Periodically Controlled Hybrid Systems
Verifying A Controller for An Autonomous Vehicle

Tichakorn Wongpiromsarn[1], Sayan Mitra[2],
Richard M. Murray[1], and Andrew Lamperski[1]

[1] California Institute of Technology
[2] University of Illinois at Urbana Champaign

Abstract. This paper introduces Periodically Controlled Hybrid Automata (PCHA) for describing a class of hybrid control systems. In a PCHA, control actions occur roughly periodically while internal and input actions, may occur in the interim changing the discrete-state or the setpoint. Based on periodicity and subtangential conditions, a new sufficient condition for verifying invariance of PCHAs is presented. This technique is used in verifying safety of the planner-controller subsystem of an autonomous ground vehicle, and in deriving geometric properties of planner generated paths that can be followed safely by the controller under environmental uncertainties.

1 Introduction

Alice, an autonomous vehicle built at Caltech, successfully accomplished two of the three tasks at the National Qualifying Event of the the 2007 DARPA Urban Challenge [4], [15], [5]. In executing the third task, which involved making left-turns while merging into traffic, its behavior was unsafe and almost led to a collision. Alice was stuck at the corner of a sharp turn dangerously stuttering in the middle of an intersection.

This behavior, it was later diagnosed, was caused by bad interactions between the *reactive obstacle avoidance subsystem (ROA)* and the relatively slowly reacting *path planner*. The planner incrementally generates a sequence of waypoints based on the road map, obstacles, and the mission goals. The ROA is designed to rapidly decelerate the vehicle when it gets too close to (possibly dynamic) obstacles or when the deviation from the planned path gets too large. Finally, for protecting the steering wheel, Alice's low-level controller limits the rate of steering at low speeds. Thus, accelerating from a low speed, if the planner produces a path with a sharp left turn, the controller is unable to execute the turn closely. Alice deviates from the path; the ROA activates and slows it down. This cycle continues leading to stuttering. For avoiding this behavior, the planner needs to be aware of the constraints imposed by the controller.

Finding this type of design bugs in hybrid control systems is important and challenging. While real world hybrid systems are large and complex, they are also engineered, and hence, have more structure than general hybrid automata [1].

Although restricted subclasses that are amenable to algorithmic analysis have been identified, such as rectangular-initialized [6], o-minimal [8], planar [14], and stormed [12] hybrid automata, they are not representative of restrictions that arise in engineered systems. With the motivation of abstractly capturing a common design pattern in hybrid control systems, such as Alice, and other motion control systems [11], in this paper, we study a new subclass of hybrid automata. Two main contributions of this paper are the following:

First, we define a class of hybrid control systems in which certain *control actions* occur roughly periodically. Each control action sets the *controlling input* to the plant or the physical process. In the interval between two consecutive control actions, the state of the system evolves continuously and discretely, but the control input remains constant. In particular, discrete state changes triggered by an external source may changes the waypoint or the set-point of the controller, which in turn may influence the computation of the next control input. For this class of *periodically controlled hybrid systems*, we present a sufficient condition for verifying invariant properties. The key requirement in applying this condition is to identify subset(s) C of the candidate invariant set $\mathcal{I}$, such that if the control action occurs when the system state is in C, then the subsequent control output guarantees that the system remains in $\mathcal{I}$ for the next period. The technique does not require one to solve the differential equations, instead, it relies on checking conditions on the periodicity and the subtangential condition at the boundary of $\mathcal{I}$. We are currently exploring the possibility of automating such checks using quantifier elimination [3] and optimization [13].

Secondly, we apply the above technique to verify a sequence of invariant properties of the planner-controller subsystems of Alice. From these invariants, we are able to deduce safety. That is, the deviation —distance of the vehicle from the planned path—remains within a certain constant bound. In the process, we also derive geometric properties of planner paths that guarantee that they can be followed safely by the vehicle.

The remainder of the paper is organized as follows: In Section 2 we briefly present the key definitions for the hybrid I/O automaton framework. In Section 3 we present PCHA and a sufficient condition for proving invariance. In Sections 4 and 5 we present the formal model and verification of Alice's Controller-Vehicle subsystem.

