Set-based Prediction of Traffic Participants Considering Occlusions and Traffic Rules

Markus Koschi and Matthias Althoff

Abstract—Provably safe motion planning for automated road vehicles must ensure that planned motions do not result in a collision with other traffic participants. This is a major challenge in autonomous driving, since the future behavior of other traffic participants is not known and since traffic participants are often hidden due to occlusions. In this work, we propose a formal set-based prediction that contains all acceptable future behaviors of both detected and potentially hidden traffic participants. Based on formalized traffic rules and nondeterministic motion models, we perform reachability analysis to predict the set of possible occupancies and velocities of vehicles, pedestrians, and cyclists. Real-world experiments with a test vehicle in various traffic situations demonstrate the applicability and real-time capability of our over-approximative prediction for both online verification and fail-safe trajectory planning. Even in congested, complex traffic scenarios, our forecasting approach enables self-driving vehicles to never cause accidents.
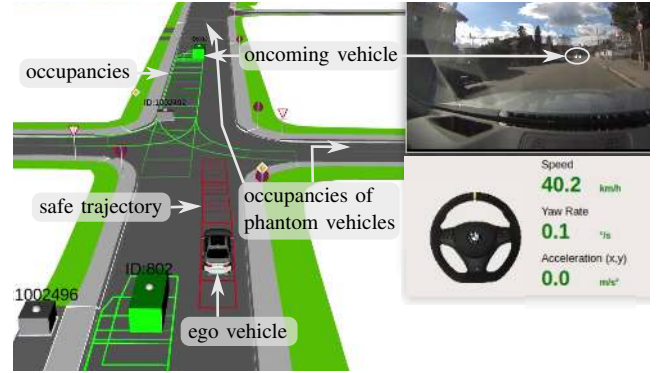

Fig. 1. Snapshot of our real-world experiments with a BMW 7 series test vehicle. The motion of the ego vehicle is provably safe if its trajectory never intersects with any predicted occupancy of detected and phantom (i. e., potentially hidden) traffic participants.

I. INTRODUCTION

BY accounting for safety in a rigorous and formal manner, we verify that autonomous vehicles do not cause any accident, which is referred to as legal safety [1]–[5]. Absolute safety is not possible, since other traffic participants can easily cause inevitable collisions, e. g., by crashing into the back of an autonomous vehicle. If every traffic participant adheres to legal safety, which most traffic participants do, no collisions will occur. Related safety concepts are passive safety [6], which requires the autonomous vehicle to be at rest when a collision occurs, and Responsibility-Sensitive Safety (RSS) [7], which determines the traffic participant responsible for a collision based on safe distances for specific driving situations.

However, if traffic participants behave differently than predicted by the autonomous vehicle, a collision for which the autonomous vehicle is responsible might be inevitable. Therefore, we propose a set-based prediction that formally encloses all acceptable future behaviors of other traffic participants. A legal specification defines which behaviors are considered to be acceptable. It explicitly represents our assumptions based on traffic rules, while the degree of conformity to traffic rules can be parameterized by the user. Some people might argue that one cannot restrict acceptable behaviors; however, these behaviors are based on applicable law, and we believe that it is better to provide guarantees under these legal assumptions than to provide no guarantees (which is the case for most probabilistic approaches).

The planned motion of the ego vehicle, i. e., the autonomous vehicle under control, is safe if its motion does not intersect

Markus Koschi and Matthias Althoff are with the Department of Informatics, Technical University of Munich, 85748 Garching, Germany (email: *markus.koschi@tum.de* and *althoff@tum.de*).

with any predicted occupancy of all detected and potentially hidden traffic participants. For example, consider a situation where the ego vehicle intends to turn left at an intersection but has to yield to oncoming traffic (cf. Fig. 1). Set-based prediction allows the ego vehicle to obtain a trajectory that is provably collision-free against all oncoming and crossing traffic. In [8], we have shown that this does not result in overly conservative behaviors for the ego vehicle. Our proposed method has several applications for autonomous vehicles and driver assistance systems:

a) Safe states: Based on the predicted occupancies, we can determine the maximum drivable area [9], the maximum Time-To-React [10], and the Point of No Return [11]. By additionally considering the predicted velocity, we can compute safe states for the ego vehicle, e. g., to maintain a safe distance to other vehicles [12]. To guarantee safety for an infinite time horizon, the planned motion of the ego vehicle must end in a state that is safe forever. Such invariably safe states can be determined using our set-based prediction [13].

b) Trajectory planning: Several trajectory planners for provably safe motions without being overly conservative use our prediction tool (SPOT [14]) [15]–[18] or assume the existence of a set-based prediction [19], [20].

c) Verification: Verification of a trajectory means that we check whether this trajectory complies with a given specification. Online verification of automated vehicles using set-based prediction is shown in [3], [8]. It can be extended to an anytime approach [21] and be embedded in any given vehicle framework [22]. For industrial robots, set-based prediction of human body parts has also been successfully used for verification [23].

A. Related work

We solely focus on motion prediction of other traffic participants [24]–[26], which is an integral part of motion planning [27]–[29] and risk assessment [24], [30]. The following related aspects are beyond the scope of this paper: extracting the information of surrounding traffic participants from sensor measurements [31]–[33], the uncertainty of these measurements [34]–[36], and implications on the prediction for connected vehicles [37], [38].

We categorize prominent early or most recent works by whether they compute *a)* a finite number of future trajectories, *b)* a probability distribution, or *c)* a bounded set of states. Since our proposed prediction considers occlusions, unlike most of the reviewed works, we subsequently present works on motion planning in the presence of occlusions[1].

a) Trajectories: Early works consider single trajectories of other traffic participants for collision avoidance [39]. To obtain a probabilistic prediction, multiple trajectory hypotheses can be weighted by probabilities obtained from Monte Carlo sampling [40]. Alternatively, intention estimation, i. e., a probabilistic classification into discrete, semantically interpretable maneuver classes, is often performed based on support vector machines [41], hidden Markov models [42], or Bayesian networks [43]–[45]; particularly for pedestrians, Gaussian process dynamical models are often used [46]. In most of these works, motion models generate a trajectory for each distinct maneuver class. In contrast, recurrent neural networks often directly predict a trajectory [47], [48]. Predicted trajectories can be compared using validation metrics [49] or similarity measures [50].

b) Probability distribution: To consider that other traffic participants have infinitely many future behaviors, we can compute a probability distribution, e. g., of kinematic variables using dynamic Bayesian networks [51]–[53]. Furthermore, neural networks have been proposed to predict most likely behaviors of vehicles on highways [54], [55], of pedestrians [56], and of cyclists [57]. For pedestrians, also linear quadratic regulator-based models are used [58]. Probability distributions can be represented as occupancy grids, which are obtained through machine learning [59]–[62] or Markov chains [63]. Overall, probability distributions can be used for motion planning [64]–[66], but they usually do not strictly bound all possible future behaviors as required for provably safe motions.

c) Bounded sets: Set-based prediction utilizes reachability analysis to compute all future behaviors of other traffic participants in accordance with the assumptions made [67]. Instead of specifying the input constraints for the reachability analysis in the assumptions, the constraints can also be estimated from Gaussian processes [68]. The work of [67] is extended in [16] by considering occlusions. Set-based prediction is also able to consider interaction between traffic participants [69] and formalized traffic rules [14], [70]. The predicted occupancy sets can also be weighted by probabilities [71], [72]

---

[1]By the term occlusion, we mean that the environment model of the ego vehicle misses information from non-observable parts outside of its field of view.

d) Occlusion: The risk from occlusions is tackled either by shrinking the field of view over the prediction horizon [73]–[76] or by introducing and predicting individual, potentially present obstacles (aka *phantom* or *virtual objects*) [1], [16], [77]–[85]. Early works considering occlusions are motion planners for mobile robots [86], [73]–[75]. Later, risk assessment systems for road vehicles have included occluded intersections [77]–[80]. In recent motion planners, a partially observable Markov decision process optimizes the behavior of the ego vehicle such that the collision risk due to occlusions is reduced [81]–[84]. In a pedestrian collision avoidance system, a partially observable Markov decision process propagates the belief states of occluded pedestrians based on reachable sets [85]. The occlusion-aware motion planner in [87] remains collision-free in specific traffic situations for which the authors have manually defined the worst-case. In contrast, the planners in [16], [88] generalize to arbitrary traffic situations, since they use a set-based prediction. In particular, [16] introduces phantom vehicles that could have right of way, and [88] extends [16] by optimizing comfort while keeping safety guarantees. Using reachability analysis, [76] guarantees passive safety for autonomous vehicles despite occlusions.

B. Contributions

This work significantly extends our previous work on set-based prediction [14], [67], [69], [70] and other previous works, especially [16], by considering 1) all safety-relevant occluded vehicles, pedestrians, and static obstacles, 2) priorities of traffic participants at intersections, 3) safe distances to the ego vehicle, 4) limited turning radii of vehicles, and 5) by validating the prediction in real-world experiments.

Overall, we present a holistic, formal prediction that enables provably safe motions for the ego vehicle. In particular, our prediction offers the following properties:

- uncertainty-aware, i. e., we consider all uncertainties from sensor measurements as well as of the future evolution of the environment;
- complete, i. e., our over-approximative prediction is guaranteed to contain any acceptable behavior;
- occlusion-aware, i. e., risks due to occlusions are considered by formally creating phantom objects;
- interaction-aware, i. e., interactions between the ego vehicle and other vehicles and between other vehicles are considered;
- considering traffic rules, i. e., restrictions due to the internationally applicable convention on road traffic [89];
- robust against traffic participants violating traffic rules, high measurement uncertainties, and incomplete environment models in the conducted experiments;
- designed for both structured and non-structured environments and not restricted to predefined behaviors;
- computes predictions for arbitrary time intervals without having to consider predictions of previous time steps; and
- real-time capable for a replanning rate of $50\,\mathrm{Hz}$.

The remainder of this paper is organized as follows. Sec. II introduces the required formalization and our problem statement. In Sec. III, we describe our legal specification and

provide an overview of the prediction algorithm. Sec. IV presents our extension for occlusions, and Sec. V details all used models for the prediction. We continue with our constraint management in Sec. VI and evaluate our prediction by numerical and real-world experiments in Sec. VII. Finally, Sec. VIII concludes this paper and proposes future work.

II. PRELIMINARIES

Throughout this paper, we will describe our method for the current planning cycle starting at t_0 when receiving an updated environment model from the ego vehicle. The initial time of the planning cycle before t_0 is denoted by t_{c-1}. The environment model $\Omega := \langle \mathcal{P}, \mathcal{N}, \mathcal{D}^{\mathcal{P}}, \mathcal{F} \rangle$ is formalized by its elements in the following subsections.

A. Notation

Vectors and matrices are written in bold and sets using a calligraphic font. For a vector $\boldsymbol{\nu} \in \mathbb{R}^n$, the operator $\mathtt{proj}_\square(\boldsymbol{\nu})$ projects $\boldsymbol{\nu}$ to its element(s) $\square$. The lower and upper limits of an interval $[\nu] \subset \mathbb{R}$ are written with overlines and underlines, respectively, i.e., $[\nu] := [\underline{\nu}, \overline{\nu}]$, and the comparison operators for intervals are defined as $[\nu] > a \Leftrightarrow \underline{\nu} > a$.

The operator $\mathtt{conv}(\mathcal{C}_1, \mathcal{C}_2)$ returns the convex hull of the sets $\mathcal{C}_1$ and $\mathcal{C}_2$, and $\mathcal{C}_1 \oplus \mathcal{C}_2$ denotes the Minkowski addition of $\mathcal{C}_1$ and $\mathcal{C}_2$. The set of the Boolean values is denoted by $\mathcal{B} := \{true, false\}$. The power set of $\mathbb{R}^n$ is denoted by $\mathtt{Pow}(\mathbb{R}^n)$. A disk, i.e., a circular area, with center $[c_x, c_y]^T$ and radius r is denoted by $\mathcal{C}\left([c_x, c_y]^T, r\right) := \left\{[x, y]^T \,|\, (x-c_x)^2 + (y-c_y)^2 \leq r^2\right\}$. The 2-dimensional rotation matrix is defined as

$$\boldsymbol{R}(\alpha) := \begin{bmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{bmatrix}. \quad (1)$$

B. Formalization of traffic participants

The state vector of a traffic participant in a Cartesian coordinate frame is $\boldsymbol{s}(t) := \begin{bmatrix} x(t), y(t), v(t), \psi(t) \end{bmatrix}^T \in \mathbb{R}^4$ and consists of the position in x-direction and y-direction $[x(t), y(t)]^T$, the scalar velocity $v(t)$, and the heading $\psi(t)$.

The set of all traffic participants is $\mathcal{P}$. Each traffic participant $p \in \mathcal{P}$ is described by the tuple $p := \langle \boldsymbol{c}^p, \mathcal{S}_0^p, \mathcal{A}^p, \mathcal{Q}^p \rangle$, where

- $\boldsymbol{c}^p \in \mathbb{C}$ is the classification consisting of the type, which is either *ego vehicle*, *pedestrian*, or *vehicle* (with subtypes *car*, *truck*, *bus*, *motorcycle*, and *bicycle*), the attribute *detected* or *phantom* (see Sec. IV), and the attribute *dynamic* or *static*. Thus, $\mathbb{C} := \{\{ego, ped, \{veh \times \{car, truck, bus, motcyc, cyc\}\}\} \times \{detected, phantom\} \times \{dyn, static\}\}$.
- $\mathcal{S}_0^p := \begin{bmatrix} [x_0], [y_0], [v_0], [\psi_0] \end{bmatrix}^T \subset \mathbb{R}^4$ is the set of uncertain initial states at t_0. Bounded measurement uncertainties can be provided by set-based observers [90], [91].
- $\mathcal{A}^p$ is the uncertain size of p. For the ego vehicle and other vehicles, we use rectangles with length $[\ell]$ and width $[w]$, and for pedestrians, we use circles with radius $[r]$. The reference point of a traffic participant is its geometric center.
- $\mathcal{Q}^p$ is the tuple of parameters for p (see Tab. I).

The superscript $\square$ in $\nu^\square$ denotes that variable ν describes traffic participant $\square \in \mathcal{P}$ or all traffic participants with classification $\square \subset \mathbb{C}$, e.g., we write ν^{veh} for all vehicles except the ego vehicle. For the sake of clarity, we write ν instead of $\nu^\square$ unless a distinction is necessary.

The operator $\mathtt{occ}(\boldsymbol{s}(t), \mathcal{A}) : \mathbb{R}^4 \times \mathbb{R}^2 \to \mathtt{Pow}(\mathbb{R}^2)$ returns the set of points in the two-dimensional Cartesian frame that are occupied by the traffic participant. For a set of states $\mathcal{S}(t)$, the occupancy operator is defined as $\mathtt{occ}(\mathcal{S}(t), \mathcal{A}) := \{\mathtt{occ}(\boldsymbol{s}(t), \mathcal{A}) \,|\, \boldsymbol{s}(t) \in \mathcal{S}(t)\}$.

To account for the limited sensor range of the ego vehicle and occlusions from other objects, we introduce the field of view:

Definition 1 (Field of view $\mathcal{F}$): The field of view $\mathcal{F} \subset \mathbb{R}^2$ is the maximum area in which all other traffic participants are guaranteed to be detected at the initial time.

C. Formalization of the road network

The road network $\mathcal{N} := \langle \mathcal{W}_{\mathrm{road}}, \mathcal{W}_{\mathrm{prio}}(t), \mathbb{D} \rangle$ describes the environment in separate layers for vehicles ($\mathcal{N}^{\mathrm{veh}}$), bicycles ($\mathcal{N}^{\mathrm{cyc}}$), and pedestrians ($\mathcal{N}^{\mathrm{ped}}$) and is formalized by its elements as follows.

Definition 2 (Allowed positions $\mathcal{W}_{\mathbf{road}}$): $\mathcal{W}_{\mathrm{road}} \subset \mathbb{R}^2$ describes all positions in the road network that the corresponding types of traffic participants may occupy.

For example, $\mathcal{W}_{\mathrm{road}}^{\mathrm{cyc}}$ can be restricted to bicycle lanes or also contain the rest of the carriageway (cf. [89, 25§1(a), 27§4]). The allowed positions $\mathcal{W}_{\mathrm{road}}^{\mathrm{ped}}$ for pedestrians consist of all sidewalks and pedestrian crossings and, if desired, other parts of the environment, e.g., parking areas or unclassified areas.

Definition 3 (Priority-based positions $\mathcal{W}_{\mathbf{prio}}$): $\mathcal{W}_{\mathrm{prio}}(t) \subset \mathcal{W}_{\mathrm{road}}$ describes the time-dependent positions that the corresponding types of traffic participants may occupy at time t without violating the priority of other traffic participants. This especially includes restrictions due to traffic lights and when turning at intersections.

