Formal Verification of Swerving Maneuvers for Car Collision Avoidance

Aakash Abhishek Harry Sood Jean-Baptiste Jeannin

***Abstract*— Many road vehicle accidents are the result of collisions with foreign objects, and automatic collision avoidance is of critical interest to car manufacturers and their customers. Previous work on formally verifying collision avoidance maneuvers typically assumes point-shaped or circular-shaped vehicles for simplicity. In this paper, we formulate and formally verify sufficient conditions for the safety of a representative collision avoidance system for cars with a realistic geometrical shape. The collision avoidance system discussed here is designed to issue swerving advisories. We model the vehicle kinematics and control advisory as a hybrid program, allowing to model both discrete decisions of the system and continuous dynamics of the car. We formally verify the collision avoidance system by providing rigorous, computer-checked mathematical proofs of collision avoidance under well-defined, explicit sufficient conditions on vehicle kinematics and parameters. This formal verification provides a mathematical guarantee that the collision avoidance system can prevent the vehicle from collision under all possible scenarios as long as certain conditions hold true.**

We model the system using differential dynamic logic d$\mathcal{L}$ and use the automated theorem prover KeYmaera X for formal verification. This work employs a purely symbolic model, and can thus be extended to verify other types of collision avoidance systems exhibiting richer behavior.

***Keywords*— Formal Verification, Hybrid Systems, Automotive Systems, Car Collision Avoidance.**

I. INTRODUCTION

A major cause of motor vehicle accidents is a collision with other fixed objects and vehicles, and the avoidance of such collisions is one of the main areas targeted by driving safety mechanisms. This task of autonomously guiding a vehicle, while avoiding surrounding objects, requires the ability to predict the vehicle's trajectory under different control inputs, and also requires the design of autonomous controllers for guiding the vehicle in a given environment. Predicting a vehicle's behavior in response to control inputs has been extensively studied through various vehicle dynamics models, e.g. [6], [21], [24]. Similarly, the area of path planning for obstacle avoidance is thoroughly developed, e.g. [8], [9], [12].

However, practical implementations of existing car collision avoidance systems involve interaction between cyber systems (discrete controllers, processing units, digital sensors) and physical systems (the vehicle). Because of the underlying strong coupling of the cyber and physical systems, successfully implementing such a collision-avoidance controller is a non-trivial task. Furthermore, it is difficult to guarantee that the collision avoidance system will work as intended – i.e., prevent collisions – in every possible scenario. Nonetheless, its correctness is of utmost importance due to the safety-critical nature of the problem. Hence, there is a need for mathematically verifying the performance and safety of such a system and of its implementation.

In this work, we have formulated and formally verified explicit sufficient conditions for the safety of a simple yet representative collision avoidance system for a planar vehicle of rectangular shape such as a car. This formal verification provides a mathematical guarantee that the system will prevent the vehicle from collisions under any possible scenario as long as some well-defined conditions are satisfied. For simplicity, we assume that the vehicle's behavior while turning conforms to pure Ackermann's steering [11], and its speed is assumed to be fixed throughout its motion. This essentially renders some points on the vehicle to be a Dubin's Vehicle, and restricts their behavior to traversing a combination of circular curves and straight lines in a fixed plane, at a constant speed. This resulting trajectory is also called a Dubin's path [4] (Fig. 1). The obstacle has been modeled as a static point in the vehicle's plane of motion. Our collision avoidance system is modeled as a discrete controller, which switches the vehicle's motion from a circular trajectory to a straight line trajectory, and vice-versa, thus rendering the overall kinematics of the vehicle piece-wise continuous. Finally, our model is purely symbolic (rather than numeric), and the results are thus applicable to a vast number of cases, with any variation of the involved parameters.

To verify our collision avoidance system, we model the overall kinematics of the vehicle as a hybrid program, and specify collision avoidance as a safety property in differential dynamic logic [16]. We then formally verify this safety property under some well-defined explicit sufficient conditions on dynamic variables, thereby guaranteeing safety of the collision avoidance system. To formalize the overall kinematics involving piece-wise continuous differential equations and to state the collision avoidance property of the system unambiguously, we have used *differential dynamic logic* d$\mathcal{L}$ [16] and utilized the d$\mathcal{L}$ theorem prover KeYmaera X [5] to perform the machine-checked formal verification.

Challenges - For a purely symbolic model of collision avoidance system and a rectangular vehicle, formulating the explicit sufficient condition that ensures collision avoidance under all possible scenarios and variations of the

Authors are with the University of Michigan, Ann Arbor, MI 48109, USA. Aakash Abhishek is an MSE student with the Department of Mechanical Engineering aakashme@umich.edu. Harry Sood is a BSE student with the Department of Aerospace Engineering hsood@umich.edu. Jean-Baptiste Jeannin is an Assistant Professor of Aerospace Engineering jeannin@umich.edu. Toyota Research Institute ("TRI") provided funds to assist the authors with their research but this article solely reflects the opinions and conclusions of its authors and not TRI or any other Toyota entity.

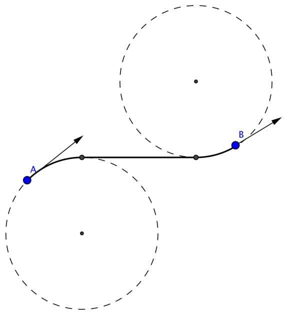

Fig. 1: Trajectory of a Dubin's vehicle

involved parameters is challenging. The developed vehicle kinematics model also has transcendental solutions involving trigonometric functions. The presence of these transcendental solutions makes the arithmetic generally undecidable. To circumvent this, we follow the method of Platzer [17], [19], modeling the involved transcendental functions as auxiliary variables within our hybrid program, and using a differential-invariant-based method for verifying the safety property.