2 Preliminaries

We use the Hybrid Input/Output Automata (HIOA) framework of [9, 7] for modelling hybrid systems and the state model-based notations introduced in [10]. A Structured Hybrid I/O Automaton (SHIOA) is a non-deterministic state machine whose state may change instantaneously through a transition, or continuously over an interval of time following a *trajectory*.

A variable structure is used to specify the states of an SHIOA. Let V be a set of variables. Each variable $v \in V$ is associated with a *type* which defines the set of values v can take. The set of valuations of V is denoted by $val(V)$.

For a valuation $\mathbf{v} \in Val(V)$ of set of variables V, its restriction to a subset of variables $Z \subseteq V$ is denoted by $\mathbf{v} \lceil Z$. A variable may be *discrete* or *continuous*. Typically, discrete variables model protocol or software state, and continuous variables model physical quantities such as time, position, and velocity.

A *trajectory* for a set of variables V models continuous evolution of the values of the variables over an interval of time. Formally, a trajectory τ is a map from a left-closed interval of $\mathbb{R}_{\geq 0}$ with left endpoint 0 to $val(V)$. The domain of τ is denoted by $\tau.dom$. The *first state* of τ, $\tau.\mathsf{fstate}$, is $\tau(0)$. A trajectory τ is *closed* if $\tau.dom = [0, t]$ for some $t \in \mathbb{R}_{\geq 0}$, in which case we define $\tau.\mathsf{ltime} \triangleq t$ and $\tau.\mathsf{lstate} \triangleq \tau(t)$. For a trajectory τ for V, its restriction to a subset of variables $Z \subseteq V$ is denoted by $\tau \downarrow Z$.

For given sets of input U, output Y, and internal X variables, a *state model* $\mathcal{S}$ is a triple $(\mathscr{F}, Inv, Stop)$, where (a) $\mathscr{F}$ is a collection of Differential and Algebraic Inequalities (DAIs) involving the continuous variables in U, Y, and X, and (b) Inv and $Stop$ are predicates on X called *invariant condition* and *stopping condition* of $\mathcal{S}$. Components of $\mathcal{S}$ are denoted by $\mathscr{F}_{\mathcal{S}}$, $Inv_{\mathcal{S}}$ and $Stop_{\mathcal{S}}$. $\mathcal{S}$ defines a set of trajectories, denoted by $traj(\mathcal{S})$, for the set of variables $V = X \cup U \cup Y$. A trajectory τ for V is in the set $trajs(\mathcal{S})$ iff (a) the discrete variables in $X \cup Y$ remain constant over τ; (b) the restriction of τ on the continuous variables in $X \cup Y$ satisfies all the DAIs in $\mathscr{F}_{\mathcal{S}}$; (c) at every point in time $t \in dom(\tau)$, $(\tau \downarrow X)(t) \in Inv$; and (d) if $(\tau \downarrow X)(t) \in Stop$ for some $t \in dom(\tau)$, then τ is closed and $t = \tau.\mathsf{ltime}$.

Definition 1. *A* Structured Hybrid I/O Automaton (SHIOA) $\mathcal{A}$ *is a tuple* $(V, Q, Q_0, A, \mathcal{D}, \mathscr{S})$ *where*

(a) V *is a set of variables partitioned into sets of* internal X, output Y *and* input U *variables;*
(b) $Q \subseteq val(X)$ *is a set of* states *and* $Q_0 \subseteq Q$ *is a nonempty set of* start states*;*
(c) A *is a set of actions partitioned into sets of* internal H, output O *and* input I *actions;*
(d) $\mathcal{D} \subseteq Q \times A \times Q$ *is a set of* discrete transitions*; and*
(e) $\mathscr{S}$ *is a collection of* state models *for* U, Y, *and* X, *such that for every* $\mathcal{S}, \mathcal{S}' \in \mathscr{S}$, $Inv_{\mathcal{S}} \cap Inv_{\mathcal{S}'} = \emptyset$ *and* $Q \subseteq \bigcup_{\mathcal{S} \in \mathscr{S}} Inv_{\mathcal{S}}$.