In each layer[2], the road network is modeled by lanelets [93], which are atomic, interconnected, and drivable/walkable road segments:

Definition 4 (Lanelet l): A lanelet l is defined by its left and right bound, where each bound is represented by an array of points, as shown in Fig. 2a for l_1.

The bounds of a lanelet should be constructed so that the lanelet is at least as wide as the real lane; to anticipate that traffic participants slightly violate lane markings, the width of a lanelet can be enlarged by a user-defined margin. The driving direction of a lanelet is implicitly defined by its left and right bound; for pedestrian lanelets, we do not make a distinction of the driving direction. If two lanelets have a drivable/walkable connection, their relation is modeled as either longitudinally adjacent (i.e., predecessor and successor) or laterally adjacent.

---

[2]Instead of separate layers, one can also use the concept in Lanelet2 [92].

We construct a graph of the road network (for each of its layers), where a node represents a set of laterally adjacent lanelets depending on the two Boolean constraint parameters $b_{\text{lane}_1} \in \{noLat, lat\}$ and $b_{\text{lane}_2} \in \{drivDir, anyDir\}$:

- if $b_{\text{lane}_1} = noLat$, a node contains only one lanelet and no laterally adjacent lanelets (see graph in Fig. 2a);
- if $b_{\text{lane}_1} = lat \wedge b_{\text{lane}_2} = drivDir$, a node contains all laterally adjacent lanelets with the same driving direction (see graph in Fig. 2b or 2c);
- if $b_{\text{lane}_1} = lat \wedge b_{\text{lane}_2} = anyDir$, a node contains all laterally adjacent lanelets (see graph in Fig. 2d).

Two nodes are connected in the graph, if at least one lanelet in the one node is longitudinally adjacent to at least one lanelet in the other node.

Definition 5 (Driving corridor D): A driving corridor D is a union of lanelets along a path through the graph of the road network, as shown in Fig. 2.

If a lanelet or its laterally adjacent lanelets have multiple successors/predecessors, as in the case of road forks/merges, multiple driving corridors are created, e.g., l_2 is included in D_2 describing a right turn (see Fig. 2b) and also in D_3 describing a left turn (see Fig. 2c). Furthermore, each driving corridor provides a speed limit $v_{\text{speedLim}} > 0$, and the operator $\text{occ}(D) : D \to \text{Pow}(\mathbb{R}^2)$ returns the occupancy of D.

Definition 6 (All driving corridors $\mathbb{D}$): The set of all driving corridors $\mathbb{D}(b_{\text{lane}_1}, b_{\text{lane}_2})$ is obtained by performing breadth-first graph search on the graph of the road network constructed for the given values of b_{lane_1} and b_{lane_2}. The initial nodes are all nodes that contain only lanelets with no predecessor, and the goal nodes are all nodes that contain only lanelets with no successor.

Definition 7 (Corridors of a traffic participant $\mathcal{D}^p$): The set of driving corridors of traffic participant p is denoted by $\mathcal{D}^p(b_{\text{lane}_1}, b_{\text{lane}_2}) \subset \mathbb{D}(b_{\text{lane}_1}, b_{\text{lane}_2})$ and is provided by the environment model.

For example, the set of driving corridors of the vehicle in Fig. 2 can be $\mathcal{D}^p(noLat, drivDir) = \{D_1\}$ or $\mathcal{D}^p(lat, drivDir) = \{D_2, D_3\}$. When using the parameters $b^p_{\text{lane}_1}, b^p_{\text{lane}_2}$ of a traffic participant p, we only write $\mathcal{D}^p$ for brevity. Furthermore, let the forward driving corridor $\vec{\mathcal{D}}$ be the part of $\mathcal{D}$ that is not behind $\text{occ}(\mathcal{S}_0, \mathcal{A})$ with respect to the driving direction (cf. $\vec{\mathcal{D}}^{\text{ego}}_{\text{reach}}$ in Fig. 3 later).

D. Reachable set of traffic participants

Let us define the prerequisites for the reachability analysis based on [67, Sec. IV].

Definition 8 (Model M): A model M is defined as the tuple $M := \langle \boldsymbol{f}_M, \mathcal{S}_M, \mathcal{U}_M \rangle$, where $\boldsymbol{f}_M$ is the right-hand side of the differential equation describing the motion of a traffic participant by

$$\dot{\boldsymbol{s}}(t) = \boldsymbol{f}_M\big(\boldsymbol{s}(t), \boldsymbol{u}(t)\big), \tag{2}$$

and $\mathcal{S}_M(t) \subseteq \mathbb{R}^n$ and $\mathcal{U}_M(t) \subseteq \mathbb{R}^m$ denote the admissible sets bounding the states $\boldsymbol{s}(t)$ and inputs $\boldsymbol{u}(t)$ of the traffic participant, respectively.

(a) D_1 using $b_{\text{lane}_1} = noLat$.

(b) D_2 using $b_{\text{lane}_1} = lat$ and $b_{\text{lane}_2} = drivDir$.

(c) D_3 using $b_{\text{lane}_1} = lat$ and $b_{\text{lane}_2} = drivDir$.

(d) D_4 using $b_{\text{lane}_1} = lat$ and $b_{\text{lane}_2} = anyDir$.
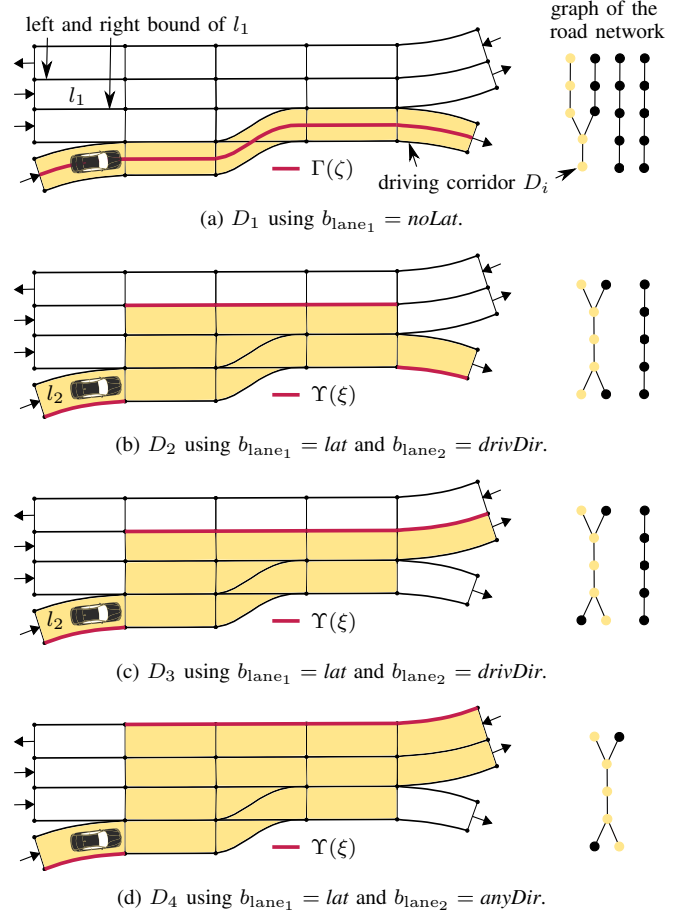
Fig. 2. The road network $\mathcal{N}$ (here, we only show the layer for vehicles) is modeled by lanelets l (see left part). (a)–(d) Given the values for b_{lane_1} and b_{lane_2}, we construct the graph of the road network (see right part) and show a possible driving corridor D_i (yellow in both left and right part).

When starting at a state $\boldsymbol{s}(t_0) \in \mathcal{S}_0$ and using an input trajectory $\boldsymbol{u}(\cdot)$, a possible solution of (2) at time $t \geq t_0$ is denoted by $\boldsymbol{\chi}\big(t; \boldsymbol{s}(t_0), \boldsymbol{u}(\cdot)\big)$.

Definition 9 (Reachable set $\mathcal{R}$): The reachable set $\mathcal{R}$ of model M is the set of states that are reachable at time $t \geq t_0$ from the initial set $\mathcal{S}_0$ when applying all admissible inputs $\mathcal{U}_M(t)$ while staying within $\mathcal{S}_M(t)$:

$$\mathcal{R}(t; M, t_0) := \bigg\{ \boldsymbol{\chi}\big(t, \boldsymbol{s}(t_0), \boldsymbol{u}(\cdot)\big) \,\bigg|\, \boldsymbol{s}(t_0) \in \mathcal{S}_0, \forall t^\star \in [t_0, t] :$$
$$\boldsymbol{\chi}\big(t^\star; \boldsymbol{s}(t_0), \boldsymbol{u}(\cdot)\big) \in \mathcal{S}_M(t^\star), \boldsymbol{u}(t^\star) \in \mathcal{U}_M(t^\star) \bigg\}.$$

To over-approximate the reachable set of a model, we introduce abstractions:

Definition 10 (Abstraction): Model M_2 is an abstraction of model M_1, if $\forall t \geq t_0 : \mathcal{R}(t; M_1, t_0) \subseteq \mathcal{R}(t; M_2, t_0)$.

To efficiently minimize the over-approximation caused by an abstraction, we use several abstractions:

Lemma 1 (Combining abstractions): If M_i, $i = 2, \ldots, m$, are abstractions of model M_1, the intersection of their reach-

able sets remains an over-approximation of the reachable set of the original model M_1:

$$\forall t \geq t_0 : \mathcal{R}(t; M_1, t_0) \subseteq \bigcap_{i=2}^{m} \mathcal{R}(t; M_i, t_0). \qquad \square$$

Proof: The over-approximation directly follows from [3, Prop. V.1]. ■

If considering the reachable set only at distinct points in time, we cannot provide any safety guarantees for the ego vehicle between these points in time. Thus, we need to compute the reachable set for a time interval $[t] := [\underline{t}, \overline{t}] \geq t_0 : \mathcal{R}([t]; M, t_0) := \bigcup_{t \in [t]} \mathcal{R}(t; M, t_0)$.

E. Problem statement

Let M_{real} be the model that exactly describes the motions of a traffic participant that can be performed in the real world and comply with all applicable traffic rules. Our goal is to predict the future reachable set of a model M_{pred} that is an abstraction of M_{real}, i.e., $\mathcal{R}(t; M_{\mathrm{real}}, t_0) \subseteq \mathcal{R}(t; M_{\mathrm{pred}}, t_0)$ for any $t \in [t]$, with as little over-approximation as possible.

III. SPECIFICATION AND OVERALL ALGORITHM

Instead of trying to explicitly describe all acceptable behaviors in abstraction M_{pred}, we define constraints in our specification that lead to an over-approximation of acceptable behaviors. Our specification is chosen such that the prediction conforms to legal safety based on traffic rules. Thus, it is in line with RSS [7] and rulebooks [94], which both specify acceptable behaviors for the ego vehicle, while we, from the prediction perspective, focus on the acceptable behaviors of other traffic participants. Note that our approach has the benefit that even if we do not model all traffic rules, our prediction remains over-approximative.

Our parameterizable specification consists of independent constraints C that are listed in Tab. I. Each constraint is defined by its parameters, textual description, formalization, and source. The Boolean parameters b allow us to enable or disable constraints individually, and the parameters Δ allow us to tune our reaction to violations of constraints (see Sec. VI later). The longitudinal direction is described with respect to the driving direction. In summary, our specification either constrains the dynamics of other traffic participants (see upper part of Tab. I) or constrains the allowed regions in the environment (see lower part of Tab. I).

Alg. 1 provides an overview of our prediction running in every planning cycle. At the current initial time t_0, we receive as input an updated environment model $\Omega_0 = \langle \mathcal{P}, \mathcal{N}, \mathcal{D}^{\mathcal{P}}, \mathcal{F} \rangle$ of the ego vehicle. If available, the environment model from the previous planning cycle can also be provided (cf. optional input of Alg. 1). The parameters $\mathcal{Q}$ (cf. Tab. I) are initialized as desired by the user (cf. Tab. IV later).

First, we create phantom traffic participants that capture the risks from potentially undetected traffic participants (line 1 of Alg. 1; cf. Sec. IV). For each traffic participant (except the ego vehicle), we validate its constraint parameters $\mathcal{Q}^p$ (line 3; cf. Sec. VI) and choose all valid abstractions $M_{\diamond}^p$ (line 4; cf.

Algorithm 1 SET-BASEDPREDICTION

Input: environment model $\Omega_0 = \langle \mathcal{P}, \mathcal{N}, \mathcal{D}^{\mathcal{P}}, \mathcal{F} \rangle$ at t_0 (containing $p = \langle \boldsymbol{c}^p, \mathcal{S}_0^p, \mathcal{A}^p, \mathcal{Q}^p \rangle$ for each $p \in \mathcal{P}$), default parameters $\mathcal{Q}$, and set τ of arbitrary time intervals $[t] \geq t_0$
Optional input: environment model Ω_{c-1} from previous cycle
Output: over-approximative reachable set $\mathcal{R}^p$ for each $p \in \mathcal{P}$

1: $\mathcal{P}.\mathrm{ADDPHANTOMS}(\mathcal{N}, \mathcal{F}, \mathcal{Q})$ ▷ consider occlusions
2: **for all** $p \in \mathcal{P}$ **do**
3:    $\mathcal{Q}^p \leftarrow \mathrm{VALIDATECONSTRAINTS}(\Omega_0, \Omega_{c-1})$
4:    $\mathcal{Q}^p \leftarrow \mathrm{SELECTVALIDABSTRACTIONS}(\boldsymbol{c}^p, \mathcal{Q}^p)$
5:    $\mathcal{R}^p(\cdot; M_{\mathrm{pred}}^p, t_0) \leftarrow \mathbb{R}^4$ ▷ initialize
6:    **for all** $M_{\diamond}^p \in \mathcal{Q}^p$ **do**
7:      **for all** $[t] \in \tau$ **do**
8:        $\mathcal{R}^p([t]; M_{\diamond}^p, t_0) \leftarrow \mathrm{REACH}([t], M_{\diamond}^p, p, \mathcal{N}, \mathcal{D}^p, \mathcal{Q}^p)$
9:        $\mathcal{R}^p([t]; M_{\mathrm{pred}}^p, t_0) \leftarrow \mathcal{R}^p([t]; M_{\mathrm{pred}}^p, t_0) \cap \mathcal{R}^p([t]; M_{\diamond}^p, t_0)$
10:      **end for**
11:    **end for**
12: **end for**
13: $\mathrm{INTERACTION}(\mathcal{R}^p(\cdot)$ for all $p \in \mathcal{P}, \mathcal{N})$ ▷ optional
14: **return** $\mathcal{R}^p([t]; M_{\mathrm{pred}}^p, t_0)$ for all $p \in \mathcal{P}$ and $[t] \in \tau$

Tab. II). Next, for each given time interval $[t]$, we compute the reachable set of each valid abstraction (line 8; cf. Sec. V) and intersect them to obtain a tight over-approximative reachable set (line 9; cf. Sec. V-F).

The time complexity of our algorithm is linear in the number of traffic participants and the number of time intervals. Our algorithm can be parallelized for each traffic participant and each abstraction. Line 13 of Alg. 1 optionally considers the interaction between vehicles as described in [69], e.g., that a vehicle cannot tunnel through a stationary vehicle.

IV. OCCLUSION

To consider traffic participants that are hidden due to occlusions and therefore cannot be predicted directly, we create all phantom traffic participants $p = \langle \boldsymbol{c}, \mathcal{S}_0, \mathcal{A}, \mathcal{Q} \rangle$ that could be relevant for the motion of the ego vehicle, as summarized in Alg. 2, visualized in Fig. 3, and described subsequently.

Def. 1 implies that no traffic participant can suddenly appear within the field of view, but may enter the field of view at any time $t > t_0$. Thus, we intersect the boundary of the field of view with all driving corridors $\mathbb{D}(lat, drivDir)$ of each layer and split the boundary at each intersection point into border segments (or edges) e (lines 1–3 of Alg. 2; cf. Fig. 3). The resulting set $\mathcal{E} := \{e_1, \ldots, e_i\}$ contains all border segments e of the field of view through which phantom traffic participants can emerge. To consider additional sources of traffic participants, e.g., doors where pedestrians can appear, each source can be modeled as an additional driving corridor.

Border segment e is relevant for the motion of the ego vehicle, if the ego vehicle can be influenced by a phantom traffic participant that is positioned at e and performs any acceptable behavior in accordance with our legal specification. Therefore, we require all forward driving corridors of the ego vehicle $\vec{\mathcal{D}}_{\mathrm{reach}}^{\mathrm{ego}} := \vec{\mathcal{D}}^{\mathrm{ego}}(b_{\mathrm{lane}_1}^{\mathrm{ego}}, b_{\mathrm{lane}_2}^{\mathrm{ego}})$, as shown in Fig. 3. When using $b_{\mathrm{lane}_1}^{\mathrm{ego}} = lat$ and $b_{\mathrm{lane}_2}^{\mathrm{ego}} = anyDir$, we will create phantom traffic participants considering all possible behaviors of the ego vehicle. In case we know that the ego vehicle will

TABLE I
LEGAL SPECIFICATION CONSTRAINING THE ACCEPTABLE BEHAVIORS OF OTHER TRAFFIC PARTICIPANTS.