II. KINEMATICS AND DIFFERENTIAL DYNAMIC LOGIC

A. *Vehicle Kinematics*

We first derive the kinematics for a point vehicle moving at a constant speed using the Unicycle motion model. Subsequently, we assume that the extended rectangular vehicle conforms to pure Ackermann's steering [11] (Fig. 2). Using this assumption along with the kinematics of a point vehicle, we generate the kinematic model of the extended vehicle. We strategically choose the location of the point vehicle to coincide with the midpoint of the extended vehicle's rear axle (point C in Fig. 2), as this provides a simplification that the heading of our extended vehicle lies parallel to the instantaneous velocity $\vec{v}$ of the point vehicle C at all times. This simplification is a direct result of the kinematic constraints implied by Ackermann's steering [11] (Fig. 2).

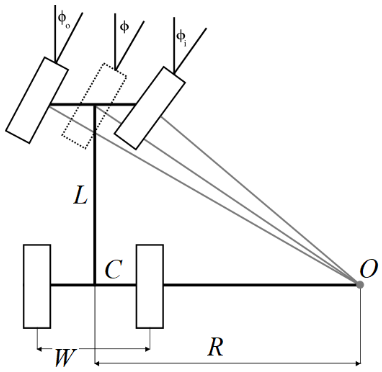

Fig. 2: Ackermann's steering geometry

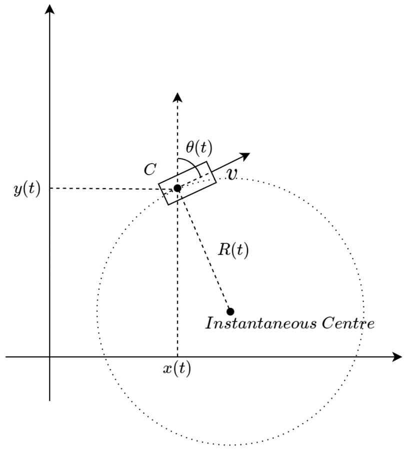

Fig. 3: Kinematic diagram

The kinematic diagram of the point vehicle is shown in Fig. 3, and describes a circle. The derived equations of motion for the extended vehicle are:

$$\dot{x}(t) = v\sin(\theta(t)) \tag{1}$$

$$\dot{y}(t) = v\cos(\theta(t)) \tag{2}$$

$$R(t) = \begin{cases} \frac{v^2}{\mu g} & \text{if } R_{min} \leq \frac{v^2}{\mu g} \text{ and } \mu \leq \mu_o \\ R_{min} & \text{if } R_{min} > \frac{v^2}{\mu g} \end{cases} \tag{3}$$

$$\omega(t) = \dot{\theta}(t) = v/R(t) \tag{4}$$

Here, $x(t), y(t)$ and $R(t)$ (Fig. 3), are the position coordinates and the instantaneous radius of curvature of the point vehicle. R_{min} is the minimum possible turning radius at the rear axle's center of the extended vehicle, due to its steering geometry's physical constraint, and (μ, μ_o) are the effective coefficients of kinetic and static friction between the vehicle and the road, respectively. $\theta(t)$ and $\omega(t)$, denote the heading angle and yaw rate of the extended vehicle. Equations (1) - (4) form the full kinematic model of our extended vehicle.

B. *Swerving Behavior*

In order to analyze the swerving behavior of the extended vehicle, we introduce the following parameters/assumptions:

- The extended vehicle's body is assumed to be a rectangle of length L and width W.
- The distances from the front and rear bumper of the vehicle to its rear axle are l_F and l_R, resp. (Fig. 4)
- While swerving, the instantaneous radius of curvature R (measured at the center of the rear axle, C) remains constant with $R \geq R_{min}$ and $R \geq \frac{v^2}{\mu_o g}$.
- c is a turn-indicating parameter; $c = -1$ if the vehicle is turning right and $c = +1$ if it is turning left.

We also assume that during the transition between straight and swerving motions, the vehicle's wheels instantly turn to match the new direction of travel. Although this instantaneous change in wheel direction is not dynamically feasible, we assume it for simplicity.

Fig. 4 depicts a scenario where the vehicle is just starting its swerve of radius R, in order to avoid colliding with the obstacle at (x_{obs}, y_{obs}). We mark this time instant as t_1. Note

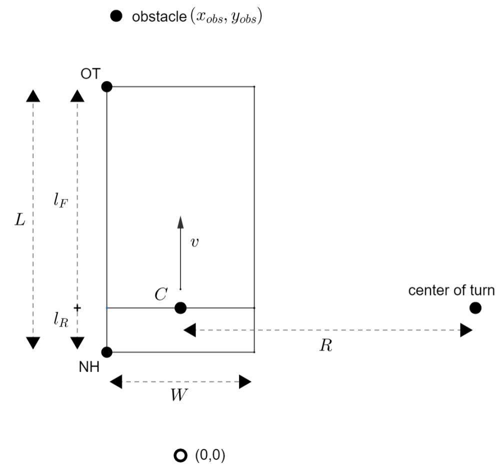

Fig. 4: Vehicle schematic at the start of turn

that here the coordinate system's origin is at the vehicle's rear axle's center at time $t = 0$. With the parameters/assumptions listed above, the closed form solution for equations of motion (1) - (4) is as follows:

$$\theta(t) = \begin{cases} 0 & \text{for } t \leq t_1 \\ \frac{-cv(t-t_1)}{R} & \text{for } t > t_1 \end{cases} \tag{5}$$

$$(x,y) = \begin{cases} (0, vt) & \text{for } t \leq t_1 \\ \Big(c\left(R\cos|\theta(t)| - R\right), & \text{for } t > t_1 \\ \quad (vt_1 + R\sin|\theta(t)|)\Big) & \end{cases} \tag{6}$$