In addition, $\mathcal{A}$ *satisfies the following axioms:*

E1 *Every input action is enabled at every state.*
E2 *Given any trajectory* υ *of the input variables* U, *any* $\mathcal{S} \in \mathscr{S}$, *and* $\mathbf{x} \in Inv_{\mathcal{S}}$, *there exists* $\tau \in trajs(\mathcal{S})$ *starting from* $\mathbf{x}$, *such that either (a)* $\tau \downarrow U = \upsilon$, *or (b)* $\tau \downarrow U$ *is a proper prefix of* υ *and some action in* $H \cup O$ *is enabled at* $\tau.lstate$.

E1 is the standard action nonblocking axiom of I/O automata. **E2** is a nonblocking axiom for individual state models: given any trajectory υ of the input variables and any state model, either time can elapse for the entire duration of υ, or time elapses to a point at which some local action of $\mathcal{A}$ is enabled.

A transition $(\mathbf{x}, a, \mathbf{x}') \in \mathcal{D}$ is written in short as $\mathbf{x} \xrightarrow{a}_{\mathcal{A}} \mathbf{x}'$ or as $\mathbf{x} \xrightarrow{a} \mathbf{x}'$ when $\mathcal{A}$ is clear from the context. An action a is said to *enabled* at $\mathbf{x}$ if there exists $\mathbf{x}'$ such that $\mathbf{x} \xrightarrow{a} \mathbf{x}'$. We denote the components of a SHIOA $\mathcal{A}$ by $X_{\mathcal{A}}, Y_{\mathcal{A}}$ etc. For a set of state variables X, a state $\mathbf{x}$ is an element of $Val(X)$. We denote the valuation of a variable $y \in X$ at state $\mathbf{x}$, by the usual (.) notation $\mathbf{x}.y$.

An execution of $\mathcal{A}$ records the valuations of all its variables and the occurrences of all actions over a particular run. An execution is *closed* if it is finite and the last trajectory in it is closed.

An *execution fragment* of $\mathcal{A}$ is a finite or infinite sequence $\alpha = \tau_0 a_1 \tau_1 a_2 \ldots$, such that for all i in the sequence, $a_i \in A$, $\tau \in trajs(\mathcal{S})$ for some $\mathcal{S} \in \mathscr{S}$, and $\tau_i.\mathsf{lstate} \xrightarrow{a_{i+1}} \tau_{i+1}.\mathsf{fstate}$. An execution fragment is an *execution* if $\tau_0.\mathsf{fstate} \in Q_0$. The first state of α, $\alpha.\mathsf{fstate}$, is $\tau_0.\mathsf{fstate}$, and for a closed α, its last state, $\alpha.\mathsf{lstate}$, is the last state of its last trajectory. The *limit time* of α, $\alpha.\mathsf{ltime}$, is defined to be $\sum_i \tau_i.\mathsf{ltime}$. The set of executions and reachable states of $\mathcal{A}$ are denoted by $\mathsf{Execs}_{\mathcal{A}}$ and $\mathsf{Reach}_{\mathcal{A}}$. A set of states $I \subseteq Q$ is said to be an *invariant* of $\mathcal{A}$ iff $\mathsf{Reach}_{\mathcal{A}} \subseteq I$.

3 Periodically Controlled Hybrid Systems

In this section, we define a subclass of SHIOAs frequently encountered in applications involving sampled control systems and embedded systems with periodic sensing and actuation. The main result of this section, Theorem 1, gives a sufficient condition for proving invariant properties of this subclass.

3.1 Periodically Controlled Hybrid I/O Automata

A *Periodically Controlled Hybrid Automaton (PCHA)* is an SHIOA with a set of (control) actions which occur roughly periodically. The execution of such a control action may change the continuous and the discrete state variables. For the sake of simplicity, we consider the PCHAs of the form shown in Figure 1, however, Theorem 1 generalizes to PCHAs with other input, output, and internal actions.