Constraint	Parameters	Description and formalization (based on state variables $\forall t \geq t_0$)	Source
$C_{a_{\max}}$	$a_{\max} > 0, \Delta_{a_{\max}} \geq 0$	Absolute acceleration, i.e., accelerating and braking, does not exceed $a_{\max}$: $|\dot{v}(t)| \leq a_{\max}$.	physical law (friction circle)
$C_{v_{\max}}$	$v_{\max} > 0, \Delta_{v_{\max}} \geq 0$	Absolute velocity does not exceed $v_{\max}$: $|v(t)| \leq v_{\max}$.	physical law and ISO 13855
C_{speedLim}	$f_{\text{speed}} \geq 1, \Delta_{f_{\text{speed}}} \geq 0$	For vehicles, longitudinal velocity does not exceed the official speed limit v_{speedLim} multiplied by a speeding factor f_{speed}: $|v_\xi(t)| \leq v_{\text{speedLim}} \cdot f_{\text{speed}}$.	[89, 13§1–2]
C_{engine}	$v_S > 0$	For vehicles, above the switching velocity v_S, longitudinal acceleration is decreasing inversely proportional to longitudinal velocity due to limited engine power: $|v_\xi(t)| < v_S \vee |\dot{v}_\xi(t)| \leq a_{\max} \cdot \frac{v_S}{|v_\xi(t)|}$.	physical law
C_{reverse}	$b_{\text{reverse}} \in \mathcal{B}, \Delta_{v_{\text{reverse}}} \leq 0$	For vehicles, it is forbidden to reverse, i.e., to drive backwards in longitudinal direction: $v_\xi(t) \geq 0$.	[89, 14§2]
$C_{v_{\min}}$	$v_{\min} \in \mathbb{R}, \Delta_{v_{\min}} \geq 0$	For vehicles, longitudinal velocity does not fall below $v_{\min}$: $v_\xi(t) \geq v_{\min}$.	[89, 13§4, 23§1]
C_{turn}	$0 \leq \delta_{\max} \leq \pi/2, \ell_{\text{wb}} > 0,$ $\underline{\ell}_{\text{ovr}} \geq 0, \overline{\ell}_{\text{ovr}} \geq \underline{\ell}_{\text{ovr}}$	For vehicles, the steering angle does not exceed $\delta_{\max}$, and turning within lanes is forbidden: $\text{occ}(s(t), \mathcal{A}) \cap \mathcal{O}_{\text{turn}}(t_{c-1}) = \emptyset$.	physical law and [89, 14§2]
C_{road}	$b_{\text{road}} \in \mathcal{B}$	It is forbidden to leave $\mathcal{W}_{\text{road}}$, which are the allowed positions for this type of traffic participant (cf. Def. 2): $\text{occ}(s(t), \mathcal{A}) \subseteq \mathcal{W}_{\text{road}}$.	[89, 1§(d)–(j)]
C_{prio}	$b_{\text{prio}} \in \mathcal{B}$	It is forbidden to occupy parts of the road network that intersect with other lanes (including forks and merging lanes) for which other traffic participants currently have priority: $\text{occ}(s(t), \mathcal{A}) \subseteq \mathcal{O}_{\text{prio}}(t; t_0)$.	[89, 18§1–7, 20§6(b), 21§2]
C_{lane}	$b_{\text{lane}_1} \in \{noLat, lat\},$ $b_{\text{lane}_2} \in \{drivDir, anyDir\}$	For vehicles, changing lanes is restricted: $\vec{\mathcal{D}}(t) \subseteq \vec{\mathcal{D}}(t_{c-1})$ using the same $\mathcal{N}$; if $b_{\text{lane}_1} = noLat$: It is forbidden to change to any other lane. if $b_{\text{lane}_2} = drivDir$: It is forbidden to change to a lane that is not appropriate with respect to the direction of traffic.	[89, 10§4–5, 11§1–11]
C_{safe}	$T^{\text{ego}} \geq 0, a^{\text{ego}}_{\text{comfort}} \geq 0$	For vehicles, a safe distance (measured along the centerline of the lanes) to the ego vehicle must be kept when driving behind the ego vehicle or merging in front of it.	[89, 13§5, 11§2(d)]

not overtake in a lane not appropriate to the direction of traffic, we can use $b^{\text{ego}}_{\text{lane}_2} = drivDir$, and if we know that the ego vehicle will not change to any laterally adjacent lane, we can
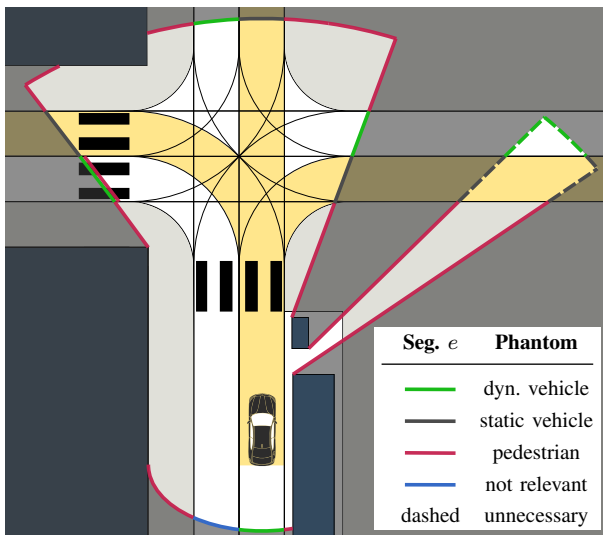

Fig. 3. When intersecting the field of view (bright area) of the ego vehicle with all driving corridors of each layer of the road network, we obtain border segments e. At each e, we introduce phantom traffic participants (see legend) if they could be relevant for the motion of the ego vehicle, which is determined using the forward driving corridors of the ego vehicle $\vec{\mathcal{D}}^{\text{ego}}_{\text{reach}} = \vec{\mathcal{D}}^{\text{ego}}(lat, drivDir)$ (yellow area) and extends [16, Fig. 2].

use $b^{\text{ego}}_{\text{lane}_1} = noLat$; this minimizes the set $\vec{\mathcal{D}}^{\text{ego}}_{\text{reach}}$ to reduce computation costs.

Let us denote the forward driving corridors when starting at e by $\vec{\mathcal{D}}(e) \subset \mathbb{D}(lat, drivDir)$. By comparing $\vec{\mathcal{D}}^{\text{ego}}_{\text{reach}}$ with $\vec{\mathcal{D}}(e)$ as described in lines 5–17 of Alg. 2, we determine whether e is relevant and what classification c for a phantom traffic participant at e is required (cf. Fig. 3). An example for a border segment that is not relevant for the motion of the ego vehicle is the blue segment in Fig. 3.

Next, in lines 18–28 of Alg. 2, we set the initial positions as the border segment e (which spans across all laterally adjacent lanelets with the same driving direction), the initial velocities as all admissible velocities in the driving corridor of e, the initial heading aligned with the driving direction, and the size to the values given in Tab. IV so that $e \subset \text{occ}(\mathcal{S}_0, \mathcal{A})$. As a result, the phantom traffic participant is modeled as an abstraction of any possibly appearing traffic participant. Finally, we add the phantom traffic participant to $\mathcal{P}$ (line 29 of Alg. 2); thus, it will be predicted analogously to the detected traffic participants (cf. Alg. 1).

We might have added multiple phantom vehicles in the same driving corridor, as shown in the right part of Fig. 3 (dashed segments). If the forward driving corridor of a dynamic phantom vehicle is completely enclosed by the forward driving corridor of another dynamic phantom vehicle, we can remove the latter phantom vehicle, since it is further away from the ego vehicle and its threat is already considered by the other, former phantom vehicle (line 31 and 40 of Alg. 2).

Algorithm 2 ADDPHANTOMS()

Input: road network $\mathcal{N}$, field of view $\mathcal{F}$, default parameters $\mathcal{Q}$
Output: set of phantom traffic participants $\mathcal{P}$

1: $\mathcal{E}^{\mathrm{veh}} \leftarrow \mathcal{F} \cap \mathbb{D}^{\mathrm{veh}}(lat, drivDir)$
2: $\mathcal{E}^{\mathrm{cyc}} \leftarrow \mathcal{F} \cap \mathbb{D}^{\mathrm{cyc}}(lat, drivDir)$
3: $\mathcal{E}^{\mathrm{ped}} \leftarrow \mathcal{F} \cap \mathbb{D}^{\mathrm{ped}}(lat, drivDir)$
4: **for all** $e \in \{\mathcal{E}^{\mathrm{veh}} \cup \mathcal{E}^{\mathrm{cyc}} \cup \mathcal{E}^{\mathrm{ped}}\}$ **do**
5:   **if** $e \in \mathcal{E}^{\mathrm{veh}}$ **and** $\vec{\mathcal{D}}(e) \subseteq \vec{\mathcal{D}}^{\mathrm{ego}}_{\mathrm{reach}}$ **then**
6:     $c \leftarrow \{\mathrm{veh, phantom, static}\}$ ▷ vehicle ahead
7:   **else if** $e \in \mathcal{E}^{\mathrm{veh}}$ **and** $\vec{\mathcal{D}}^{\mathrm{ego}}_{\mathrm{reach}} \subseteq \vec{\mathcal{D}}(e)$ **then**
8:     $c \leftarrow \{\mathrm{veh, phantom, dyn}\}$ ▷ vehicle behind
9:   **else if** $e \in \mathcal{E}^{\mathrm{veh}}$ **and** $\mathrm{occ}(\vec{\mathcal{D}}^{\mathrm{ego}}_{\mathrm{reach}}) \cap \mathrm{occ}(\vec{\mathcal{D}}(e)) \neq \emptyset$ **then**
10:     $c \leftarrow \{\mathrm{veh, phantom, dyn}\}$ ▷ crossing vehicle
11:   **else if** $e \in \mathcal{E}^{\mathrm{cyc}}$ **and** $\mathrm{occ}(\vec{\mathcal{D}}^{\mathrm{ego}}_{\mathrm{reach}}) \cap \mathrm{occ}(\vec{\mathcal{D}}(e)) \neq \emptyset$ **then**
12:     $c \leftarrow \{\mathrm{cyc, phantom, dyn}\}$ ▷ crossing cyclist
13:   **else if** $e \in \mathcal{E}^{\mathrm{ped}}$ **then**
14:     $c \leftarrow \{\mathrm{ped, phantom, dyn}\}$ ▷ pedestrian
15:   **else**
16:     **continue** ▷ not relevant, as no interaction with ego vehicle
17:   **end if**
18:   **if** $\mathrm{ped} \in c$ **then**   ▷ initial state for pedestrian
19:     $[v_0] \leftarrow [0, v^{\mathrm{ped}}_{\max}]$ ▷ from $\mathcal{Q}$
20:     $[\psi_0] \leftarrow [-\pi, \pi]$
21:     $\mathcal{A} \leftarrow$ CREATECIRCLE($\mathcal{Q}$)
22:   **else**   ▷ initial state for vehicle (incl. cyclist)
23:     $[v_0] \leftarrow [0, v_{\max, \xi}]$ ▷ from $\mathcal{Q}$ and (5)
24:     $\psi_0 \leftarrow$ GETDRIVINGDIRECTION($\vec{\mathcal{D}}(e)$)
25:     $\mathcal{A} \leftarrow$ CREATERECTANGLE($\mathcal{Q}$)
26:   **end if**
27:   $[[x_0], [y_0]]^T \leftarrow$ CREATEBOUNDINGBOX(e)
28:   $\mathcal{D} \leftarrow \mathcal{D}(e)$
29:   $\mathcal{P}$.ADD($\langle c, [[x_0], [y_0], [v_0], [\psi_0]]^T, \mathcal{A}, \mathcal{Q} \rangle$)
30: **end for**
31: $\mathcal{P} \leftarrow$ REMOVEUNNECESSARYPHANTOMS($\mathcal{P}, \mathcal{N}$)   ▷ optional
32: **return** $\mathcal{P}$

33: **function** REMOVEUNNECESSARYPHANTOMS($\mathcal{P}, \mathcal{N}$)
34:   **for all** $i, j \in \mathcal{P}$ **do**
35:     **if** $i = j$ **or** $\mathrm{veh} \notin c^i$ **or** $\mathrm{phantom} \notin c^i$ **or** $c^i \neq c^j$ **then**
36:       **break**
37:     **else if** $\mathrm{static} \in c^i$ **and** $\vec{\mathcal{D}}^i \subseteq \vec{\mathcal{D}}^j$ **then**
38:       $\mathcal{P}$.REMOVE(i)   ▷ j is behind i and the ego vehicle is behind both
39:     **else if** $\mathrm{dyn} \in c^i$ **and** $\vec{\mathcal{D}}^i \subseteq \vec{\mathcal{D}}^j$ **then**
40:       $\mathcal{P}$.REMOVE(j)   ▷ i is in front of j and either both are behind the ego vehicle or both are approaching the ego vehicle
41:     **end if**
42:   **end for**
43:   **return** $\mathcal{P}$
44: **end function**

TABLE II
OVERVIEW OF THE ABSTRACTIONS.

Abstraction	Covers constraints	Requires	See
M_{acc}	$C_{a_{\max}}$	n/a	Sec. V-A
M_{vel}	$C_{v_{\max}}$	n/a	Sec. V-A
M_{long}	C_{speedLim}, C_{engine}, C_{reverse}, $C_{v_{\min}}$, C_{road}, C_{lane} (and both $C_{a_{\max}}$ and $C_{v_{\max}}$ only in longitudinal direction)	b_{road}	Sec. V-B
M_{turn}	C_{turn}	$b_{\mathrm{road}} \wedge b_{\mathrm{reverse}}$	Sec. V-D
M_{prio}	C_{prio}	$b_{\mathrm{road}} \wedge b_{\mathrm{prio}}$	Sec. V-E
M_{safe}	C_{safe}	$b_{\mathrm{road}} \wedge b_{\mathrm{reverse}}$	Sec. V-C

A. Abstractions based on point-mass model (M_{acc} and M_{vel})

To describe a point-mass model, let us rewrite the state vector as $\boldsymbol{s}(t) = [x(t), y(t), v_x(t), v_y(t)]^T \in \mathbb{R}^4$ with $v_x(t) = v(t) \cdot \cos(\psi(t))$ and $v_y(t) = v(t) \cdot \sin(\psi(t))$. Analogously, the set of initial states is $\mathcal{S}_0 = [[x_0], [y_0], [v_{x_0}], [v_{y_0}]]^T \subset \mathbb{R}^4$. The input for the abstractions based on a point-mass model consists of the acceleration in x-direction and y-direction, i.e., $\boldsymbol{u}(t) = [u_x(t), u_y(t)]^T \in \mathbb{R}^2$.