In order to monitor that the extended vehicle does not collide with the obstacle, we track the position of its critical boundary points. In Fig. 4, OT and NH are respectively the points on the front and rear edge of the vehicle, farther from the center of the turning circle. Since the other boundary points of the rectangular vehicle are not critical in avoiding a collision, their analysis is omitted. The trajectory for OT and NH can be found using Equation (6):

$$\begin{aligned}(x_{OT}, y_{OT}) := \Big(&\Big(x - c\big(l_f \sin|\theta(t)| - \frac{W}{2}\cos|\theta(t)|\big)\Big), \\ &\Big(y + l_f \cos|\theta(t)| + \frac{W}{2}\sin|\theta(t)|\Big)\Big)\end{aligned} \tag{7}$$

$$\begin{aligned}(x_{NH}, y_{NH}) := \Big(&\Big(x + c\big(l_r \sin|\theta(t)| + \frac{W}{2}\cos|\theta(t)|\big)\Big), \\ &\Big(y - l_r \cos|\theta(t)| + \frac{W}{2}\sin|\theta(t)|\Big)\Big)\end{aligned} \tag{8}$$

Fig. 5 depicts the trajectory of the boundary points of the vehicle for a right-turn. This figure has been generated by numerically simulating equations (5)-(8) in MATLAB, using standard values for the various parameters involved. Fig. 5 also shows that while turning right, for a brief period of time, the boundary point NH moves towards the left. This is purposely exaggerated in the inset of Fig. 5. This phenomenon leads to the formation of a "notch", where NH protrudes to the left from the initial (at $t = t_1$) left edge of the vehicle. The time duration t_{NH}, for which the point NH stays in this notch and the maximum distance dev_{NH}, that it sticks out from the vehicle's initial left boundary can be calculated as:

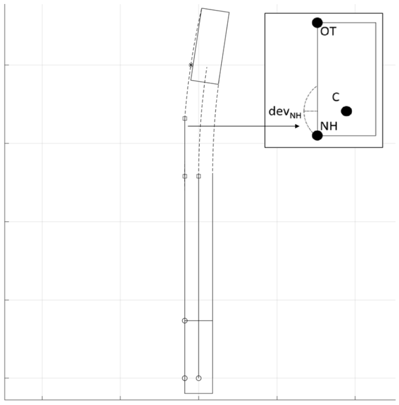

Fig. 5: Vehicle's trajectory and notch formation while turning

$$t_{NH} = \frac{2\tan^{-1}\left(\frac{l_R}{R+\frac{W}{2}}\right)}{\omega} \tag{9}$$

$$dev_{NH} = \sqrt{l_R^2 + \left(R + \frac{W}{2}\right)^2} - R - \frac{W}{2} \tag{10}$$

The value of dev_{NH} for standard automobiles is usually of the order of centimeters, e.g. for a 2020 Toyota Corolla XLE [1], with $R = 10$ m, $dev_{NH} = 4.2689$ cm.

In the rest of this work, the rectangular vehicle is assumed to have no body extending behind its rear axle, i.e. $l_R = 0$. This assumption is made to avoid the effects of the "notch" formed by the vehicle body extending behind its rear axle. This is reasonable as point NH (Fig.4) stays inside the boundary traced by point OT, except for the "notch" which is negligible (a few centimeters) for standard automobiles. For vehicles with a longer length behind the rear-axle such as busses, the notch becomes more significant.

C. Differential Dynamic Logic d$\mathscr{L}$

The differential dynamic logic d$\mathscr{L}$ [16] is an extension of dynamic logic supporting ordinary differential equations. It supports discrete assignments, implementation of choice and control loops, and execution of differential equations [17]–[19], which makes it an appropriate modeling choice for our work. We model our system as a hybrid program (HP) [17], as used by differential dynamic logic. A brief description of some of the operators of d$\mathscr{L}$ used in our model is given below.

- α^* : non-deterministic repetition operator which repeats the program α for zero or more times.
- $(x' = \theta \ \& \ Q)$: continuous evolution of the state x within the evolution domain Q, along the differential equation $(x' = \theta)$, for any arbitrary (positive) amount of time.

- $p \rightarrow [\alpha]\ q$: says that all executions of hybrid program α starting in a state satisfying logical formula p, end up in a state satisfying q.

For a more comprehensive description of differential dynamic logic d$\mathscr{L}$ and its operators, readers are referred to original sources such as [16], [17], [19].

III. FORMAL VERIFICATION OF A SWERVING MANEUVER

A. Collision Avoidance System

We have modeled our collision avoidance system as a discrete controller. This controller acts by providing steering inputs to the vehicle, thereby swerving it in a circular trajectory through a certain angle in order to prevent collision. Subsequently, after passing the obstacle, the system straightens the wheel to zero the steering input, and the car continues in a straight line. Fig. 6 shows the schematic of the collision avoidance system.

The collision avoidance system's advisories are assumed to be of the following form:

- Advisory issued from the collision avoidance system is of the form (R, θ^{max}), where R is the suggested radius of turn (measured at point C) and θ^{max} is the advised angle of turn with respect to the initial direction of travel.
- Advisory is valid i.e. $R \geq R_{min}$, $\frac{v^2}{R} \leq \mu_0 g$ and $\theta^{max} < \frac{\pi}{2}$.
- We assume that the values of $\cos(\theta^{max}) = c_{min}$ and $\sin(\theta^{max}) = s_{max}$ are available to us a priority.
- After following the advisory, i.e., turning through angle θ^{max} with a constant speed of $v = v_o$, the car proceeds straight with the same speed.
- The advisory is assumed to involve right turn only. This does not result in any loss of generality, since the case of left turn is symmetric.