Let $\mathcal{X} \subseteq \mathbb{R}^n$, for some $n \in \mathbb{N}$, and $\mathcal{L}, \mathcal{Z}$, and $\mathcal{U}$ be arbitrary types. Four key variables of PCHA $\mathcal{A}$ are (a) *continuous state* variable s of type $\mathcal{X}$, initialized to x_0, (b) discrete state (*location* or *mode*) variable *loc* of type $\mathcal{L}$, initialized to l_0, (c) *command* variable z of type $\mathcal{Z}$, initialized to z_0, and (d) *control* variable u of type $\mathcal{U}$, initialized to u_0. The *now* and *next* variables are used for triggering the control action periodically. The type $\mathcal{X} \subseteq \mathbb{R}^n$, for some $n \in \mathbb{N}$, the types $\mathcal{L}, \mathcal{Z}$, and $\mathcal{U}$ are arbitrary.

PCHA $\mathcal{A}$ has two types of actions: (a) through input action update $\mathcal{A}$ learns about new externally produced input commands such as set-points, waypoints. When an update(z') action occurs, z' is recorded in the command variable z. (b) The control action changes the control variable u. This action occurs roughly periodically starting from time 0; the time gap between two successive occurrences is within $[\Delta_1, \Delta_1 + \Delta_2]$ where $\Delta_1 > 0, \Delta_2 \geq 0$. When control occurs, *loc*

and s are computed as a function of their current values and that of z, and u is computed as a function of the new values of loc and s.

For each value of $l \in \mathcal{L}$, the continuous state s evolves according to the trajectories specified by state model $smodel(l)$. That is, s evolves according to the differential equation $\dot{s} = f_l(s, u)$. The timing of control behavior is enforced by the precondition of control and the stopping condition of the state models.

```
signature
  internal control
  input update(z' : Z)

variables
  internal s : X := x_0
  internal discrete loc : L := l_0,
    z : Z := z_0, u : U := u_0
  internal now : R_≥0 := 0,
    next : R_≥0 := −Δ_2

transitions
  input update(z')
  eff z := z'

  internal control
  pre now ≥ next
  eff next := now + Δ_1
    ⟨loc, s⟩ := h(loc, s, z); u := g(loc, s)

trajectories
  trajdef smodel(l : L)
    invariant loc = l
    evolve d(now) = 1; d(s) = f_l(s, u)
    stop when now = next + Δ_2
```

Fig. 1. PHCA with parameters Δ_1, Δ_2, g, h, $\{f_l\}_{l \in \mathcal{L}}$. See, for example, [10] for the description of the language.

3.2 Describing and Proving Invariants

Given a candidate invariant set $\mathcal{I} \subseteq Q$, we are interested in verifying that $\mathsf{Reach}_A \subseteq \mathcal{I}$. For continuous dynamical systems, checking the well-known subtangential condition (see, for example [2]) provides a sufficient condition for proving invariance of a set $\mathcal{I}$ that is bounded by a closed surface. Theorem 1 provides an analogous sufficient condition for PCHAs. In general, however, invariant sets $\mathcal{I}$ for PCHAs have to be defined by a collection of functions instead of a single function. For each mode $l \in \mathcal{L}$, we assume that the invariant set $I_l \subseteq \mathcal{X}$ for the continuous state is defined by a collection of m *boundary functions* $\{F_{lk}\}_{k=1}^{m}$, where m is some natural number and each $F_{lk} : \mathcal{X} \to \mathbb{R}$ is a differentiable function[1]. Formally,

$$I_l \triangleq \{x \in \mathcal{X} \mid \forall k \in \{1, \ldots, m\}, F_{lk}(x) \geq 0\} \text{ and } \mathcal{I} \triangleq \{\mathbf{x} \in Q \mid \mathbf{x}.s \in I_{\mathbf{x}.loc}\}.$$

Note that $\mathcal{I}$ does not restrict the values of the command or the control variables. Lemma 1 modifies the standard inductive technique for proving invariance, so that it suffices to check invariance with respect to Control transitions and Control-free execution fragments.

[1] Identical size m of the collections simplifies our notation; different number of boundary functions for different values of l can be handled by extending the theorem in an obvious way.