Definition 11 (Acceleration-bounded abstraction M_{acc}):
Abstraction $M_{\mathrm{acc}} := \langle \boldsymbol{f}_{M_{\mathrm{acc}}}, \mathcal{S}_{M_{\mathrm{acc}}}, \mathcal{U}_{M_{\mathrm{acc}}} \rangle$ is an acceleration-bounded point-mass model ($C_{a_{\max}}$), where

$$\dot{x}(t) = v_x(t), \dot{y}(t) = v_y(t), \dot{v}_x(t) = u_x(t), \dot{v}_y(t) = u_y(t),$$
$$\mathcal{S}_{M_{\mathrm{acc}}} := \mathbb{R}^4,$$
$$\mathcal{U}_{M_{\mathrm{acc}}} := \left\{ [u_x(t), u_y(t)]^T \mid \sqrt{u_x(t)^2 + u_y(t)^2} \leq a_{\max} \right\}.$$

Proposition 1 (Reachable set of M_{acc}): The reachable set of M_{acc} for a time interval $[t] \geq t_0$ is

$$\mathcal{R}([t]; M_{\mathrm{acc}}, t_0) = \mathrm{conv}\big(\boldsymbol{T}_{\mathrm{hom}}(\underline{t}) \cdot \mathcal{S}_0, \boldsymbol{T}_{\mathrm{hom}}(\overline{t}) \cdot \mathcal{S}_0\big) \oplus \boldsymbol{T}_{\mathrm{inp}}(\overline{t}) \cdot \mathcal{U}_{M_{\mathrm{acc}}},$$

as shown in the blue part of Fig. 4 and where

$$\boldsymbol{T}_{\mathrm{hom}}(t) = \begin{bmatrix} 1 & 0 & t - t_0 & 0 \\ 0 & 1 & 0 & t - t_0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$\boldsymbol{T}_{\mathrm{inp}}(t) = \begin{bmatrix} 1/2 \cdot (t - t_0)^2 & 0 \\ 0 & 1/2 \cdot (t - t_0)^2 \\ t - t_0 & 0 \\ 0 & t - t_0 \end{bmatrix}. \qquad \square$$

Proof: The reachable set directly follows from [70, Prop. 2]. ∎

To compute the occupancy of $\mathcal{R}([t]; M_{\mathrm{acc}}, t_0)$ for vehicles, we require the heading. However, due to the state representation of the point-mass model, the reachable set does not contain a bound for the heading. In our previous work [67], we have assumed that the heading is constant over the prediction horizon. In this work, we do not make this assumption. We can bound the heading until the earliest point in time $t_{v=0}$ at

---

V. ABSTRACTIONS

We minimize the over-approximation of our prediction by using several abstractions (cf. Lemma 1). Tab. II provides an overview of the proposed abstractions and their covered constraints so that all constraints of Tab. I are considered. Some abstractions require that other constraints have not been violated, i.e., the Boolean parameters given in Tab. II must be *true*; otherwise, this abstraction cannot be computed and gets disabled, e.g., M_{long} is omitted if $b_{\mathrm{road}} = \textit{false}$. In the following subsections, we define these abstractions and present how to compute their reachable set and occupancy.
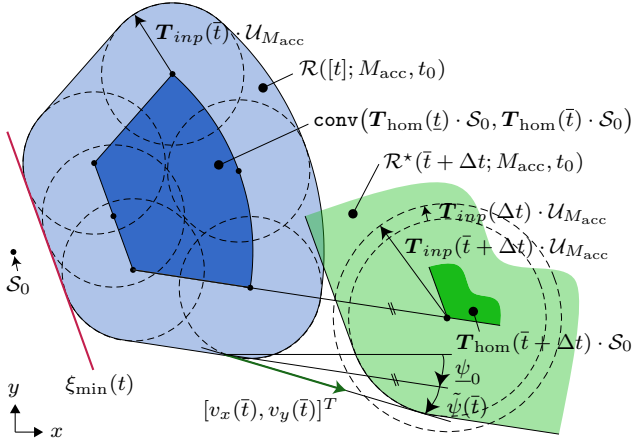
Fig. 4. Blue part (upper left): The reachable set $\mathcal{R}([t]; M_{\mathrm{acc}}, t_0)$ is bounded by the Minkowski addition of the homogeneous solution $\boldsymbol{T}_{\mathrm{hom}}([t]) \cdot \mathcal{S}_0$ with the input solution $\boldsymbol{T}_{\mathrm{inp}}(\bar{t}) \cdot \mathcal{U}_{M_{\mathrm{acc}}}$ (cf. Prop. 1 and [70, Fig. 3]). Green part (lower right): A bound on the heading $\psi([t])$ for M_{acc} is obtained from the velocity vector $[v_x(\bar{t}), v_y(\bar{t})]^T$ that has to point within $\mathcal{R}^\star(\bar{t}+\Delta t; M_{\mathrm{acc}}, t_0)$ (cf. Lemma 2). Red line (left): To prevent reversing, we restrict the minimum positions in M_{long} to $\xi_{\mathrm{min}}(t)$ based on $\mathcal{R}(t_{v=0}; M_{\mathrm{acc}}, t_0)$ (cf. (8)). Note that all sets are projected onto the position domain.

which the vehicle can come to a standstill when fully braking:

$$t_{v=0} := \begin{cases} \frac{\underline{v}_0}{a_{\mathrm{max}}} + t_0 & \text{if } \underline{v}_0 \geq 0 \\ -\infty & \text{otherwise.} \end{cases} \tag{3}$$

Lemma 2 (Bounds for ψ of M_{acc}): Due to the limited acceleration in M_{acc}, the heading of a vehicle for $[t] \geq t_0$ is

$$\psi([t]) \in \begin{cases} \left[\underline{\psi}_0 - \tilde{\psi}(\bar{t}), \overline{\psi}_0 + \tilde{\psi}(\bar{t})\right] & \text{if } \bar{t} < t_{v=0} \\ \mathbb{R} & \text{otherwise,} \end{cases}$$

with $\tilde{\psi}(\bar{t}) := \sin^{-1}\left(\frac{a_{\mathrm{max}}}{\underline{v}_0} \cdot (\bar{t} - t_0)\right)$. $\qquad\square$

Proof: Let $\Delta t > 0$, $\bar{t} \geq t_0$, and $\bar{t} + \Delta t < t_{v=0}$. A velocity vector $[v_x(\bar{t}), v_y(\bar{t})]^T$ at $\bar{t}$ in $\mathcal{R}(\bar{t}; M_{\mathrm{acc}}, t_0)$ has to point to a position in $\mathcal{R}^\star(\bar{t} + \Delta t; M_{\mathrm{acc}}, t_0) := \boldsymbol{T}_{\mathrm{hom}}(\bar{t}+\Delta t) \cdot \mathcal{S}_0 \oplus \left(\boldsymbol{T}_{\mathrm{inp}}(\bar{t}+\Delta t) \cdot \mathcal{U}_{M_{\mathrm{acc}}} - \boldsymbol{T}_{\mathrm{inp}}(\Delta t) \cdot \mathcal{U}_{M_{\mathrm{acc}}}\right)$, since we can accelerate by $\mathcal{U}_{M_{\mathrm{acc}}}$ during Δt but must satisfy Prop. 1 at $\bar{t} + \Delta t$ (see Fig. 4). The maximum angle of this velocity vector can be described by the tangent against $\mathrm{proj}_{x,y}\left(\mathcal{R}(\bar{t}; M_{\mathrm{acc}}, t_0)\right)$ and $\mathrm{proj}_{x,y}\left(\mathcal{R}^\star(\bar{t}+\Delta t; M_{\mathrm{acc}}, t_0)\right)$. The angle of a tangent on two circles is the inverse of the sine function of the difference of their radii divided by the distance of their center points [95]; for our case (see Fig. 4), $\tilde{\psi}(\bar{t}) = \sin^{-1}\left(\frac{\mathrm{proj}_{x,y}\left((\boldsymbol{T}_{\mathrm{inp}}(\bar{t}+\Delta t) - \boldsymbol{T}_{\mathrm{inp}}(\Delta t)) \cdot \mathcal{U}_{M_{\mathrm{acc}}} - \boldsymbol{T}_{\mathrm{inp}}(\bar{t}) \cdot \mathcal{U}_{M_{\mathrm{acc}}}\right)}{\left\|\mathrm{proj}_{x,y}\left(\boldsymbol{T}_{\mathrm{hom}}(\bar{t}+\Delta t) \cdot \mathcal{S}_0 - \boldsymbol{T}_{\mathrm{hom}}(\bar{t}) \cdot \mathcal{S}_0\right)\right\|_2}\right)$. Using $t^\star := \bar{t} - t_0$ and a $v_0 \in [\underline{v}_0]$, this evaluates to $\tilde{\psi}(\bar{t}) = \sin^{-1}\left(\frac{1/2 \cdot ((t^\star+\Delta t)^2 - \Delta t^2) \cdot a_{\mathrm{max}} - 1/2 \cdot t^\star \cdot a_{\mathrm{max}}}{v_0 \cdot (t^\star + \Delta t) - v_0 \cdot t^\star}\right)$. After simplifying the term and by selecting the $v_0 \in [\underline{v}_0]$ that maximizes $\tilde{\psi}(\bar{t})$, we obtain $\tilde{\psi}(\bar{t}) = \sin^{-1}\left(\frac{a_{\mathrm{max}}}{\underline{v}_0} \cdot (\bar{t} - t_0)\right)$. Since the inverse of the sine function is monotonic, $\forall t \in [\underline{t}, \bar{t}] : \tilde{\psi}(t) \leq \tilde{\psi}(\bar{t})$. Finally, we add the initial heading $[\psi_0]$ and obtain the bound on $\psi([t])$. $\qquad\blacksquare$

Definition 12 (Velocity-bounded abstraction M_{vel}): Abstraction $M_{\mathrm{vel}} := \langle \boldsymbol{f}_{M_{\mathrm{acc}}}, \mathcal{S}_{M_{\mathrm{vel}}}, \mathcal{U}_{M_{\mathrm{vel}}} \rangle$ is a velocity-bounded point-mass model ($C_{v_{\mathrm{max}}}$), where

$$\mathcal{S}_{M_{\mathrm{vel}}} := \left\{[x(t), y(t), v_x(t), v_y(t)]^T \mid \right.$$
$$\left. \sqrt{v_x(t)^2 + v_y(t)^2} \leq v_{\mathrm{max}}\right\},$$
$$\mathcal{U}_{M_{\mathrm{vel}}} := \mathbb{R}^2.$$

When using M_{acc} and M_{vel} at the same time, the constraint on acceleration is more restrictive than the constraint on velocity until the earliest point in time $t_{v_{\mathrm{max}}}$ at which v_{max} or $-v_{\mathrm{max}}$ can be reached:

$$t_{v_{\mathrm{max}}} = \frac{v_{\mathrm{max}} - \max\left(|\underline{v}_0|, |\overline{v}_0|\right)}{a_{\mathrm{max}}} + t_0. \tag{4}$$

Thus, if $t_{v_{\mathrm{max}}} > t_0$, we can reduce the over-approximation in the reachable set of M_{vel} by initializing it at $t_{v_{\mathrm{max}}}$ with the result of M_{acc} (instead of at t_0 with $\mathcal{S}_0$):

Proposition 2 (Reachable set of M_{vel}): The reachable set of M_{vel} for $[t] > t_{v_{\mathrm{max}}}$ is

$$\mathcal{R}([t]; M_{\mathrm{vel}}, t_{v_{\mathrm{max}}}) = \left\{[x, y, v, \psi]^T \mid [x, y]^T \in \right.$$

$$\mathrm{proj}_{x,y}\left(\mathcal{R}(t_{v_{\mathrm{max}}}; M_{\mathrm{acc}}, t_0)\right) \oplus \mathcal{C}\left([0,0]^T, v_{\mathrm{max}} \cdot (\bar{t} - t_{v_{\mathrm{max}}})\right),$$

$$\left. v \in [-v_{\mathrm{max}}, v_{\mathrm{max}}], \psi \in \mathbb{R}\right\}. \qquad\square$$

Proof: The reachable set directly follows from [70, (9)]. $\qquad\blacksquare$

B. Abstraction in longitudinal direction (M_{long})

So far, we have covered constraints on absolute acceleration and absolute velocity. With abstraction M_{long}, we restrict the motion of vehicles in longitudinal direction and to the road. According to C_{road} and C_{lane}, the admissible positions on the road are obtained from the driving corridors of vehicle p as $\mathrm{occ}(\mathcal{D}^p)$.

For each driving corridor $D \in \mathcal{D}^p$, we define a curvilinear coordinate frame along a reference path $\Upsilon(\xi) : \mathbb{R} \to \mathbb{R}^2$, where the path variable ξ represents the arc length. Since we want to over-approximate the behavior of vehicles when accelerating in driving direction, we require that $\Upsilon(\xi)$ is the shortest possible path through the driving corridor. This shortest path is obtained by following the inner bound of the driving corridor (i.e., the bound in the inside of the curve), while jumping at inflection points instantaneously to the new inner bound, as described in [67, Def. 8] and illustrated in Fig. 2b–2d.

To describe motions along $\Upsilon(\xi)$, we rewrite $\boldsymbol{s}(t) = [\xi(t), v_\xi(t)]^T \in \mathbb{R}^2$ and $\mathcal{S}_0 = \left[[\xi_0], [v_{\xi_0}]\right]^T \subset \mathbb{R}^2$ by using $v_\xi(t) = v(t)$, i.e., we over-approximate the longitudinal velocity by the absolute velocity. The maximum longitudinal velocity is determined by the more restrictive constraint of C_{speedLim} and $C_{v_{\mathrm{max}}}$ (cf. Tab. I) as

$$v_{\mathrm{max}, \xi} := \min(v_{\mathrm{speedLim}} \cdot f_{\mathrm{speed}}, v_{\mathrm{max}}), \tag{5}$$

and the minimum longitudinal velocity is determined by the more restrictive constraint of C_{reverse}, $C_{v_{\min}}$, and $C_{v_{\max}}$ as

$$
v_{\min,\xi} := \begin{cases} \max(v_{\min}, 0) & \text{if } b_{\text{reverse}} = \textit{true} \\ \max(v_{\min}, -v_{\max,\xi}) & \text{otherwise.} \end{cases} \tag{6}
$$

In combination with $C_{a_{\max}}$ (only in longitudinal direction) and C_{engine}, we describe the maximum longitudinal acceleration $a_{\max,\xi}$ (i.e., the limit on increasing the signed velocity) and the minimum longitudinal acceleration $a_{\min,\xi}$ (i.e., the limit on decreasing the signed velocity) as

$$
a_{\max,\xi}\big(v_\xi(t)\big) := \tag{7a}
$$
$$
\begin{cases} 0 & \text{if } v_\xi(t) \geq v_{\max,\xi} \\ a_{\max} \cdot \frac{v_S}{|v_\xi(t)|} & \text{if } v_S \leq v_\xi(t) < v_{\max,\xi} \\ a_{\max} & \text{if } 0 \leq v_\xi(t) < \min(v_S, v_{\max,\xi}) \\ \infty & \text{if } v_\xi(t) < 0, \end{cases}
$$
$$
a_{\min,\xi}\big(v_\xi(t)\big) := \tag{7b}
$$
$$
\begin{cases} -\infty & \text{if } v_\xi(t) > 0 \\ -a_{\max} & \text{if } 0 \geq v_\xi(t) > \max(-v_S, v_{\min,\xi}) \\ -a_{\max} \cdot \frac{v_S}{|v_\xi(t)|} & \text{if } -v_S \geq v_\xi(t) > v_{\min,\xi} \\ 0 & \text{if } v_\xi(t) \leq \min(0, v_{\min,\xi}), \end{cases}
$$

which extends [67, $a_{\text{c2,long}}$] by considering reversing. Note that in (7a) and (7b), the braking acceleration (i.e., decreasing the absolute velocity) is set to infinity, since braking behaviors cannot be over-approximated using the shortest path. However, braking behaviors are already considered by M_{acc}. Since M_{acc} does not consider $v_{\min,\xi}$, we restrict the minimum reachable position (see red line in Fig. 4) to

$$
\xi_{\min}(t) := \tag{8}
$$
$$
\begin{cases} \texttt{proj}_x\big(\mathcal{R}(t_{v=0}; M_{\text{acc}}, t_0)\big) & \text{if } v_{\min,\xi} \geq 0 \wedge t \geq t_{v=0} \geq t_0 \\ -\infty & \text{otherwise,} \end{cases}
$$

when assuming without loss of generality that the mean heading is aligned with the x-axis and by transforming $\xi_{\min}(t)$ to $\Upsilon(\xi)$. Using the above definitions, we define our abstraction:

Definition 13 (Abstraction M_{long} for driving corridors): Abstraction $M_{\text{long}} := \langle \boldsymbol{f}_{M_{\text{long}}}, \mathcal{S}_{M_{\text{long}}}, \mathcal{U}_{M_{\text{long}}} \rangle$ is defined along the shortest path $\Upsilon(\xi)$ of each driving corridor D:

$$
\dot{\xi}(t) = v_\xi(t), \dot{v}_\xi(t) = u_\xi(t),
$$
$$
\mathcal{S}_{M_{\text{long}}} := \big\{ [\xi(t), v_\xi(t)]^T \,\big|\, \xi(t) \geq \xi_{\min}(t),
$$
$$
v_\xi(t) \in [v_{\min,\xi}, v_{\max,\xi}] \big\},
$$
$$
\mathcal{U}_{M_{\text{long}}} := \big\{ u_\xi(t) \in [a_{\min,\xi}\big(v_\xi(t)\big), a_{\max,\xi}\big(v_\xi(t)\big)] \big\}.
$$

Proposition 3 (Reachable set of M_{long}): The reachable set of M_{long} for $[t] \geq t_0$ is

$$
\mathcal{R}([t]; M_{\text{long}}, t_0) = \bigg\{ [\xi, v_\xi]^T \,\bigg|
$$
$$
\xi \in \bigg[\max\bigg(\int_{t_0}^{\bar{t}} \int_{t_0}^{\bar{t}} a_{\min,\xi}\big(\underline{v}_\xi(t)\big) \,\mathrm{d}^2 t, \xi_{\min}(\bar{t}) \bigg),
$$
$$
\int_{t_0}^{\bar{t}} \int_{t_0}^{\bar{t}} a_{\max,\xi}\big(\overline{v}_\xi(t)\big) \,\mathrm{d}^2 t \bigg],
$$

$$
v_\xi \in \bigg[\int_{t_0}^{\bar{t}} a_{\min,\xi}\big(\underline{v}_\xi(t)\big) \,\mathrm{d}t, \int_{t_0}^{\bar{t}} a_{\max,\xi}\big(\overline{v}_\xi(t)\big) \,\mathrm{d}t \bigg] \bigg\},
$$

where the integrals can be solved stepwise according to the discontinuities in (7). $\square$

Proof: The reachable set directly follows from [67, Thm. 2].∎

To compute the occupancy of $\mathcal{R}([t]; M_{\text{long}}, t_0)$, we enlarge $[\xi([t])]$ by $\pm\big(\overline{\ell}^2 + \overline{w}^2\big)^{1/2}$ so that all headings $\psi(t) \in \mathbb{R}$ are considered, and we restrict the lateral positions such that the occupancy remains within $\texttt{occ}(D)$.