The coordinate frame for the model is centered at the center of the circular path suggested by the advisory and t is considered 0 at the instant the vehicle starts turning. Furthermore, an auxiliary parameter, $t_o = \frac{R\theta^{max}}{v_o}$, is introduced as the time instant when the vehicle leaves the circular trajectory and starts moving straight.

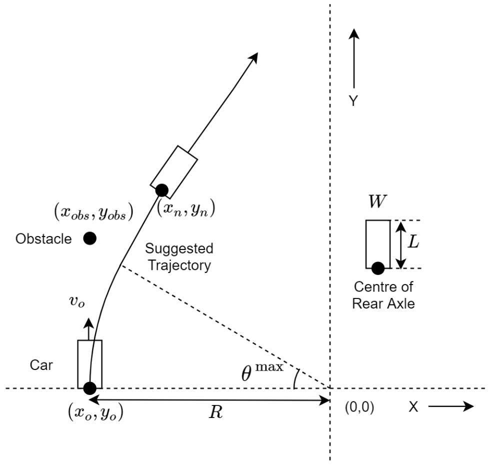

Fig. 6: Schematic of collision avoidance system

Under the assumptions listed above, the solution trajectories for Equations (1) - (4) are given by (11) and (12). These trajectories have been used in formulating the d$\mathscr{L}$ model.

$$t \leq t_o : \begin{cases} x(t) = -R\cos(\theta(t)) \\ y(t) = R\sin(\theta(t)) \\ \theta(t) = (v_o t)/R \end{cases} \tag{11}$$

$$t > t_o : \begin{cases} x(t) = -R\cos(\theta^{max}) + v_o(t - t_o)\sin(\theta^{max}) \\ y(t) = R\sin(\theta^{max}) + v_o(t - t_o)\cos(\theta^{max}) \\ \theta(t) = \theta^{max} \end{cases} \tag{12}$$

B. d$\mathscr{L}$ Model[1]

In developing the d$\mathscr{L}$ model of our collision avoidance system, we have utilized the notion of "safety regions" [10] for a given advisory (R, θ^{max}). A safety region for a given advisory is defined as the set of all possible positions of an obstacle, such that the current advisory prevents the vehicle from colliding with the obstacle. Using this definition, all the points to the left of the outer boundary formed by the trajectory of OT (Fig. 7) and below the horizontal axis $y = 0$, fall into the safety region. Points on the right side of the of trajectory of IN, fall into the safety region as well.

The full double-sided safety region is shown in Fig. 8. In Fig. 9, only the left side part of the full safety region is shown, defining it as the single-sided safety region. In this paper, we have worked with only single-sided safety regions and, have omitted the cases where the obstacle lies on the right side of the advised trajectory. Readers interested in the formal proves of collision avoidance with double-sided safety regions are referred to [2]. Also, the safety region depiction will look different for different relative values of the involved parameters and advisory. Fig. 10 shows one such possible variation of the single-sided safety region. However, since our d$\mathscr{L}$ model is purely symbolic, the theorems and their

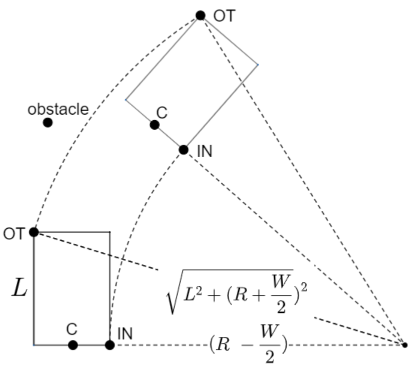

Fig. 7: Turning circle for swerving

[1] The formal models and proofs described in this paper are available at https://jeannin.github.io/papers/acc20.zip

formal proofs discussed here are constructed in a manner that encompasses all such possible geometric variations.

To verify the collision avoidance system, we use two different (but equivalent) formulations of the safety region: an *implicit* formulation, which is better amenable to formal proofs but cannot directly be checked at run-time because it contains quantifiers; and an *explicit* formulation, which contains explicit expressions for the safety region boundary but is comparatively less amenable to formal proofs. Our approach consists of proving our model with respect to the implicit formulation (it is easier), then proving that our implicit and explicit formulations are equivalent. Therefore, we formulate the following safety theorems, that we make more precise in the next section:

Theorem 1 (sketch):
(obstacle initially in the implicit safety region)
$\rightarrow$ [(Turning Dynamics)*] (No collisions in the future)
Theorem 2 (sketch):
(implicit safety region) $\leftrightarrow$ (explicit safety region)
Corollary 1 (sketch):
(obstacle initially in the explicit safety region)
$\rightarrow$ [(Turning Dynamics)*] (No collisions in the future)

The first theorem is a safety property of the hybrid program modeling our collision avoidance system. It encodes the requirement for the collision avoidance system to never let the car collide with the obstacle. The second theorem states the equivalence between two definitions of safety regions, thereby providing sufficient conditions for collision avoidance which can be checked at run-time. In the following d$\mathscr{L}$ theorems, the following notation is used:

- Point C's location (center of the rear axle) (Fig.7) is represented by the coordinate (x, y).
- The sine and cosine of the vehicle's heading angle when it is at (x, y) is represented by s and c.
- The time t is the time spent in straight-line motion after the circular turn. t during the turn is set ideally to 0.
- A general point located on the nominal trajectory (solution trajectory) is represented by the coordinate (x_n, y_n).
- The sine and cosine of the vehicle's heading angle at (x_n, y_n) is represented by s_n and c_n.
- The time t_n is the associated time in straight-line motion for the nominal trajectory.
- (x_{obs}, y_{obs}) represent the stationary obstacle's location.

