19], [20], the developed approach derives a safe free space by making direct usage of traffic rules and shows that the ego vehicle is located within this space at any time during the lane change. If a collision occurred and the self-driving vehicle has respected our approach (and thus the traffic rules), another traffic participant must have violated the traffic rules and caused the collision.

The presented method is based on straightforward algebraic equations, which in contrast to other approaches can be efficiently implemented and thus ensures fast run-times. Possible misbehavior of other traffic participants during lane changes has been considered as well, and feasible solutions to regain safety have been proposed. The presented approaches have been evaluated using real traffic data provided by the NGSIM project and simulated safe and unsafe lane changes. Additionally, our approach enables the ego vehicle to drive more dynamically during the lane change, while still guaranteeing safety.

Future work involves testing the developed approach on a self-driving vehicle for real-world validation and applying formalized traffic rules to other types of maneuvers.

ACKNOWLEDGMENTS

The authors thank Albert Rizaldi for his valuable contribution to the safe distance definitions. This work is partially funded by the German Federal Ministry of Economics and Technology through the research initiative Ko-HAF (`https://www.ko-haf.de/`).

REFERENCES

[1] Bureau of Transportation Statistics, "Motor Vehicle Safety Data," Washington, D.C.: Research and Innovative Technology Administration, U.S. Department of Transportation, Tech. Rep., 2015. [Online]. Available: http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/html/table_02_17.html

[2] N. Kalra and S. M. Paddock, "Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?" *Transportation Research Part A: Policy and Practice*, vol. 94, pp. 182–193, 2016.

[3] T. Fraichard, "A short paper about motion safety," in *Proc. of the IEEE Int. Conf. on Robotics and Automation*, 2007, pp. 1140–1145.

[4] S. Petti and T. Fraichard, "Safe motion planning in dynamic environments," in *Proc. of the IEEE Int. Conf. on Intelligent Robots and Systems*, 2005, pp. 2210–2215.

[5] R. Dahlhaus, J. Kurths, P. Maass, and J. Timmer, *Mathematical Methods in Time Series Analysis and Digital Image Processing*, ser. Understanding Complex Systems. Springer, 2008.

[6] M. Werling, J. Ziegler, S. Kammel, and S. Thrun, "Optimal trajectory generation for dynamic street scenarios in a Frenet Frame," in *Proc. of the IEEE Int. Conf. on Robotics and Automation*, 2010, pp. 987–993.

[7] J. Ziegler and M. Werling, "Navigating car-like robots in unstructured environments using an obstacle sensitive cost function," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2008, pp. 787–791.

[8] E. Frazzoli, M. A. Dahleh, and E. Feron, "Real-time motion planning for agile autonomous vehicles," in *Proc. of the American Control Conference*, 2001, pp. 43–49.

[9] T. Fraichard and H. Asama, "Inevitable collision states. A step towards safer robots?" pp. 388–393, 2004.

[10] L. Martinez-Gomez and T. Fraichard, "An efficient and generic 2D Inevitable Collision State-checker," in *Proc. of the IEEE Int. Conf. on Intelligent Robots and Systems*, 2008, pp. 234–241.

[11] D. Althoff, M. Buss, A. Lawitzky, M. Werling, and D. Wollherr, "On-line Trajectory Generation for Safe and Optimal Vehicle Motion Planning," in *Autonomous Mobile Systems*, 2012, pp. 99–107.

[12] S. Bouraine, T. Fraichard, and H. Salhi, "Provably safe navigation for mobile robots with limited field-of-views in dynamic environments," in *Proc. of the IEEE Int. Conf. on Robotics and Automation*, 2012, pp. 174–179.

[13] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747 – 1767, 1999.

[14] T. Schouwenaars, "Safe trajectory planning of autonomous vehicles," Dissertation, Massachusetts Institute of Technology, 2006.