C. Abstraction based on safe distance (M_{safe})

To consider that vehicles have to maintain a safe distance to the ego vehicle (C_{safe}), we determine the area $\mathcal{O}_{\text{safe}}$ that has to be kept free by other vehicles. In contrast to the other abstractions, we need to construct $\mathcal{O}_{\text{safe}}$ such that it is under-approximative, since $\mathcal{O}_{\text{safe}}$ is subtracted from the prediction via set difference.

We apply this abstraction M_{safe} for each forward driving corridor of the ego vehicle without laterally adjacent lanelets, i.e., $\forall \vec{D}_{\text{safe}}^{\text{ego}} \in \vec{\mathcal{D}}^{\text{ego}}(\textit{noLat}, \textit{drivDir})$ (cf. Fig. 5 and Def. 7). Vehicles driving in front of the ego vehicle are excluded for M_{safe}, since it is the responsibility of the ego vehicle to maintain a safe distance in this case. Thus, we only consider vehicles for M_{safe} that drive behind or next to the ego vehicle with the same driving direction or that can eventually merge into the lane of the ego vehicle, i.e., $\big(\vec{\mathcal{D}}(\textit{noLat}, \textit{drivDir}) \not\subseteq \vec{D}_{\text{safe}}^{\text{ego}}\big) \wedge \big(\vec{\mathcal{D}}(\textit{lat}, \textit{drivDir}) \cap \vec{D}_{\text{safe}}^{\text{ego}} \neq \emptyset\big)$ (cf. Fig. 2 and 5).

To compute the safe distance, we assume that vehicles brake until standstill and do not reverse, i.e., $b_{\text{reverse}} = \textit{true}$. We further assume that the ego vehicle may accelerate with $a_{\text{comfort}}^{\text{ego}} \geq 0$ until $v_{\max,\xi}^{\text{ego}}$ (cf. (5)), i.e., its velocity is at least $\underline{v}^{\text{ego}}(t) := \min(\underline{v}_0^{\text{ego}} + a_{\text{comfort}}^{\text{ego}} \cdot (t - t_0), v_{\max,\xi}^{\text{ego}})$. If another vehicle merges in front of the ego vehicle and performs emergency braking, we assume that the ego vehicle is able to react by braking with $-a_{\max}^{\text{ego}}$ after its reaction delay T^{ego}.

Lemma 3 (Relative safe distance): A vehicle is only allowed to merge in front of the ego vehicle if it maintains at least the safe distance d_{safe}:

$$
d_{\text{safe}}([t]) := \begin{cases} d_{\text{safe,1}} & \text{if } (a_{\max} < a_{\max}^{\text{ego}}) \wedge \Big(\frac{v^{\text{ego}}}{a_{\max}^{\text{ego}}} < \frac{v_\star}{a_{\max}} \Big) \wedge \\ & \quad (v_\star < v^{\text{ego}}) \\ d_{\text{safe,2}} & \text{otherwise,} \end{cases}
$$

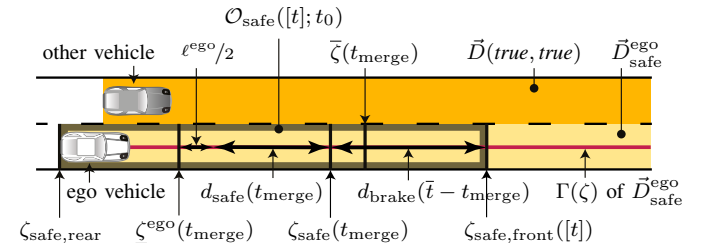
Fig. 5. The safe distance occupancy $\mathcal{O}_{\text{safe}}([t]; t_0)$ is constructed from $\zeta_{\text{safe,rear}}$ to $\zeta_{\text{safe,front}}([t])$ along $\Gamma(\zeta)$ of each $\vec{D}_{\text{safe}}^{\text{ego}}$ and considers that the other vehicle may legally be allowed to merge in front of the ego vehicle.

where

$$d_{\mathrm{safe},1} := \frac{\left(v - a_{\max} \cdot T^{\mathrm{ego}} - v^{\mathrm{ego}}\right)^2}{2 \cdot \left(a_{\max}^{\mathrm{ego}} - a_{\max}\right)} + 1/2 \cdot a_{\max} \cdot T^{\mathrm{ego}\,2} + \left(v^{\mathrm{ego}} - v\right) \cdot T^{\mathrm{ego}},$$

$$d_{\mathrm{safe},2} := \frac{v^{\mathrm{ego}\,2}}{2 \cdot a_{\max}^{\mathrm{ego}}} - \frac{v^2}{2 \cdot a_{\max}} + v^{\mathrm{ego}} \cdot T^{\mathrm{ego}},$$

with, for $[t] \geq t_0$,

$$v := \max\big(\mathrm{proj}_{\overline{v}_\xi}(\mathcal{R}(\overline{t}; M_{\mathrm{long}}, t_0)), 0\big),$$
$$v_\star := \max\big(\mathrm{proj}_{\overline{v}_\xi}(\mathcal{R}(\overline{t}; M_{\mathrm{long}}, t_0)) - a_{\max} \cdot T^{\mathrm{ego}}, 0\big),$$
$$v^{\mathrm{ego}} := \max\big(\underline{v}^{\mathrm{ego}}(\underline{t} + T^{\mathrm{ego}}), 0\big). \qquad \square$$

Proof: The safe distance for exact velocities, a single point in time, and constant velocity of the ego vehicle during T^{ego} is provided in [96, Thm. 2.8]. Since the safe distance is monotonic with respect to v and v^{ego} (which can be easily shown by computing the derivative of $d_{\mathrm{safe},1}$ and $d_{\mathrm{safe},2}$) and both v and v^{ego} are monotonic with respect to t, we can select the bound of each interval such that the safe distance is under-approximated, i.e., $\mathrm{argmin}\big(d_{\mathrm{safe}}(\cdot)\big)$, and we can allow the ego vehicle to accelerate during its reaction delay. ∎

To describe the safe distance along the centerline of the road and relative to the minimum position of the ego vehicle for an under-approximation, we define a curvilinear coordinate frame along the reference path $\Gamma(\zeta)$ for each driving corridor $\vec{D}_{\mathrm{safe}}^{\mathrm{ego}}$, where $\Gamma(\zeta)$ corresponds to the centerline (cf. Fig. 2a and 5). Thus, we rewrite the state vector as $\boldsymbol{s}(t) = [\zeta(t), v_\zeta(t)]^T$ and the safe distance in front of the ego vehicle (see Fig. 5) as

$$\zeta_{\mathrm{safe}}([t]) := \underline{\zeta}^{\mathrm{ego}}(\underline{t}) + \ell^{\mathrm{ego}}/2 + d_{\mathrm{safe}}([t]), \qquad (9)$$

where $\underline{\zeta}^{\mathrm{ego}}(\underline{t})$ is obtained from $\underline{v}^{\mathrm{ego}}(\underline{t})$. However, a vehicle can merge in front of the ego vehicle while maintaining the safe distance at

$$t_{\mathrm{merge}} := \min \big(\{t \geq t_0 \,|\, \overline{\zeta}(t) - \ell/2 \geq \zeta_{\mathrm{safe}}(t)\}\big), \qquad (10)$$

where $\overline{\zeta}(t)$ is obtained by transforming $\mathrm{proj}_{\overline{\xi}}\big(\mathcal{R}(t; M_{\mathrm{long}}, t_0)\big)$ to $\Gamma(\zeta)$ of $\vec{D}_{\mathrm{safe}}^{\mathrm{ego}}$ (see Fig. 5).

Proposition 4 (Safe distance in front of the ego vehicle): The under-approximative safe distance in front of the ego vehicle (see Fig. 5) is

$$\zeta_{\mathrm{safe,front}}([t]) :=$$
$$\begin{cases} \zeta_{\mathrm{safe}}([t]) & \text{if } \overline{t} < t_{\mathrm{merge}} \\ \zeta_{\mathrm{safe}}(t_{\mathrm{merge}}) + d_{\mathrm{brake}}(\overline{t} - t_{\mathrm{merge}}) & \text{if } t_{\mathrm{merge}} \leq \overline{t} < t_{\mathrm{standstill}} \\ \zeta_{\mathrm{safe}}(t_{\mathrm{merge}}) + d_{\mathrm{brake}}(t_{\mathrm{standstill}} - t_{\mathrm{merge}}) & \text{otherwise,} \end{cases}$$

where $d_{\mathrm{brake}}(t) := -1/2 \cdot a_{\max} \cdot t^2 + v_{\mathrm{merge}} \cdot t$, $v_{\mathrm{merge}} := \max(\mathrm{proj}_{\overline{v}_\xi}(\mathcal{R}(t_{\mathrm{merge}}; M_{\mathrm{long}}, t_0)), 0)$, and $t_{\mathrm{standstill}} := v_{\mathrm{merge}}/a_{\max} + t_0$. $\qquad \square$

Proof: For $\overline{t} < t_{\mathrm{merge}}$, (9) holds (cf. Lemma 3). At t_{merge}, the other vehicle can legally merge into $\vec{D}_{\mathrm{safe}}^{\mathrm{ego}}$ and can brake with $-a_{\max}$. Thus, for $t_{\mathrm{merge}} \leq \overline{t} < t_{\mathrm{standstill}}$, the minimum distance between the ego vehicle and the other vehicle is $\zeta_{\mathrm{safe}}(t_{\mathrm{merge}})$ plus its braking distance $d_{\mathrm{brake}}(\overline{t} - t_{\mathrm{merge}})$. For

$\overline{t} \geq t_{\mathrm{standstill}}$, the safe distance is no longer increasing, since the other vehicle could have come to a standstill. ∎

For the case that the other vehicle remains behind the ego vehicle, the safe distance is the initial position of the ego vehicle (see Fig. 5):

$$\zeta_{\mathrm{safe,rear}} := \underline{\zeta}_0^{\mathrm{ego}} - \ell^{\mathrm{ego}}/2, \qquad (11)$$

since this over-approximates a legally allowed emergency braking maneuver by the ego vehicle.

Finally, the safe distance occupancy $\mathcal{O}_{\mathrm{safe}}([t]; t_0)$ is obtained by transforming $[\zeta_{\mathrm{safe,rear}}, \zeta_{\mathrm{safe,front}}([t])]$ to the Cartesian coordinate frame and limiting the lateral positions to $\mathrm{occ}(\vec{D}_{\mathrm{safe}}^{\mathrm{ego}})$, as shown in Fig. 5.

D. Abstraction for kinematic constraints (M_{turn})

So far, we have only covered dynamic constraints that do not consider the nonholonomic constraints of vehicles. In particular, we are interested in the minimum turning radius (C_{turn}):

Definition 14 (Turning radius abstraction M_{turn}): Derived from the kinematic single-track model [97, Sec. 2.2], abstraction M_{turn} removes the maximum area a vehicle does not penetrate when turning with positive velocity and steering angle up to $\delta_{\max}$, as shown in Fig. 6:

$$\mathcal{S}_{M_{\mathrm{turn}}} := \mathbb{R}^4 \setminus (\mathcal{C}_{\mathrm{turn,left}} \cup \mathcal{C}_{\mathrm{turn,right}}),$$

where

$$\mathcal{C}_{\mathrm{turn,left}} := \mathcal{C}\big(\boldsymbol{R}(\psi) \cdot [x_{\mathrm{turn}}, R_{\mathrm{turn}}]^T + [x, y]^T, r_{\mathrm{turn}}\big),$$
$$\mathcal{C}_{\mathrm{turn,right}} := \mathcal{C}\big(\boldsymbol{R}(\psi) \cdot [x_{\mathrm{turn}}, -R_{\mathrm{turn}}]^T + [x, y]^T, r_{\mathrm{turn}}\big),$$

with $x_{\mathrm{turn}} := -\ell/2 + \ell_{\mathrm{ovr}}$, $R_{\mathrm{turn}} := \ell_{\mathrm{wb}} \cdot \tan(\pi/2 - \delta_{\max})$, and $r_{\mathrm{turn}} := R_{\mathrm{turn}} - w/2$. The rear overhang ℓ_{ovr} and the wheelbase ℓ_{wb} are vehicle parameters.

Note that the turning radius is often referred to as the radius of the path the outside front wheel is describing during turning. In contrast, our definition of r_{turn} describes the smaller radius of the path of the inside rear wheel (cf. Fig. 6). Moreover, since it is possible to enter the turning circle $\mathcal{C}_{\mathrm{turn}}$ when performing a full turn, constraint C_{turn} assumes that vehicles do not turn within lanes (cf. Tab. I and [89, 14§2]).

Given a set of initial states and uncertain vehicle parameters, we under-approximate the minimum turning radius:

Proposition 5 (Non-reachable occupancy of M_{turn}): As illustrated in Fig. 6, the time-independent area not reachable due to M_{turn} for any $[t] \geq t_0$ is

$$\mathcal{O}_{\mathrm{turn}} = \mathcal{O}_{\mathrm{turn,left}} \cup \mathcal{O}_{\mathrm{turn,right}},$$

where $\mathcal{O}_{\mathrm{turn,left}} =$

$$\bigcap_{[x_0, y_0, \psi_0, x_{\mathrm{turn}}]^T \in \mathbb{S}} \mathcal{C}\big(\boldsymbol{R}(\psi_0) \cdot [x_{\mathrm{turn}}, \underline{R}_{\mathrm{turn}}]^T + [x_0, y_0]^T, \underline{r}_{\mathrm{turn}}\big),$$

with $\mathbb{S} := \big\{\{\underline{x}_0, \overline{x}_0\} \times \{\underline{y}_0, \overline{y}_0\} \times \{\underline{\psi}_0, \overline{\psi}_0\} \times \{\underline{x}_{\mathrm{turn}}, \overline{x}_{\mathrm{turn}}\}\big\}$, $\underline{x}_{\mathrm{turn}} = -\ell/2 + \ell_{\mathrm{ovr}}$, $\overline{x}_{\mathrm{turn}} = \min(-\ell/2 + \overline{\ell}_{\mathrm{ovr}}, 0)$, $\underline{R}_{\mathrm{turn}} = \underline{\ell}_{\mathrm{wb}} \cdot \tan(\pi/2 - \delta_{\max})$, and $\underline{r}_{\mathrm{turn}} = \max(|\underline{R}_{\mathrm{turn}}| - \overline{w}/2, 0)$.
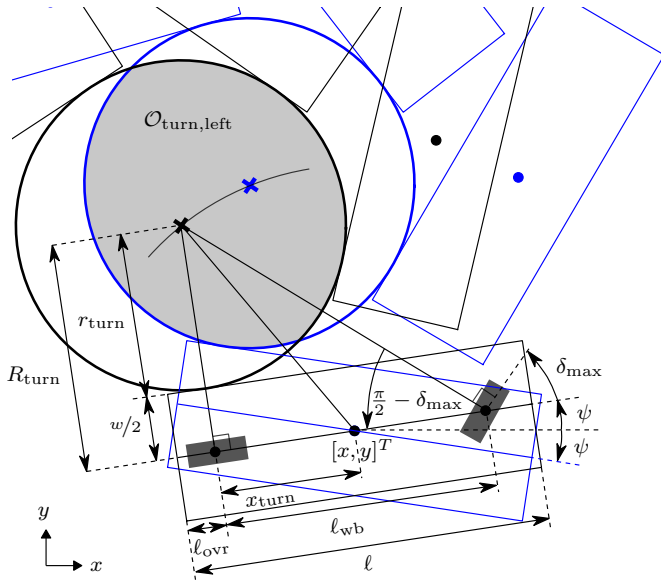
Fig. 6. $\mathcal{O}_{\mathrm{turn}}$ is constructed by intersecting the minimum turning circles of the kinematic single-track vehicle model for all initial states and uncertain vehicle parameters. For the sake of clarity, we only show the vehicle traces and turning circles for $\pm\psi$ (black and blue).