Lemma 1. *Suppose $Q_0 \subseteq \mathcal{I}$ and the following two conditions hold:*

(a) (Control steps) For each state $\mathbf{x}, \mathbf{x}' \in Q$, if $\mathbf{x} \overset{\mathsf{control}}{\rightarrow} \mathbf{x}'$ and $\mathbf{x} \in \mathcal{I}$ then $\mathbf{x}' \in \mathcal{I}$,
(b) (Control-free fragments) For each closed execution fragment $\beta = \tau_0\ \mathsf{update}(z_1)\ \tau_1\ \mathsf{update}(z_2)\ \ldots\ \tau_n$ starting from a state $\mathbf{x} \in \mathcal{I}$ where each $z_i \in \mathcal{Z}$, if $\mathbf{x}.next - \mathbf{x}.now = \Delta_1$ and $\beta.\mathsf{ltime} \leq \Delta_1 + \Delta_2$, then $\beta.\mathsf{lstate} \in \mathcal{I}$.

Then $\mathsf{Reach}_{\mathcal{A}} \subseteq \mathcal{I}$.

Proof. Consider any reachable state $\mathbf{x}$ of $\mathcal{A}$ and any execution α such that $\alpha.\mathsf{lstate} = \mathbf{x}$. We can write α as $\beta_0\ \mathsf{control}\ \beta_1\ \mathsf{control}\ \ldots \beta_k$, where each β_i is $\mathsf{control}$-free execution fragment of $\mathcal{A}$, i.e., execution fragments in which only update actions occur. From condition (a), it follows that for each $i \in \{0, \ldots, k\}$, if $\beta_i.\mathsf{lstate} \in \mathcal{I}$, then $\beta_{i+1}.\mathsf{fstate} \in \mathcal{I}$.

Thus, it suffices to prove that for each $i \in \{0, \ldots, k\}$, if $\beta_i.\mathsf{fstate} \in \mathcal{I}$, then $\beta_i.\mathsf{lstate} \in \mathcal{I}$. We fix an $i \in \{0, \ldots, k\}$ and assume that $\beta_i.\mathsf{fstate} \in \mathcal{I}$. Let $\beta_i = \tau_0\ \mathsf{update}(z_1)\ \tau_1 \mathsf{update}(z_2) \ldots \tau_n$, where for $j \in \{0, \ldots, n\}$, $z_j \in \mathcal{Z}$ and τ_j is a trajectory of $\mathcal{A}$. If $i = 0$, then $\beta_i.\mathsf{ltime} = 0$ and $\beta_i.\mathsf{lstate} \lceil \{loc, s\} = \beta_i.\mathsf{fstate} \lceil \{loc, s\}$ since the first $\mathsf{control}$ action occurs at time 0 and update transitions do not affect the value of loc and s. Therefore, $\beta_i.\mathsf{lstate} \in \mathcal{I}$. Otherwise, $i > 0$ and since β_i starts immediately after a $\mathsf{control}$ action $\beta.\mathsf{fstate} \lceil next - \beta.\mathsf{fstate} \lceil now = \Delta_1$. From periodicity of main actions, we know that $\beta_i.\mathsf{ltime} \leq \Delta_1 + \Delta_2$, and hence from condition (b) it follows that $\beta_i.\mathsf{lstate} \in \mathcal{I}$.

The next key lemma provides a sufficient condition for proving invariance of control-free fragments. Since, control-free fragments do not change the valuation of the loc variable, for this part, we fix a value $l \in \mathcal{L}$. For each $j \in \{1, \ldots m\}$, we define the set ∂I_j to be part of the set I_l where the function F_{lj} vanishes. That is, $\partial I_j \triangleq \{x \in \mathcal{X} \mid F_{lj}(x) = 0\}$. In this paper, we call ∂I_j the jth boundary of I_l even though strictly speaking, the jth boundary of I_l is only a subset of ∂I_j according on the standard topological definition. Similarly, we say that the *boundary* of I_l, is $\partial I_l = \bigcup_{j \in \{1, \ldots, m\}} \partial I_j$.