[15] M. Althoff and J. M. Dolan, "Online Verification of Automated Road Vehicles Using Reachability Analysis," *IEEE Transactions on Robotics*, vol. 30, no. 4, pp. 903–918, 2014.

[16] ——, "Set-based computation of vehicle behaviors for the online verification of autonomous vehicles," in *Proc. of the IEEE Int. Conf. on Intelligent Transportation Systems*, 2011, pp. 1162–1167.

[17] M. Althoff, D. Althoff, D. Wollherr, and M. Buss, "Safety verification of autonomous vehicles for coordinated evasive maneuvers," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2010, pp. 1078–1083.

[18] S. Söntges and M. Althoff, "Determining the Nonexistence of Evasive Trajectories for Collision Avoidance Systems," in *Proc. of the IEEE Int. Conf. on Intelligent Robots and Systems*, 2015, pp. 956–961.

[19] M. Hilscher, S. Linker, and E.-R. Olderog, "Proving Safety of Traffic Manoeuvres on Country Roads," in *Theories of Programming and Formal Methods*. Springer, 2013, pp. 196–212.

[20] W. Damm, H.-J. Peter, J. Rakow, and B. Westphal, "Can we build it: formal synthesis of control strategies for cooperative driver assistance systems," *Mathematical Structures in Computer Science*, vol. 23, no. 04, pp. 676–725, 2013.

[21] A. Rizaldi and M. Althoff, "Formalising Traffic Rules for Accountability of Autonomous Vehicles," in *Proc. of the IEEE Int. Conf. on Intelligent Transportation Systems*, 2015, pp. 1658–1665.

[22] H. Beck, T. Eiter, and T. Krennwallner, "Inconsistency Management for Traffic Regulations: Formalization and Complexity Results," in *Logics in Artificial Intelligence*, 2012, vol. 7519, pp. 80–93.

[23] Economic Comission for Europe: Inland Transport Committee, "Vienna convention on Road Traffic," Nov. 1968. [Online]. Available: http://www.unece.org/fileadmin/DAM/trans/conventn/crt1968e.pdf

[24] M. Koschi and M. Althoff, "SPOT: A tool for set-based prediction of traffic participants," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2017.

[25] A. Rizaldi, F. Immler, and M. Althoff, "A Formally Verified Checker of the Safe Distance Traffic Rules for Autonomous Vehicles," in *NASA Formal Methods Symposium*, 2016, pp. 175–190.

[26] T. Nipkow, L. C. Paulson, and M. Wenzel, *Isabelle/HOL A Proof Assistant for Higher-Order Logic*, ser. LNCS. Springer, 2002, vol. 2283.

[27] S. M. Loos, A. Platzer, and L. Nistor, "Adaptive Cruise Control: Hybrid, Distributed, and Now Formally Verified," in *Proc. of the Int. Symposium on Formal Methods*, 2011, pp. 42–56.

[28] S. Mitsch, S. M. Loos, and A. Platzer, "Towards Formal Verification of Freeway Traffic Control," in *Proc. of the IEEE Int. Conf. on Cyber-Physical Systems*, 2012, pp. 171–180.

[29] R. W. Allen, H. T. Szostak, D. H. Klyde, T. J. Rosenthal, and K. J. Owens, "Vehicle dynamic stability and rollover," *NASA STI/Recon Technical Report N*, vol. 93, 1992.

[30] C. Ackermann, R. Isermann, S. Min, and C. Kim, "Design of a decision maker for an evasive or braking maneuver for collision avoidance," in *14. Internationales Stuttgarter Symposium: Automobil- und Motorentechnik*. Springer, 2014, pp. 401–415.

[31] Federal Highway Administration Research and Technology, "US Highway 101 Dataset," Jan. 2007. [Online]. Available: https://www.fhwa.dot.gov/publications/research/operations/07030/

[32] G. Johansson and K. Rumar, "Drivers' brake reaction times," *Human Factors*, vol. 13, no. 1, pp. 23–27, 1971.