$\mathcal{O}_{\mathrm{turn,right}}$ is constructed analogous as $\mathcal{O}_{\mathrm{turn,left}}$ except that $\underline{R}_{\mathrm{turn}}$ is multiplied by -1. $\square$

Proof: To under-approximate Def. 14 for all intervals $[x_0]$, $[y_0]$, $[\psi_0]$, $[\ell]$, $[w]$, $[\ell_{\mathrm{ovr}}]$, and $[\ell_{\mathrm{wb}}]$, we would require infinitely many intersections of all possible combinations with all interval values. However, we can reduce the solution to a finite amount of intersections. The intersection of the solution using $\underline{x}_0$ and the one using $\overline{x}_0$ contains the solution for all $[x_0]$, since x_0 only linearly translates the solution over a closed interval. In addition, $[x_0]$ has no influence on the other variables. Both properties also apply to $[y_0]$ as well as $[\ell]$ and $[\ell_{\mathrm{ovr}}]$. We only need to consider the upper bound of $[w]$, since $\overline{w}$ is minimizing r_{turn} and all intersections of arbitrary circles with the same center always contain the circle with the minimum radius. Due to the same reason, the lower bound of $[\ell_{\mathrm{wb}}]$ suffices. The centers (see crosses in Fig. 6) of the turning circles with $\psi_0 \in [\underline{\psi}_0, \overline{\psi}_0]$ lie on a circular arc with radius $\|[x_{\mathrm{turn}}, R_{\mathrm{turn}}]^T\|_2$. Since $\underline{r}_{\mathrm{turn}} \leq \|[x_{\mathrm{turn}}, R_{\mathrm{turn}}]^T\|_2$ for all possible x_{turn} and R_{turn}, the intersection of the solution using $\underline{\psi}_0$ and the one using $\overline{\psi}_0$ contains the solution for all $[\psi_0]$. By intersecting the solution of all possible combinations of the remaining extreme values given in $\mathbb{S}$, we obtain the result. $\blacksquare$

In summary, abstraction M_{turn} especially reduces the over-approximation in the prediction for low initial velocities and small initial heading intervals. For high measurement uncertainties, however, $\mathcal{O}_{\mathrm{turn}}$ can also be empty.

E. Abstraction based on priority traffic rules (M_{prio})

The only constraint we have not yet considered is C_{prio}.

Definition 15 (Priority-based abstraction $M_{\mathbf{prio}}$): Based on priority traffic rules, abstraction M_{prio} restricts the

occupancy to $\mathcal{W}_{\mathrm{prio}}(t)$, which is provided by the environment model (cf. Def. 3), without constraining the dynamics.

The occupancy of M_{prio} for $[t] \geq t_0$ is $\mathcal{O}_{\mathrm{prio}}([t]; t_0) = \bigcup_{t \in [t]} \mathcal{W}_{\mathrm{prio}}(t)$. Since pedestrians often do not observe the priority of vehicular traffic, e.g., by jaywalking, $\mathcal{O}_{\mathrm{prio}}^{\mathrm{ped}}(t; t_0)$ can be extended to a more sophisticated prediction of pedestrians stepping on the road and potentially crossing it as described in [70, Sec. III-B].

F. Summary of abstractions

After introducing all abstractions and the computation of their reachable set and occupancy, we summarize the prediction for each type of traffic participant for a time interval $[t] \geq t_0$ in accordance with Lemma 1 and such that all applicable constraints of Tab. I are considered (cf. Tab. II). For vehicles, the reachable occupancy is

$$\begin{aligned}
\mathcal{O}^{\mathrm{veh}}([t]; t_0) := \ &\mathrm{occ}\big(\mathcal{R}([t]; M_{\mathrm{acc}}, t_0), \mathcal{A}\big) \cap \mathcal{O}_{\mathrm{turn}}^{\complement} \\
&\cap \mathrm{occ}\big(\mathcal{R}([t]; M_{\mathrm{long}}, t_0), \mathcal{A}\big) \\
&\cap \mathcal{O}_{\mathrm{safe}}^{\complement}([t]; t_0) \cap \mathcal{O}_{\mathrm{prio}}([t]; t_0),
\end{aligned} \tag{12}$$

where $\mathcal{O}^{\complement}$ denotes the complement of $\mathcal{O}$. For pedestrians, the reachable occupancy is

$$\begin{aligned}
\mathcal{O}^{\mathrm{ped}}([t]; t_0) := \ &\mathrm{occ}\big(\mathcal{R}([t]; M_{\mathrm{acc}}, t_0), \mathcal{A}\big) \\
&\cap \mathrm{occ}\big(\mathcal{R}([t]; M_{\mathrm{vel}}, t_0), \mathcal{A}\big) \cap \mathcal{O}_{\mathrm{prio}}([t]; t_0),
\end{aligned} \tag{13}$$

since the other abstractions are only applicable to vehicles.

VI. CONSTRAINT MANAGEMENT

Our assumptions can become violated, if other traffic participants misbehave, i.e., perform an unacceptable behavior, or if measurement uncertainties are very high. To enable the ego vehicle to react to these violations, we validate the constraint parameters $\mathcal{Q}^p$ of each traffic participant based on the current environment model Ω_0 and, if available, on the environment model Ω_{c-1} of the previous planning cycle.

We adjust the constraint parameters in case of violations such that observed but unacceptable behavior gets no longer excluded from our prediction, as described in Tab. III, which extends [14, Tab. III]. Numerical parameters are updated to the measured state plus a threshold, where we use thresholds $\Delta_{a_{\max}}, \Delta_{v_{\max}}, \Delta_{f_{\mathrm{speed}}}, \Delta_{v_{\min}}$ to prevent an updated constraint from directly being violated again, and threshold $\Delta_{v_{\mathrm{reverse}}}$ to prevent noisy velocity measurements slightly below 0 from being considered as reversing. Boolean parameters are updated to *false* so that violated constraints get disabled. C_{engine} and C_{turn} also get disabled in case of a violation by setting their parameter to the maximum value (cf. Tab. III).

Our default set of parameters $\mathcal{Q}$ is provided in Tab. IV. Note that these values are suggestions to over-approximate the real and legal motions of traffic participants in accordance with M_{real}, but that they can be adjusted to user preferences. Especially, the parameters for C_{turn} to under-approximate the turning radius should be adapted to the applicable legal regulations of the target country (cf. [89, 30§4–5]). The default values for C_{lane} forbid vehicles to overtake in a lane not

TABLE III
CONSTRAINT MANAGEMENT.

Constraint of Tab. I	If formalization of Tab. I evaluates to *false* for $t = t_0$, update parameters as
$C_{a_{\max}}$	$a_{\max} \leftarrow \bar{a}_0 + \Delta_{a_{\max}}$
$C_{v_{\max}}$	$v_{\max} \leftarrow \max\left(|\underline{v}_0|, |\bar{v}_0|\right) + \Delta_{v_{\max}}$
C_{speedLim}	$f_{\text{speed}} \leftarrow \frac{\bar{v}_0}{v_{\text{speedLim}}} + \Delta_{f_{\text{speed}}}$
C_{engine}	$v_S \leftarrow \infty$
C_{reverse}	if $\underline{v}_0 < \Delta_{v_{\text{reverse}}} : b_{\text{reverse}} \leftarrow$ *false*
$C_{v_{\min}}$	$v_{\min} \leftarrow \underline{v}_0 - \Delta_{v_{\min}}$
C_{turn}	$\delta_{\max} \leftarrow \pi/2$
C_{road}	$b_{\text{road}} \leftarrow$ *false*
C_{prio}	$b_{\text{prio}} \leftarrow$ *false*
C_{lane}	if $b_{\text{lane}_1} =$ *noLat* $: b_{\text{lane}_1} \leftarrow$ *lat* else if $b_{\text{lane}_2} =$ *drivDir* $: b_{\text{lane}_2} \leftarrow$ *anyDir* else: $b_{\text{road}} \leftarrow$ *false*

TABLE IV
DEFAULT PARAMETERS.

Constraint of Tab. I	Parameter and its default value					
$C_{a_{\max}}$	$a_{\max}^{\text{veh}}$	$8.0\,\text{m/s}^2$	$a_{\max}^{\text{ped}}$	$1.0\,\text{m/s}^2$	$a_{\max}^{\text{cyc}}$	$3.5\,\text{m/s}^2$
	$\Delta_{a_{\max}}$	$0.5\,\text{m/s}^2$				
$C_{v_{\max}}$	$v_{\max}^{\text{veh}}$	$70.0\,\text{m/s}$	$v_{\max}^{\text{ped}}$	$2.0\,\text{m/s}$	$v_{\max}^{\text{cyc}}$	$12.0\,\text{m/s}$
	$\Delta_{v_{\max}}^{\text{veh}}$	$0.5\,\text{m/s}$				
C_{speedLim}	f_{speed}	1.2	$\Delta_{f_{\text{speed}}}$	0.1		
C_{engine}	v_S^{veh}	$7.0\,\text{m/s}$	v_S^{cyc}	∞		
C_{reverse}	b_{reverse}	*true*	$\Delta_{v_{\text{reverse}}}$	$-1.0\,\text{m/s}$		
$C_{v_{\min}}$	$v_{\min}$	$-10.0\,\text{m/s}$	$\Delta_{v_{\min}}$	$1.0\,\text{m/s}$		
C_{turn}	$\underline{\ell}_{\text{wb}}^{\text{car}}$	$1.8\,\text{m}$	$\underline{\ell}_{\text{wb}}^{\text{motcyc}}$	$1.1\,\text{m}$	$\underline{\ell}_{\text{wb}}^{\text{cyc}}$	$0.8\,\text{m}$
	$\underline{\ell}_{\text{wb}}^{\text{truck}}$	$3.0\,\text{m}$	$\underline{\ell}_{\text{wb}}^{\text{bus}}$	$3.0\,\text{m}$		
	$\delta_{\max}$	$1.0\,\text{rad}$	$\underline{\ell}_{\text{ovr}}$	0		
	$\bar{\ell}_{\text{ovr}}^{\text{car}}$	$3.7\,\text{m}$	$\bar{\ell}_{\text{ovr}}^{\text{motcyc}}$	$1.0\,\text{m}$	$\bar{\ell}_{\text{ovr}}^{\text{cyc}}$	$1.0\,\text{m}$
	$\bar{\ell}_{\text{ovr}}^{\text{truck}}$	$3.7\,\text{m}$	$\bar{\ell}_{\text{ovr}}^{\text{bus}}$	$4.9\,\text{m}$		
C_{road}	b_{road}	*true*				
C_{prio}	b_{prio}	*true*				
C_{lane}	b_{lane_1}	*lat*	b_{lane_2}	*drivDir*		
C_{safe}	T^{ego}	$1.0\,\text{s}$	$a_{\text{comfort}}^{\text{ego}}$	$1.0\,\text{m/s}^2$		
$\mathcal{A}^{\text{phantom}}$	w	0	ℓ	$0.5\,\text{m}$	r	$0.25\,\text{m}$

appropriate to the direction of traffic, since such a behavior is only allowed if not endangering or interfering with oncoming traffic [88, 11§2(c)], and thus it is forbidden in the vicinity of the ego vehicle.

VII. EXPERIMENTAL RESULTS

For a prediction that claims to be over-approximative (cf. our problem statement in Sec. II-E), it is crucial to demonstrate this property. In our previous work, we have already shown

conformance of the prediction on recorded data of 1074 vehicles in [67, Sec. V-C] and of 400 pedestrians in [70, Sec. IV-A], and we have evaluated how conservative the prediction is against a high-fidelity vehicle model in [67, Sec. V-B]. These results demonstrate that the ground-truth trajectories were always contained in the prediction and that the over-approximation was not unreasonably conservative.

In this paper, we want to demonstrate that our prediction works on complicated, real-world scenarios and, despite being over-approximative, allows the ego vehicle to obtain collision-free trajectories. Therefore, we simulate an urban intersection with occlusions in Sec. VII-A, and, for the first time, we present real-world experiments with test vehicles in Sec. VII-B and VII-C. The video attachment of this paper[3] contains further results. For all experiments, we used the parameters of Tab. IV if not noted otherwise and implemented Alg. 1 without considering interaction, i.e., we omitted the optional line 13. Initial positions are over-approximated either by rectangles aligned with the mean heading of the traffic participant or by circles to ease the consideration of the traffic participant's size. As representation for the predicted set, we choose polygons for the position domain and intervals for the other states. Thus, the states are not coupled with each other to allow for efficient computations despite some over-approximations.

A. Intersection with occlusions and priorities

Fig. 7 presents an urban intersection with different detected traffic participants. The road network is provided with one layer for vehicles and one for bicycles, and the speed limit of all lanes is $v_{\text{speedLim}} = 13.89\,\text{m/s}$. Due to occlusions and a limited sensor range with radius of $33\,\text{m}$, the field of view $\mathcal{F}_0$ is restricted. To capture this risk, our approach creates 3 phantom vehicles, 2 phantoms cyclists, and 24 static phantom obstacles. The prediction result is shown for a time horizon of $1.0\,\text{s}$ with a time step size of $0.1\,\text{s}$. The oncoming phantom vehicle (from the top) is forbidden to make a left turn, since the ego vehicle has the right of way, which is modeled by $\mathcal{W}_{\text{prio}}(t)$. Based on the predicted occupancies, the ego vehicle can decide when to safely proceed into the intersection.

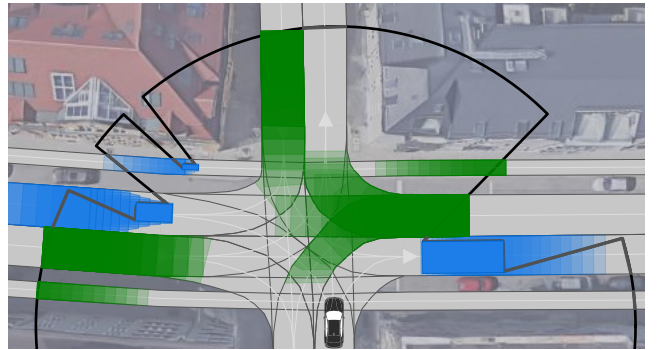[3]The video attachment is also available at http://go.tum.de/812843.

Fig. 7. Urban intersection (CommonRoad ID: S=DEU_Muc-30_1_S-1:2018b [98]): the ego vehicle (black) has to yield to crossing traffic. Since two vehicles (blue) and one cyclist (blue) cause occlusions, we create phantom traffic participants (dynamic: green, static: grey) at the boundary of the field of view (black). (background image: Google, GeoBasis-DE/BKG)
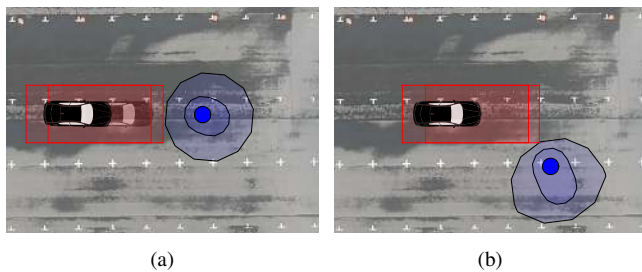
(a)   (b)

Fig. 8. Online verification of parking maneuvers for the ego vehicle (black) considering a pedestrian (blue). The predicted occupancy of the pedestrian (light blue) and the occupancy of the verified maneuver of the ego vehicle including safety margins (red) are both shown for two time intervals, $t \in [0\,\text{s}, 0.8\,\text{s}]$ and $[0.8\,\text{s}, 1.6\,\text{s}]$. (a) The ego vehicle executed a verified braking maneuver such that it definitely will come to a stop in front of the pedestrian. The recorded stopping position of the ego vehicle $1.6\,\text{s}$ later is shown transparently. (b) Since the occupancies did not intersect anymore, a new maneuver for the ego vehicle has been verified as safe. A video of this real-world experiment is attached to this paper[3].

B. Online verification considering pedestrians

We have performed online verification of maneuvers in the presence of pedestrians. Online verification ensures that the ego vehicle only executes trajectories that have been verified as safe [3], [8]. For our experiments, we want to achieve passive safety, i.e., a trajectory is verified as safe if the maneuver is collision-free against all acceptable future behaviors of surrounding traffic participants and brings the ego vehicle to a standstill. In particular, our self-driving BMW 5 series test vehicle has to avoid collisions with pedestrians in a parking lot, i.e., an unstructured environment. The ego vehicle receives trajectories that are following a predefined path with constant velocity $v_{\text{des}}^{\text{ego}} = 2.0\,\text{m/s}$ for a planning horizon of $t_h = 1.6\,\text{s}$ (with constant time offset to be robust against processing time delays). These intended trajectories are not aware of pedestrians. Thus, we append a path-consistent braking profile to the given intended trajectory such that the ego vehicle comes to a stop within t_h, and we predict the pedestrians using $a_{\text{max}}^{\text{ped}} = 2.0\,\text{m/s}^2$. If the new trajectory does not intersect with the predicted occupancies, the ego vehicle will execute it; otherwise, it will keep executing the trajectory that has been verified in the previous planning cycle.