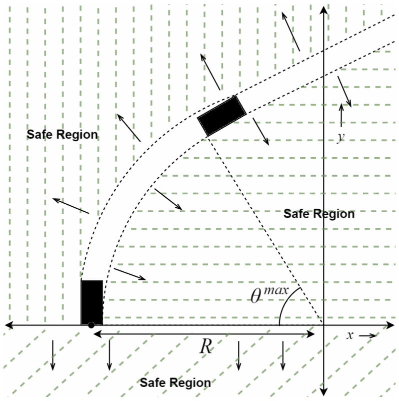

Fig. 8: Double-sided safety region

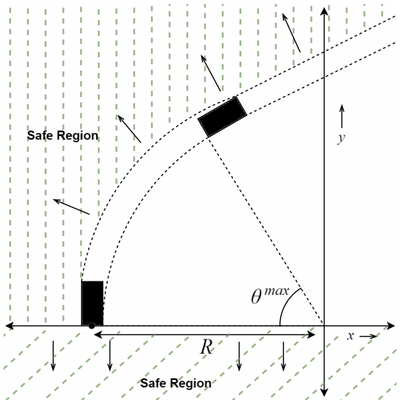

Fig. 9: Single-sided safety region

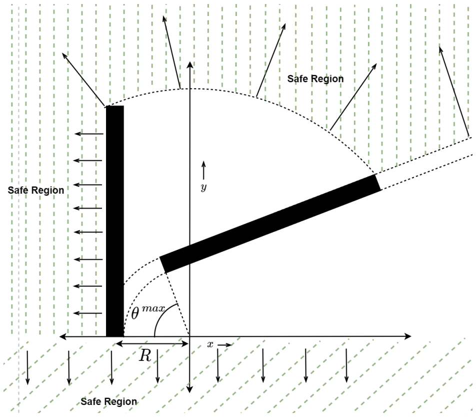

Fig. 10: Variation of single-sided safety region

C. d$\mathscr{L}$ Theorem

The following theorems are a mathematical representation of the sketches presented before. The intuition behind the *implicit* formulation of the safety region is: "for any position of the car along its trajectory ($\forall x_n, y_n, t_n, s_n, c_n$), no obstacle should intersect the car (a rectangle) at that position." "$(c(x_{obs} - x) - s(y_{obs} - y) > W/2 \vee |s(x_{obs} - x) + c(y_{obs} - y) - L/2| > L/2)$". In contrast, the *explicit* safety region explicitly models the safety region drawn on Fig. (9)-(10). $case_1 \rightarrow bound_1$ encodes the safety of the bottom half-plane ($y_{obs} < 0$); $case_2 \rightarrow bound_2$ and $case_3 \rightarrow bound_3$ encode the safety regions surrounding the turning part of the maneuver, while $case_4 \rightarrow bound_4$ encodes the safety region surrounding the straight part of the maneuver. Fig. 7 can be referred to interpret some of the expressions appearing in the *explicit* formulation L_{expl} of the safety region.

$$
\begin{aligned}
init \equiv \ \Big(& v_o > 0 \ \wedge \ l \geq 0 \ \wedge \ w \geq 0 \ \wedge \ R > \frac{W}{2} \\
& \wedge \ c_{min} > 0 \ \wedge \ c_{min} \leq 1 \ \wedge \ s = 0 \wedge \ c = 1 \ \wedge \\
& x = -R \wedge \ y = 0 \wedge \ t = 0 \ \Big)
\end{aligned}
$$

Implicit Formulation: Single Sided Safety Region

$$
\begin{aligned}
L_{impl} \equiv \;\; & \forall x_n, \forall y_n, \forall t_n, \forall s_n, \forall c_n \Big(\\
& \Big(\big(t_n = 0 \;\wedge\; c_n \geq c_{min} \;\wedge\; s_n \geq 0 \;\wedge\; s_n^2 = 1 - c_n^2 \\
& \wedge\; x_n = -Rc_n \;\wedge\; y_n = Rs_n \big) \\
& \vee\; \big(t_n \geq 0 \;\wedge\; c_n = c_{min} \wedge\; s_n \geq 0 \\
& \wedge\; s_n^2 = 1 - c_n^2 \;\wedge\; x_n = -Rc_n + v_o t_n s_n \\
& \wedge\; y_n = Rs_n + v_o t_n c_n \big) \Big) \\
& \rightarrow \Big(y_{obs} < 0 \vee \Big(c(x_{obs} - x_n) - s(y_{obs} - y_n) < -\frac{W}{2} \Big) \\
& \quad \vee \;\; \Big(\mid s(x_{obs} - x_n) + c(y_{obs} - y_n) - \frac{L}{2} \mid \; > \frac{L}{2} \Big) \Big)
\end{aligned}
$$