This online verification has been executed on our test vehicle on November 09, 2018, and Fig. 8 shows recordings of these real-world experiments. Since the pedestrian was blocking the path of the ego vehicle, the ego vehicle eventually could not verify a new trajectory and, by executing the previously verified trajectory, came to a stop (see Fig. 8a). A few seconds later, the pedestrian walked away and a new trajectory has been verified as safe (see Fig. 8b).

C. Online experiments on public roads

We have executed our prediction online in a test vehicle on public roads. Therefore, we implemented our approach in C++ on a BMW 7 series test vehicle. The environment model provides the initial states of surrounding traffic participants based on [33] and the rectangular field of view without occlusions that extends $100\,\text{m}$ in longitudinal and $60\,\text{m}$ in lateral direction of the current pose of the ego vehicle. We use

the planner of [15] to obtain trajectories for the ego vehicle that are collision-free against all predicted occupancies and bring the ego vehicle to a standstill; for the few cases the initial velocity is too high to come to a standstill within the planning horizon, we constrain the final state to comply with safe distances to predicted traffic participants. The prediction and planning horizon is $3.0\,\text{s}$ with a time step size of $0.25\,\text{s}$.

We conducted four test drives in Germany from 1.30 p.m. to 5 p.m. on Wednesday, March 13, 2019. Each test drive was along the $17\,\text{km}$ long route between the BMW Autonomous Driving Campus in Unterschleißheim and the BMW Research and Innovation Center in Munich and contains both urban and rural multi-lane roads with speed limits ranging from $8.3\,\text{m/s}$ to $27.8\,\text{m/s}$. While we have performed the prediction online, we did not perform the trajectory planning closed-loop but offline in a postprecessing step, since approval by authorities has not yet been given. In all test drives combined, we have predicted $163,715$ detected and $211,863$ phantom traffic participants (dynamic and static) in $29,818$ replanning steps. Fig. 1 and 9 show exemplary results. Predicted occupancies and planned trajectories are shown for the full time horizon. The visualization of the ego vehicle, its trajectory, and other traffic participants can have a slight time offset to each other due to the asynchronous updates. Overall, the results demonstrate that the prediction performs well in arbitrary road networks and with vast numbers of traffic participants. Even in crowded environments, the prediction incorporates the interaction with the ego vehicle and allows to obtain collision-free trajectories, while containing all acceptable behaviors of other traffic participants. Only in a few situations, a new safe trajectory for the ego vehicle could not be obtained, as shown in Fig. 10; since the prediction was not provided with $\mathcal{W}_{\text{prio}}(t)$, it could not consider the right of way for the ego vehicle.

During the real-world experiments, our legal specification has been violated a few times by the recorded traffic participants. Tab. V evaluates how often the constraint management had to update the values of the constraints according to Tab. III, when using as initial values the ones of Tab. IV except for v_{min}. For each parameter, we present its relative number of updates for all detected, dynamic traffic participants in our test drives (i.e., for $90,779$ motorized vehicles, $15,650$ pedestrians, and $4,770$ cyclists), the maximum value it has been updated to, and the mean value of all updated values. Note that the maximum and mean values are the measured values plus our thresholds (cf. Tab. III). In most cases, the violations were caused by high measurement uncertainties or an incomplete environment model, e.g., when no driving corridor was provided for a traffic participant (see Fig. 10). In other cases, a traffic participant indeed violated our specification. Since the mean values of all violations are only slightly above the initial values, the initial parameterization seems reasonable, but can be adjusted to user preferences. To reduce the influence of violated constraints on the safety of motion plans, we refer to [11]. Legal safety can be ensured despite constraint violations by planning fail-safe trajectories [15] and switching to a reactive mode for collision mitigation in case of inevitable collisions.

(b) The pedestrian is predicted to cross the road perpendicular plus a deviation depending on its heading.

(a) Even on multi-lane roads, the ego vehicle has enough free space, since the safe distance forbids passing vehicles from merging directly in front of the ego vehicle.

(c) While overtaking a truck, a vehicle ahead is merging into the lane of the ego vehicle.

Fig. 9. Set-based prediction of various traffic participants (car: green, truck/bus: red, cyclist: turquoise, motorcyclist: blue, pedestrian: magenta, static: grey box, phantom: grey area) in different urban and rural scenarios of our real-world experiments. Based on the predicted occupancies, we successfully obtained collision-free trajectories (red) for the ego vehicle (silver-colored vehicle). Videos of further real-world experiments are attached[3].

Let us finally evaluate the required computation times for the prediction, i.e., for the loop over all traffic participants in Alg. 1. The test vehicle is equipped with an Intel i7 6900K processor and 64 GB memory; the frequency of the processor is underclocked from 3.2 GHz to 1.2 GHz to improve the energy consumption and heat management. The mean computation time for one planning cycle was $9.86\,\text{ms}$ with a standard deviation of $12.02\,\text{ms}$ for a prediction horizon of $2.0\,\text{s}$. Note that the outliers mostly occurred due to high computational load caused by other software modules. Further

experiments showed that the computation time is linear with the prediction horizon.

VIII. CONCLUSIONS AND FUTURE WORK

We have presented a set-based prediction for provably safe motion planning based on legal safety. Our prediction is guaranteed to contain all acceptable behaviors in accordance with a legal specification. This is achieved by rigorous computations in a formal manner, nondeterministic models that over-approximate the dynamics of the traffic participants, and conservative parameterization. As prediction features, we use longitudinal and lateral dynamics, the motion history, and the types of traffic participants in combination with contextual information and the field of view.

For the first time, we have validated our prediction in test vehicles. These real-world experiments demonstrate that our

TABLE V
EVALUATION OF THE CONSTRAINT MANAGEMENT.

| Constraint of Tab. I	Parameter	Initial value	Mean value of updates	Max. value of updates	Num. of updates
$C_{a_{\max}}$	$a_{\max}^{\text{veh}}$	$8.0\,\text{m/s}^2$	$9.50\,\text{m/s}^2$	$15.14\,\text{m/s}^2$	$0.03\,\%$
	$a_{\max}^{\text{ped}}$	$1.0\,\text{m/s}^2$	$2.18\,\text{m/s}^2$	$7.41\,\text{m/s}^2$	$6.91\,\%$
	$a_{\max}^{\text{cyc}}$	$3.5\,\text{m/s}^2$	$4.57\,\text{m/s}^2$	$7.89\,\text{m/s}^2$	$0.59\,\%$
$C_{v_{\max}}$	$v_{\max}^{\text{veh}}$	$70.0\,\text{m/s}$	n/a	n/a	$0.00\,\%$
	$v_{\max}^{\text{ped}}$	$2.0\,\text{m/s}$	$3.39\,\text{m/s}$	$6.78\,\text{m/s}$	$5.83\,\%$
	$v_{\max}^{\text{cyc}}$	$12.0\,\text{m/s}$	$12.92\,\text{m/s}$	$13.48\,\text{m/s}$	$0.27\,\%$
C_{speedLim}	f_s^{veh}	1.2	1.43	3.36	$0.21\,\%$
C_{engine}	v_s^{veh}	$7.0\,\text{m/s}$	n/a	∞	$0.83\,\%$
C_{reverse}	$b_{\text{reverse}}^{\text{veh}}$	*true*	n/a	n/a	$2.01\,\%$
	$b_{\text{reverse}}^{\text{cyc}}$	*true*	n/a	n/a	$0.27\,\%$
$C_{v_{\min}}$	$v_{\min}^{\text{veh}}$	$-1.0\,\text{m/s}$	$-1.64\,\text{m/s}$	$-10.93\,\text{m/s}$	$2.01\,\%$
	$v_{\min}^{\text{cyc}}$	$-1.0\,\text{m/s}$	$-2.10\,\text{m/s}$	$-5.84\,\text{m/s}$	$0.27\,\%$
$C_{\text{lane}}/\,C_{\text{road}}$	$b_{\text{road}}^{\text{veh}}$	*true*	n/a	n/a	$2.27\,\%$
	$b_{\text{road}}^{\text{cyc}}$	*true*	n/a	n/a	$31.07\,\%$
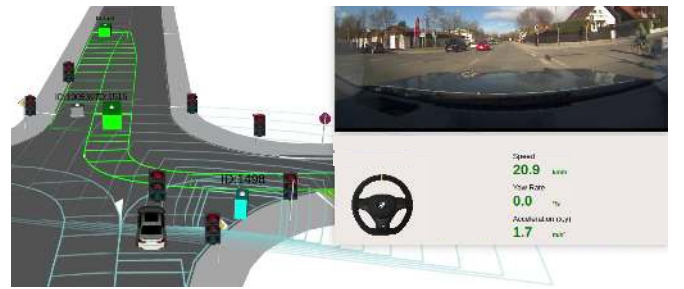
Fig. 10. Situation of our real-world experiments (cf. Fig. 9) in which a safe trajectory could not be obtained. Since the environment model did not restrict the priority-based positions $\mathcal{W}_{\text{prio}}(t)$ for the oncoming vehicle (ID 1515), the prediction allows this vehicle to traverse the lane of the ego vehicle. In addition, since the environment model did not provide a driving corridor for the cyclist (ID 1498) next to the ego vehicle, the constraint management updated $b_{\text{road}} \leftarrow$ *false* and the prediction of this cyclist can only use M_{acc}.

prediction runs online in arbitrary traffic scenarios and that motion planners are able to obtain collision-free trajectories despite the over-approximative prediction and even in congested environments. In addition, our constraint management successfully dealt with traffic participants that violate traffic rules, high measurement uncertainties, and incomplete environment models.

For a good performance of the prediction, we require a detailed and precise environment model with strictly bounded measurement uncertainties. Future work includes more restrictive bounds on the admissible velocity by considering the curvature of the road and on the admissible lateral acceleration (e.g., based on [99]) while remaining over-approximative. It also seems interesting to use our proposed set-based prediction as propagation model for object tracking.

ACKNOWLEDGMENTS

REFERENCES

[1] B. Vanholme, D. Gruyer, B. Lusetti, S. Glaser, and S. Mammar, "Highly automated driving on highways based on legal safety," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 1, pp. 333–347, 2013.

[2] R. Kianfar, P. Falcone, and J. Fredriksson, "Safety verification of automated driving systems," *IEEE Intelligent Transportation Systems Magazine*, vol. 5, pp. 73–86, 2013.

[3] 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.

[4] S. Mitsch, K. Ghorbal, D. Vogelbacher, and A. Platzer, "Formal verification of obstacle avoidance and navigation of ground robots," *Int. Journal of Robotics Research*, vol. 36, no. 12, pp. 1312–1340, 2017.

[5] W. Schwarting, J. Alonso-Mora, and D. Rus, "Planning and decision-making for autonomous vehicles," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 1, no. 1, pp. 187–210, 2018.

[6] K. Maček, D. Vasquez, T. Fraichard, and R. Siegwart, "Towards safe vehicle navigation in dynamic urban scenarios," *Automatika*, vol. 50, no. 3-4, pp. 184–194, 2009.

[7] S. Shalev-Shwartz, S. Shammah, and A. Shashua, "On a formal model of safe and scalable self-driving cars," *arXiv:1708.06374v1 [cs.RO]*, pp. 1–25, 2017.

[8] C. Pek, S. Manzinger, M. Koschi, and M. Althoff, "Using online verification to prevent autonomous vehicles from causing accidents," *Nature Machine Intelligence*, vol. 2, pp. 518–528, 2020.

[9] S. Söntges and M. Althoff, "Computing the drivable area of autonomous road vehicles in dynamic road scenes," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 6, pp. 1855–1866, 2018.

[10] S. Söntges, M. Koschi, and M. Althoff, "Worst-case analysis of the time-to-react using reachable sets," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2018, pp. 1891–1897.

[11] C. Pek, M. Koschi, M. Werling, and M. Althoff, "Enhancing motion safety by identifying safety-critical passageways," in *Proc. of the 56th IEEE Conference on Decision and Control*, 2017, pp. 320–326.

[12] M. Koschi, C. Pek, S. Maierhofer, and M. Althoff, "Computationally efficient safety falsification of adaptive cruise control systems," in *Proc. of the 22nd IEEE Int. Conf. on Intelligent Transportation Systems*, 2019, pp. 2879–2886.

[13] C. Pek and M. Althoff, "Efficient computation of invariably safe states for motion planning of self-driving vehicles," in *Proc. of the IEEE Int. Conf. on Intelligent Robots and Systems*, 2018, pp. 3523–3530.

[14] M. Koschi and M. Althoff, "SPOT: A tool for set-based prediction of traffic participants," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2017, pp. 1679–1686.

[15] C. Pek and M. Althoff, "Computationally efficient fail-safe trajectory planning for self-driving vehicles using convex optimization," in *Proc. of the 21st IEEE Int. Conf. on Intelligent Transportation Systems*, 2018, pp. 1447–1454.

[16] P. F. Orzechowski, A. Meyer, and M. Lauer, "Tackling occlusions & limited sensor range with set-based safety verification," in *Proc. of the 21st IEEE Int. Conf. on Intelligent Transportation Systems*, 2018, pp. 1729–1736.

[17] P. F. Orzechowski, K. Li, and M. Lauer, "Towards responsibility-sensitive safety of automated vehicles with reachable set analysis," in *Proc. of the IEEE Int. Conf. on Connected Vehicles and Expo*, 2019, pp. 1–6.

[18] S. Manzinger, C. Pek, and M. Althoff, "Using reachable sets for trajectory planning of automated vehicles," *IEEE Transactions on Intelligent Vehicles*, 2020, [available online].

[19] W. Zhan, C. Liu, C. Chan, and M. Tomizuka, "A non-conservatively defensive strategy for urban autonomous driving," in *Proc. of the 19th IEEE Int. Conf. on Intelligent Transportation Systems*, 2016, pp. 459–464.

[20] S. Vaskov, H. Larson, S. Kousik, M. Johnson-Roberson, and R. Vasudevan, "Not-at-fault driving in traffic: A reachability-based approach," in *Proc. of the 22nd IEEE Int. Conf. on Intelligent Transportation Systems*, 2019, pp. 2785–2790.

[21] F. Gruber and M. Althoff, "Anytime safety verification of autonomous vehicles," in *Proc. of the 21st IEEE Int. Conf. on Intelligent Transportation Systems*, 2018, pp. 1708–1714.

[22] C. Pek, M. Koschi, and M. Althoff, "An online verification framework for motion planning of self-driving vehicles with safety guarantees," in *AAET - Automatisiertes und vernetztes Fahren*, 2019, pp. 260–274.

[23] M. Althoff, A. Giusti, S. B. Liu, and A. Pereira, "Effortless creation of safe robots from modules through self-programming and self-verification," *Science Robotics*, vol. 4, no. 31, 2019.

[24] S. Lefèvre, D. Vasquez, and C. Laugier, "A survey on motion prediction and risk assessment for intelligent vehicles," *ROBOMECH Journal*, vol. 1, no. 1, pp. 1–14, 2014.

[25] A. Rudenko, L. Palmieri, M. Herman, K. M. Kitani, D. M. Gavrila, and K. O. Arras, "Human motion trajectory prediction: A survey," *Int. Journal of Robotics Research*, vol. 39, no. 8, pp. 895–935, 2020.

[26] F. Camara, N. Bellotto, S. Cosar, F. Weber, D. Nathanael, M. Althoff, J. Wu, J. Ruenz, A. Dietrich, G. Markkula, A. Schieben, F. Tango, N. Merat, and C. Fox, "Pedestrian models for autonomous driving part II: High level models of human behaviour," *IEEE Transactions on Intelligent Transportation Systems*, 2020, [available online].

[27] L. Claussmann, M. Revilloud, D. Gruyer, and S. Glaser, "A review of motion planning for highway autonomous driving," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 5, pp. 1826–1848, 2019.

[28] D. González, J. Pérez, V. Milanés, and F. Nashashibi, "A review of motion planning techniques for automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1135–1145, 2016.

[29] B. Paden, M. Čáp, S. Z. Yong, D. Yershov, and E. Frazzoli, "A survey of motion planning and control techniques for self-driving urban vehicles," *IEEE Transactions on Intelligent Vehicles*, vol. 1, no. 1, pp. 33–55, 2016.

[30] J. Dahl, G. R. de Campos, C. Olsson, and J. Fredriksson, "Collision avoidance: A literature review on threat-assessment techniques," *IEEE Transactions on Intelligent Vehicles*, vol. 4, no. 1, pp. 101–113, 2019.

[31] A. Rangesh and M. M. Trivedi, "No blind spots: Full-surround multi-object tracking for autonomous vehicles using cameras and lidars," *IEEE Transactions on Intelligent Vehicles*, vol. 4, no. 4, pp. 588–599, 2019.

[32] A. Brunetti, D. Buongiorno, G. F. Trotta, and V. Bevilacqua, "Computer vision and deep learning techniques for pedestrian detection and tracking: A survey," *Neurocomputing*, vol. 300, pp. 17–33, 2018.