Explicit Formulation: Single Sided Safety Region

$$
\begin{aligned}
case_1 &\equiv y_{obs} < 0 \\
bound_1 &\equiv -\infty \leq x_{obs} \leq \infty
\end{aligned}
$$

$$
\begin{aligned}
case_2 &\equiv 0 \leq y_{obs} < L \\
bound_2 &\equiv x_{obs} < -\Big(R + \frac{W}{2}\Big) \\
& \qquad \vee \Big(y_{obs} \geq \Big(R + \frac{W}{2}\Big) s_{max} + Lc_{min} \\
& \qquad \wedge x_{obs}^2 > L^2 + \Big(R + \frac{W}{2}\Big)^2 - y_{obs}^2 \\
& \qquad \wedge x_{obs} < -\Big(\frac{(R + \frac{W}{2}) - y_{obs} s_{max}}{c_{min}} \Big) \Big)
\end{aligned}
$$

$$
\begin{aligned}
case_3 &\equiv L \leq y_{obs} < \sqrt{\Big(L^2 + \Big(R + \frac{W}{2}\Big)^2 \Big)} \\
bound_3 &\equiv x_{obs} < -\Big(R + \frac{W}{2}\Big) \\
& \qquad \vee \;\; \Big(L \leq y_{obs} < \Big(R + \frac{W}{2}\Big) s_{max} + Lc_{min} \\
& \qquad \wedge \;\; x_{obs}^2 > \Big(R + \frac{W}{2}\Big)^2 + L^2 - y_{obs}^2 \Big) \\
& \qquad \vee \;\; \Big(\Big(R + \frac{W}{2}\Big) s_{max} + Lc_{min} \;\; \leq y_{obs} \\
& \qquad \wedge \;\; x_{obs} < -\Big(\frac{(R + \frac{W}{2}) - y_{obs} s_{max}}{c_{min}} \Big) \\
& \qquad \wedge \;\; x_{obs}^2 > \Big(R + \frac{W}{2}\Big)^2 + L^2 - y_{obs}^2 \Big)
\end{aligned}
$$

$$
\begin{aligned}
case_4 &\equiv \sqrt{\Big(L^2 + \Big(R + \frac{W}{2}\Big)^2 \Big)} \;\; \leq y_{obs} \\
bound_4 &\equiv x_{obs} < -\Big(\frac{(R + \frac{W}{2}) - y_{obs} s_{max}}{c_{min}} \Big)
\end{aligned}
$$

$$
L_{expl} \equiv (\wedge_{i=1}^{4} (case_i \rightarrow bound_i))
$$

Theorem 1: Verification for Collision Avoidance

$$
\begin{aligned}
& init \wedge L_{impl} \rightarrow \\
& \qquad \Big[\Big(\Big(\big(\dot{s} = c\frac{v_o}{R}, \dot{c} = -s\frac{V_o}{R}, \dot{x} = v_o s, \dot{y} = v_o c \\
& \qquad \& \; t = 0 \wedge c \geq \; c_{min} \big) \\
& \qquad \cup \big(\dot{t} = 1, \dot{x} = v_o s, \dot{y} = v_o c \& \; c = c_{min} \big) \Big)^* \Big] \\
& \qquad \Big(\; \mid c(x_{obs} - x) - s(y_{obs} - y) \mid \; > \frac{W}{2} \\
& \qquad \vee \mid s(x_{obs} - x) + c(y_{obs} - y) - \frac{L}{2} \mid \; > \frac{L}{2} \Big)
\end{aligned}
\tag{13}
$$

Theorem 2: Implict-Explicit Safety Region Equivalence

$$
init \rightarrow \big(L_{impl} \;\; \leftrightarrow \;\; L_{expl} \big) \tag{14}
$$

Corollary 1: Verification for Collision Avoidance

$$
\begin{aligned}
& init \wedge L_{expl} \rightarrow \\
& \qquad \Big[\Big(\Big(\big(\dot{s} = c\frac{v_o}{R}, \dot{c} = -s\frac{V_o}{R}, \dot{x} = v_o s, \dot{y} = v_o c \\
& \qquad \& \; t = 0 \wedge c \geq \; c_{min} \big) \\
& \qquad \cup \big(\dot{t} = 1, \dot{x} = v_o s, \dot{y} = v_o c \& \; c = c_{min} \big) \Big)^* \Big] \\
& \qquad \Big(\; \mid c(x_{obs} - x) - s(y_{obs} - y) \mid \; > \frac{W}{2} \\
& \qquad \vee \mid s(x_{obs} - x) + c(y_{obs} - y) - \frac{L}{2} \mid \; > \frac{L}{2} \Big)
\end{aligned}
\tag{15}
$$

Both Theorem 1 and Theorem 2 have been formally verified in the theorem prover KeYmaera X.

D. Proof Strategy

The proof of **Theorem 2** (14) involves quantifier ($\forall$) elimination. This is done by substituting strategic values of the nominal coordinates in the expression L_{impl}. Since L_{impl} addresses all possible coordinates of the nominal trajectory, proving the equivalence between L_{impl} and L_{expl} amounts to smartly substituting values in the expression L_{impl}. This theorem is needed as an intermediate step. Proving the collision avoidance safety condition directly for the explicit region would be more complicated, and would equate to simulating the vehicle's overall kinematics for each and every possible position of an obstacle in this region, and then evaluating the correctness of the safety condition. This is problematic because (i) there is an infinite number of points in the explicit region; and (ii) to evaluate the safety condition this way requires the use of solution trajectories which involve undecidable algebra.

Techniques using hybrid automata [7] also prove safety properties for hybrid systems involving differential equations, but they require to first *obtain the solutions* of the differential equations. Such techniques cannot easily be used here as our turning kinematics have trigonometric solutions which are arithmetically undecidable. Instead, we utilize differential invariants [17], [19] of our vehicle's turning kinematics to prove the safety property.

In order to prove **Theorem 1** (13), we equivalently proof the following:

- The nominal trajectory T_{nom} (16) is a differential invariant of the vehicle dynamics. This means that if the vehicle starts from any point on T_{nom} and evolves through the dynamic equations for any non-negative time duration, then the vehicle can only end up at a point on T_{nom}. This is equivalent to saying that once the car gets on the nominal trajectory, it forever stays on it.

$$\begin{aligned} T_{nom} \equiv & \qquad\qquad\qquad\qquad\qquad\qquad\qquad (16)\\ & \Big(\big(t_n = 0 \ \wedge\ c_n \geq c_{min} \ \wedge\ s_n \geq 0 \ \wedge\ s_n^2 = 1 - c_n^2 \\ & \wedge\ x_n = -Rc_n \ \wedge\ y_n = Rs_n\big) \\ & \vee\ \big(t_n \geq 0 \ \wedge\ c_n = c_{min} \wedge\ s_n \geq 0 \\ & \wedge\ s_n^2 = 1 - c_n^2 \ \wedge\ x_n = -Rc_n + v_0 t_n s_n \\ & \wedge\ y_n = Rs_n + v_0 t_n c_n\big)\Big) \end{aligned}$$

  To prove that T_{nom} is a differential invariant of the vehicle dynamics, we observe that differentials of the relations that define T_{nom} (16), are all 0 along the direction of system of differential equations that govern the dynamics.
- The vehicle is on the nominal trajectory T_{nom} at $t = 0$. This fact is easily proved by evaluating the relations of T_{nom} at $t = 0$ and observing that the initial state of the vehicle satisfies those relations.
- If the vehicle is on the nominal trajectory T_{nom}, then it is not colliding with the obstacle. This fact easily follows from the definition of implicit safety region L_{impl}.

This completes the proof of **Theorem 1** (13). **Corollary 1** (15) follows from **Theorem 1** (13) and **Theorem 2** (14).

IV. RELATED WORK

Formal verification of collision avoidance has been of great interest to the formal methods community. Much of the past work has focused on airplane collision avoidance, but collision avoidance for robots has found new interest in recent years.

Regarding robot collision avoidance, S. Mitsch *et al.* [15] formally verify the collision avoidance for planar robots using non-linear dynamic program based modeling. Their collision model is based purely upon the center to center distance, essentially modeling a circular-shaped robot, without considering any realistic geometry for the robot's body. B. Martin *et al.* [14] formally verify station keeping maneuvers for a planar robot. They have used a non-linear hybrid program to model the overall dynamics and a differential-invariant-based approach for proving related safety properties. However they consider the robot's environment free of any obstacles, and do not analyze collision avoidance conditions.

Regarding aircraft collision avoidance, C. Tomlin *et al.* [23] formally verify conflict resolution maneuvers for aircraft, using an approach based upon automata-theoretic modal logic. A. Platzer and E. M. Clarke [20] formally verify collision avoidance maneuvers for aircraft. They analyze planar turning maneuvers but they don't consider any extended geometry for the aircraft, instead modeling collision purely on the basis of center to center distance. J.-B. Jeannin *et al.* [10] formally verify the ACAS X (Next-Generation Airborne Collision Avoidance System) industrial system developed by the Federal Aviation Administration (FAA). They determine and formally verify the geometric configurations of aircraft, under which the advice given by ACAS X is safe. They use a hybrid program and a safety-region-based approach for the task of formal verification, however the dynamic model considered is linear and does not consider rotations of the aircraft. G. Dowek *et al.* [3] provide a provably safe distributed conflict resolution strategy for aircraft, considering both horizontal and vertical maneuvers. Their dynamics model is similar to [10], and does not consider rotation of the safety buffer around the aircraft.

Regarding car collision avoidance, S. M. Loos *et al.* [13], and T. Sturm and A. Tiwari [22] formally verify the correctness of adaptive cruise control algorithms. However the dynamic motion of the car is constrained to a straight line in both of these works and does not include any turning maneuver.

Overall, our approach is different from previous related works in that:

- unlike [23], we base the model of our non-linear hybrid program on d$\mathscr{L}$ which is much more suitable for handling differential equations.
- unlike [13]–[15], [20], [22], we utilize a safety region based modeling technique for formally verifying the safety property of the hybrid program. This technique provides a superior and much faster on-line implementation for the task of vehicle guidance.
- unlike [10], we consider a non-linear hybrid program for the dynamics model which includes the effect of vehicle body rotation.
- unlike [10], [13], [15], [20], [22], our vehicle model is more realistic having an extended, rotating, rectangular geometric body.

V. CONCLUSIONS AND FUTURE WORKS

A. Conclusions

The current collision avoidance system guides the vehicle around a stationary obstacle with a formally verified swerving maneuver. This guidance system guarantees that the vehicle will not collide with any stationary obstacle as

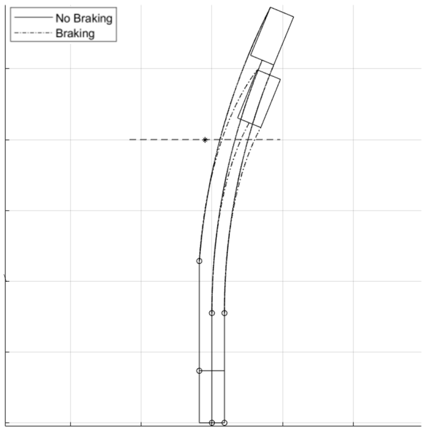

Fig. 11: Trajectory comparison

long as the system variables satisfy certain well defined conditions. These conditions come in the form of the explicit safety region L_{expl}. Hence, as long as at $t = 0$, the obstacle lies within the safety region of the advisory (R, θ^{max}), the vehicle is guaranteed to avoid it safely.

With the current result, given a geometric configuration for the vehicle and the static obstacle, we can obtain a set of provably correct swerving maneuvers of the form (R, θ^{max}). This set can then be further analyzed to obtain advisories which fulfill additional requirements, e.g., maintaining a minimum required safety distance from the obstacle, minimizing the extra control effort in avoiding collision, etc.