[33] S. Steyer, C. Lenk, D. Kellner, G. Tanzmeister, and D. Wollherr, "Grid-based object tracking with nonlinear dynamic state and shape estimation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 7, pp. 2874–2893, 2019.

[34] Y. Emzivat, J. Ibanez-Guzman, H. Illy, P. Martinet, and O. H. Roux, "A formal approach for the design of a dependable perception system for autonomous vehicles," in *Proc. of the 21st IEEE Int. Conf. on Intelligent Transportation Systems*, 2018, pp. 2452–2459.

[35] D. Feng, L. Rosenbaum, and K. Dietmayer, "Towards safe autonomous driving: Capture uncertainty in the deep neural network for lidar 3d vehicle detection," in *Proc. of the 21st IEEE Int. Conf. on Intelligent Transportation Systems*, 2018, pp. 3266–3273.

[36] M. T. Le, F. Diehl, T. Brunner, and A. Knoll, "Uncertainty estimation for deep neural object detectors in safety-critical applications," in *Proc. of the 21st IEEE Int. Conf. on Intelligent Transportation Systems*, 2018, pp. 3873–3878.

[37] D. Elliott, W. Keen, and L. Miao, "Recent advances in connected and automated vehicles," *Journal of Traffic and Transportation Engineering*, vol. 6, no. 2, pp. 109–131, 2019.

[38] S. W. Loke, "Cooperative automated vehicles: A review of opportunities and challenges in socially intelligent vehicles beyond networking," *IEEE Transactions on Intelligent Vehicles*, vol. 4, no. 4, pp. 509–518, 2019.

[39] M. Brännström, E. Coelingh, and J. Sjöberg, "Model-based threat assessment for avoiding arbitrary vehicle collisions," *IEEE Transactions on Intelligent Transportation Systems*, vol. 11, no. 3, pp. 658–669, 2010.

[40] A. Eidehall and L. Petersson, "Statistical threat assessment for general road scenes using Monte Carlo sampling," *IEEE Transactions on Intelligent Transportation Systems*, vol. 9, pp. 137–147, 2008.

[41] C. Lienke, C. Wissing, M. Keller, T. Nattermann, and T. Bertram, "Predictive driving: Fusing prediction and planning for automated highway driving," *IEEE Transactions on Intelligent Vehicles*, vol. 4, no. 3, pp. 456–467, 2019.

[42] N. Deo, A. Rangesh, and M. M. Trivedi, "How would surround vehicles move? A unified framework for maneuver classification and motion prediction," *IEEE Transactions on Intelligent Vehicles*, vol. 3, no. 2, pp. 129–140, 2018.

[43] M. Bahram, C. Hubmann, A. Lawitzky, M. Aeberhard, and D. Wollherr, "A combined model- and learning-based framework for interaction-aware maneuver prediction," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 6, pp. 1538–1550, 2016.

[44] M. Schreier, V. Willert, and J. Adamy, "An integrated approach to maneuver-based trajectory prediction and criticality assessment in arbitrary road environments," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 10, pp. 2751–2766, 2016.

[45] J. Schulz, C. Hubmann, J. Löchner, and D. Burschka, "Interaction-aware probabilistic behavior prediction in urban environments," in *Proc. of the IEEE/RSJ Int. Conf. on Intelligent Robots and Systems*, 2018, pp. 3999–4006.

[46] R. Quintero Mínguez, I. Parra Alonso, D. Fernández-Llorca, and M. A. Sotelo, "Pedestrian path, pose, and intention prediction through gaussian process dynamical models and pedestrian activity recognition," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1803–1814, 2019.

[47] F. Altché and A. de La Fortelle, "An LSTM network for highway trajectory prediction," in *Proc. of the 20th IEEE Int. Conf. on Intelligent Transportation Systems*, 2017, pp. 353–359.

[48] H. Xiong, F. B. Flohr, S. Wang, B. Wang, J. Wang, and K. Li, "Recurrent neural network architectures for vulnerable road user trajectory prediction," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2019, pp. 171–178.

[49] T. A. Wheeler, P. Robbel, and M. J. Kochenderfer, "Analysis of microscopic behavior models for probabilistic modeling of driver behavior," in *Proc. of the 19th IEEE Int. Conf. on Intelligent Transportation Systems*, 2016, pp. 1604–1609.

[50] J. Quehl, H. Hu, O. Ş. Taş, E. Rehder, and M. Lauer, "How good is my prediction? Finding a similarity measure for trajectory prediction evaluation," in *Proc. of the 20th IEEE Int. Conf. on Intelligent Transportation Systems*, 2017, pp. 1–6.

[51] T. Gindele, S. Brechtel, and R. Dillmann, "Learning driver behavior models from traffic observations for decision making and planning," *IEEE Intelligent Transportation Systems Magazine*, vol. 7, no. 1, pp. 69–79, 2015.

[52] G. Xie, H. Gao, L. Qian, B. Huang, K. Li, and J. Wang, "Vehicle trajectory prediction by integrating physics- and maneuver-based approaches using interactive multiple models," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 7, pp. 5999–6008, 2018.

[53] L. Sun, W. Zhan, D. Wang, and M. Tomizuka, "Interactive prediction for multiple, heterogeneous traffic participants with multi-agent hybrid dynamic bayesian network," in *Proc. of the 22nd IEEE Int. Conf. on Intelligent Transportation Systems*, 2019, pp. 1025–1031.

[54] D. Lenz, F. Diehl, M. T. Le, and A. Knoll, "Deep neural networks for markovian interactive scene prediction in highway scenarios," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2017, pp. 685–692.

[55] C. Tang, J. Chen, and M. Tomizuka, "Adaptive probabilistic vehicle trajectory prediction through physically feasible bayesian recurrent neural network," in *Proc. of the IEEE Int. Conf. on Robotics and Automation*, 2019, pp. 3846–3852.

[56] S. Zernetsch, H. Reichert, V. Kress, K. Doll, and B. Sick, "Trajectory forecasts with uncertainties of vulnerable road users by means of neural networks," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2019, pp. 810–815.

[57] E. A. I. Pool, J. F. P. Kooij, and D. M. Gavrila, "Context-based cyclist path prediction using recurrent neural networks," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2019, pp. 824–830.

[58] I. Batkovic, M. Zanon, N. Lubbe, and P. Falcone, "A computationally efficient model for pedestrian motion prediction," in *Proc. of the European Control Conference*, 2018, pp. 374–379.

[59] P. Nadarajan and M. Botsch, "Probability estimation for predicted-occupancy grids in vehicle safety applications based on machine learning," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2016, pp. 1285–1292.

[60] B. Kim, C. M. Kang, J. Kim, S. H. Lee, C. C. Chung, and J. W. Choi, "Probabilistic vehicle trajectory prediction over occupancy grid map via recurrent neural network," in *Proc. of the 20th IEEE Int. Conf. on Intelligent Transportation Systems*, 2017, pp. 399–404.

[61] S. Hoermann, M. Bach, and K. Dietmayer, "Dynamic occupancy grid prediction for urban autonomous driving: A deep learning approach with fully automatic labeling," in *Proc. of the IEEE Int. Conf. on Robotics and Automation*, 2018, pp. 2056–2063.

[62] M. Itkina, K. Driggs-Campbell, and M. J. Kochenderfer, "Dynamic environment prediction in urban scenes using recurrent representation learning," in *Proc. of the 22nd IEEE Int. Conf. on Intelligent Transportation Systems*, 2019, pp. 2052–2059.

[63] J. Wu, J. Ruenz, and M. Althoff, "Probabilistic map-based pedestrian motion prediction taking traffic participants into consideration," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2018, pp. 1285–1292.

[64] W. Zhan, A. de La Fortelle, Y. Chen, C. Chan, and M. Tomizuka, "Probabilistic prediction from planning perspective: Problem formulation, representation simplification and evaluation metric," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2018, pp. 1150–1156.

[65] M. Brännström, F. Sandblom, and L. Hammarstrand, "A probabilistic framework for decision-making in collision avoidance systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 2, pp. 637–648, 2013.

[66] M. Althoff, O. Stursberg, and M. Buss, "Model-based probabilistic collision detection in autonomous driving," *IEEE Transactions on Intelligent Transportation Systems*, vol. 10, no. 2, pp. 299–310, 2009.

[67] M. Althoff and S. Magdici, "Set-based prediction of traffic participants on arbitrary road networks," *IEEE Transactions on Intelligent Vehicles*, vol. 1, no. 2, pp. 187–202, 2016.

[68] M. Hartmann and D. Watzenig, "Optimal motion planning with reachable sets of vulnerable road users," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2019, pp. 891–898.

[69] M. Koschi and M. Althoff, "Interaction-aware occupancy prediction of road vehicles," in *Proc. of the 20th IEEE Int. Conf. on Intelligent Transportation Systems*, 2017, pp. 1885–1892.

[70] M. Koschi, C. Pek, M. Beikirch, and M. Althoff, "Set-based prediction of pedestrians in urban environments considering formalized traffic rules," in *Proc. of the 21st IEEE Int. Conf. on Intelligent Transportation Systems*, 2018, pp. 2704–2711.

[71] K. Driggs-Campbell, R. Dong, and R. Bajcsy, "Robust, informative human-in-the-loop predictions via empirical reachable sets," *IEEE Transactions on Intelligent Vehicles*, vol. 3, no. 3, pp. 300–309, 2018.

[72] P. Zechel, R. Streiter, K. Bogenberger, and U. Göhner, "Pedestrian occupancy prediction for autonomous vehicles," in *Proc. of the 3rd IEEE Int. Conf. on Robotic Computing*, 2019, pp. 230–235.

[73] W. Chung, S. Kim, M. Choi, J. Choi, H. Kim, C. Moon, and J. Song, "Safe navigation of a mobile robot considering visibility of environment," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 3941–3950, 2009.

[74] S. Bouraine, T. Fraichard, and H. Salhi, "Provably safe navigation for mobile robots with limited field-of-views in dynamic environments," *Autonomous Robots*, vol. 32, pp. 267–283, 2012.

[75] D. Phan, J. Yang, R. Grosu, S. A. Smolka, and S. D. Stoller, "Collision avoidance for mobile robots with limited sensing and limited information about moving obstacles," *Formal Methods in System Design*, vol. 51, no. 1, pp. 62–86, 2017.

[76] Y. Nager, A. Censi, and E. Frazzoli, "What lies in the shadows? Safe and computation-aware motion planning for autonomous vehicles using intent-aware dynamic shadow regions," in *Proc. of the IEEE Int. Conf. on Robotics and Automation*, 2019, pp. 5800–5806.

[77] R. Matsumi, P. Raksincharoensak, and M. Nagai, "Study on autonomous intelligent drive system based on potential field with hazard anticipation," *Journal of Robotics and Mechatronics*, vol. 27, no. 1, pp. 5–11, 2015.

[78] F. Damerow, T. Puphal, Y. Li, and J. Eggert, "Risk-based driver assistance for approaching intersections of limited visibility," in *Proc. of the IEEE Int. Conf. on Vehicular Electronics and Safety*, 2017, pp. 178–184.

[79] M. Lee, K. Jo, and M. Sunwoo, "Collision risk assessment for possible collision vehicle in occluded area based on precise map," in *Proc. of the 20th IEEE Int. Conf. on Intelligent Transportation Systems*, 2017, pp. 1–6.

[80] M. Yu, R. Vasudevan, and M. Johnson-Roberson, "Occlusion-aware risk assessment for autonomous driving in urban environments," *IEEE Robotics and Automation Letters*, vol. 4, no. 2, pp. 2235–2241, 2019.

[81] S. Brechtel, T. Gindele, and R. Dillmann, "Probabilistic decision-making under uncertainty for autonomous driving using continuous POMDPs," in *Proc. of the 17th IEEE Int. Conf. on Intelligent Transportation Systems*, 2014, pp. 392–399.

[82] M. Bouton, A. Nakhaei, K. Fujimura, and M. J. Kochenderfer, "Scalable decision making with sensor occlusions for autonomous driving," in *Proc. of the IEEE Int. Conf. on Robotics and Automation*, 2018, pp. 2076–2081.

[83] C. Hubmann, N. Quetschlich, J. Schulz, J. Bernhard, D. Althoff, and C. Stiller, "A POMDP maneuver planner for occlusions in urban scenarios," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2019, pp. 1909–1916.

[84] X. Lin, J. Zhang, J. Shang, Y. Wang, H. Yu, and X. Zhang, "Decision making through occluded intersections for autonomous driving," in *Proc. of the 22nd IEEE Int. Conf. on Intelligent Transportation Systems*, 2019, pp. 2449–2455.

[85] M. Schratter, M. Bouton, M. J. Kochenderfer, and D. Watzenig, "Pedestrian collision avoidance system for scenarios with occlusions," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2019, pp. 1054–1060.

[86] M. Sadou, V. Polotski, and P. Cohen, "Occlusions in obstacle detection for safe navigation," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2004, pp. 716–721.

[87] O. Ş. Taş and C. Stiller, "Limited visibility and uncertainty aware motion planning for automated driving," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2018, pp. 1171–1178.

[88] M. Naumann, H. Konigshof, M. Lauer, and C. Stiller, "Safe but not overcautious motion planning under occlusions and limited sensor range," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2019, pp. 140–145.

[89] United Nations Economic Commission for Europe, "Convention on road traffic," United Nations Conference on Road Traffic, 1968, (consolidated version of 2006), https://www.unece.org/fileadmin/DAM/trans/conventn/Conv_road_traffic_EN.pdf.

[90] A. Gning and P. Bonnifait, "Constraints propagation techniques on intervals for a guaranteed localization using redundant data," *Automatica*, vol. 42, no. 7, pp. 1167–1175, 2006.

[91] A. Lambert, D. Gruyer, B. Vincke, and E. Seignez, "Consistent outdoor vehicle localization by bounded-error state estimation," in *Proc. of the IEEE/RSJ Int. Conf. on Intelligent Robots and Systems*, 2009, pp. 1211–1216.

[92] F. Poggenhans, J.-H. Pauls, J. Janosovits, S. Orf, M. Naumann, F. Kuhnt, and M. Mayr, "Lanelet2: A high-definition map framework for the future

[93] of automated driving," in *Proc. of the 21st IEEE Int. Conf. on Intelligent Transportation Systems*, 2018, pp. 1672–1679.

[93] P. Bender, J. Ziegler, and C. Stiller, "Lanelets: Efficient map representation for autonomous driving," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2014, pp. 420–425.

[94] A. Censi, K. Slutsky, T. Wongpiromsarn, D. Yershov, S. Pendleton, J. Fu, and E. Frazzoli, "Liability, ethics, and culture-aware behavior specification using rulebooks," in *Proc. of the IEEE/RSJ Int. Conf. on Intelligent Robots and Systems*, 2019, pp. 8536–8542.

[95] J. Casey, *A Sequel to the First Six Books of the Elements of Euclid, Containing an Easy Introduction to Modern Geometry with Numerous Examples.* Dublin: Hodges, Figgis, & Co., 1888.

[96] A. Rizaldi, "Formal specification, monitoring, and verification of autonomous vehicles with Isabelle/HOL," Dissertation, Technische Universität München, 2019, http://nbn-resolving.de/urn/resolver.pl?urn:nbn:de:bvb:91-diss-20191218-1484146-1-4.

[97] R. Rajamani, *Vehicle Dynamics and Control.* Springer, 2012.

[98] M. Althoff, M. Koschi, and S. Manzinger, "CommonRoad: Composable benchmarks for motion planning on roads," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2017, pp. 719–726.

[99] P. Zechel, R. Streiter, K. Bogenberger, and U. Göhner, "Assumptions of lateral acceleration behavior limits for prediction tasks in autonomous vehicles," in *Proc. of the 7th Int. Conf. on Mechatronics Engineering*, 2019, pp. 1–6.

Markus Koschi is a research associate in the Cyber-Physical Systems Group at the Department of Informatics of the Technical University of Munich, Germany, since 2016. He received the Master of Science degree in mechanical engineering from the Technical University of Munich in 2016. His research interests include motion planning, behavior prediction, safety verification, and falsification of autonomous vehicles towards a future of zero traffic accidents.

Matthias Althoff is an associate professor in computer science at Technische Universität München, Germany. He received his diploma engineering degree in mechanical engineering in 2005, and his Ph.D. degree in electrical engineering in 2010, both from Technische Universität München, Germany. From 2010 to 2012 he was a postdoctoral researcher at Carnegie Mellon University, Pittsburgh, USA, and from 2012 to 2013 an assistant professor at Technische Universität Ilmenau, Germany. His research interests include formal verification of continuous and hybrid systems, reachability analysis, planning algorithms, nonlinear control, automated vehicles, and power systems.