B. Ongoing and Future Work

The current work analyses and formally verifies a collision avoidance system which issues emergency maneuvers involving swerving. The effectiveness of such a collision avoidance system in robustly deterring any collision of the vehicle with the obstacle, depends upon the size of the safety region for the advised maneuver ((R, θ^{max}) in this work).

If we allow the vehicle speed v to be actively reduced by applying the brakes while swerving, the resulting trajectory can exhibit much sharper turns (Fig. 11). Hence, by turning and braking simultaneously, the vehicle can avoid obstacles which it would not have by swerving alone. In other words, we can increase the safety region of the system by issuing advisories of combined maneuvers of turning and braking.

In ongoing work [2], we are extending the scope of the current collision avoidance system, by analyzing simultaneous braking and swerving. The collision avoidance system presented in this paper can be seen as a special case of that more generalized version. By the addition of braking effect to the system, the resulting overall kinematics becomes more complicated, and the formal verification is more involved.

Acknowledgements

We wish to thank Nikos Aréchiga for helpful discussions. Toyota Research Institute ("TRI") provided funds to assist the authors with their research but this article solely reflects the opinions and conclusions of its authors and not TRI or any other Toyota entity.

References

[1] 2020 Toyota Corolla Interior: Exterior Dimensions, 2020. http://www.toyota.com/corolla/features/dimensions/1882/1863/1856. Retrieved March 19, 2020.

[2] A. Abhishek, H. Sood, and J.-B. Jeannin. Formal verification of braking while swerving in automobiles. In *Proceedings of the 23rd ACM International Conference on Hybrid Systems: Computation and Control*, 2020.

[3] G. Dowek, C. Munoz, and V. Carreño. Provably safe coordinated strategy for distributed conflict resolution. In *AIAA guidance, navigation, and control conference and exhibit*, page 6047, 2005.

[4] L. E. Dubins. On curves of minimal length with a constraint on average curvature, and with prescribed initial and terminal positions and tangents. *American Journal of mathematics*, 79(3):497–516, 1957.

[5] N. Fulton, S. Mitsch, J.-D. Quesel, M. Völp, and A. Platzer. KeYmaera X: An axiomatic tactical theorem prover for hybrid systems. In *International Conference on Automated Deduction*, pages 527–538. Springer, 2015.

[6] T. D. Gillespie. Fundamentals of vehicle dynamics. Technical report, SAE Technical Paper, 1992.

[7] T. A. Henzinger. The theory of hybrid automata. In *Verification of Digital and Hybrid Systems*, pages 265–292. Springer, 2000.

[8] M. Hoy, A. S. Matveev, and A. V. Savkin. Algorithms for collision-free navigation of mobile robots in complex cluttered environments: a survey. *Robotica*, 33(3):463–497, 2015.

[9] Y. K. Hwang and N. Ahuja. Gross motion planninga survey. *ACM Computing Surveys (CSUR)*, 24(3):219–291, 1992.

[10] J.-B. Jeannin, K. Ghorbal, Y. Kouskoulas, A. Schmidt, R. Gardner, S. Mitsch, and A. Platzer. A formally verified hybrid system for safe advisories in the next-generation airborne collision avoidance system. *International Journal on Software Tools for Technology Transfer*, 19(6):717–741, 2017.

[11] D. King-Hele. Erasmus Darwin's improved design for steering carriages—and cars. *Notes and records of the Royal Society of London*, 56(1):41–62, 2002.

[12] J.-P. Laumond et al. *Robot motion planning and control*, volume 229. Springer, 1998.

[13] S. M. Loos, A. Platzer, and L. Nistor. Adaptive cruise control: Hybrid, distributed, and now formally verified. In *International Symposium on Formal Methods*, pages 42–56. Springer, 2011.

[14] B. Martin, K. Ghorbal, E. Goubault, and S. Putot. Formal verification of station keeping maneuvers for a planar autonomous hybrid system. In *First Workshop on Formal Verification of Autonomous Vehicles (FVAV)*, pages 91–104.

[15] S. Mitsch, K. Ghorbal, D. Vogelbacher, and A. Platzer. Formal verification of obstacle avoidance and navigation of ground robots. *The International Journal of Robotics Research*, 36(12):1312–1340, 2017.

[16] A. Platzer. Differential dynamic logic for hybrid systems. *Journal of Automated Reasoning*, 41(2):143–189, 2008.

[17] A. Platzer. *Logical analysis of hybrid systems: proving theorems for complex dynamics*. Springer Science & Business Media, 2010.

[18] A. Platzer. Logics of dynamical systems. In *Proceedings of the 2012 27th Annual IEEE/ACM Symposium on Logic in Computer Science*, pages 13–24. IEEE Computer Society, 2012.

[19] A. Platzer. *Logical Foundations of Cyber-Physical Systems*. Springer, 2018.

[20] A. Platzer and E. M. Clarke. Formal verification of curved flight collision avoidance maneuvers: A case study. In *International Symposium on Formal Methods (FM)*, pages 547–562. Springer, 2009.

[21] R. Rajamani. *Vehicle dynamics and control*. Springer Science & Business Media, 2011.

[22] T. Sturm and A. Tiwari. Verification and synthesis using real quantifier elimination. In *Proceedings of the 36th international symposium on Symbolic and algebraic computation*, pages 329–336. ACM, 2011.

[23] C. Tomlin, G. J. Pappas, and S. Sastry. Conflict resolution for air traffic management: A study in multiagent hybrid systems. *IEEE Transactions on automatic control*, 43(4):509–521, 1998.

[24] S. Yang, Y. Lu, and S. Li. An overview on vehicle dynamics. *International Journal of Dynamics and Control*, 1(4):385–395, 2013.