Lemma 2. *Suppose that there exists a collection $\{C_j\}_{j=1}^m$ of subsets of I_l such that the following conditions hold:*

(a) (Subtangential) For each $s_0 \in I_l \setminus C_j$ and $s \in \partial I_j$, $\frac{\partial F_{lj}(s)}{\partial s} \cdot f_l(s, g(l, s_0)) \geq 0$.
(b) (Bounded distance) $\exists\ c_j > 0$ such that $\forall\ s_0 \in C_j, s \in \partial I_j$, $||s - s_0|| \geq c_j$.
(c) (Bounded speed) $\exists\ b_j > 0$ such that $\forall\ s_0 \in C_j, s \in I_l$, $||f_l(s, g(l, s_0))|| \leq b_j$,
(d) (Fast sampling) $\Delta_1 + \Delta_2 \leq \min_{j \in \{1, \ldots, m\}} \frac{c_j}{b_j}$.

Then, any $\mathsf{control}$-free execution fragment starting from a state in I_l where $next - now = \Delta_1$, remains within I_l.

Condition (a) requires that if the control variable u is evaluated when the continuous variable s is outside of the set C_j, then on the jth boundary, the vector-field governing the evolution of the continuous variable s is pointing inwards with respect to the jth boundary. Condition (b) requires that there is a

minimum sepatration c_j between C_j and the jth boundary of I_l. Condition (c) requires that the continuous state s evolves at a bounded speed b_j if the control variable u is evaluated when the continuous state s is within the set C_j. And finally, (d) requires that the minimum ratio c_j/b_j, over all j's is greater than the maximum periodicity $\Delta_1 + \Delta_2$ of the control action. A graphical explanation of this lemma is provided in Figure 2.

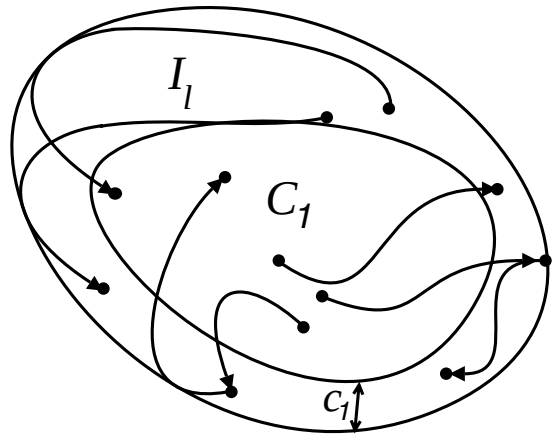


Fig. 2. A graphical explanation of Lemma 2 showing the sets I_l and $\{C_j\}_{j=1}^m$. Here $m = 1$, so the boundary of I_l is a subset of ∂I_1. The control and control-free fragments are shown by bullets and lines. Observe that a fragment starting in $\mathcal{I}$ and leaving $\mathcal{I}$ must cross ∂I_1. Condition (a) guarantees that if u is evaluated outside C_1, then the fragment does not leave I_l because when it reaches ∂I_1, the vector field governing its evolution points inwards with respect to ∂I_1. For a fragment starting inside C_1, condition (b) and (c) guarantee that it takes finite time before it reaches ∂I_1 and condition (d) guarantees that this finite time is at least $\Delta_1 + \Delta_2$; thus, before the trajectory crosses ∂I_1, u is evaluated again.

Proof. We fix a control-free execution fragment $\beta = \tau_0 \mathsf{update}(z_1)\tau_1 \mathsf{update}(z_2) \ldots \tau_n$ such that at $\beta.\mathsf{fstate}$, $next - now = \Delta_1$. Without loss of generality we assume that at $\beta.\mathsf{fstate}$, $z = z_1$, $loc = l$, and $s = x_1$, where $z_1 \in \mathcal{Z}, l \in \mathcal{L}$ and $x_1 \in I_l$. We have to show that at $\beta.\mathsf{lstate}$, $s \in I_l$.

First, observe that for each $k \in \{0, \ldots, n\}$, $(\tau_k \downarrow s)$ is a solution of the differential equation(s) $d(s) = f_l(s, g(l, x_1))$. Let τ be the pasted trajectory $\tau_0 \frown \tau_1 \frown \ldots \tau_n$.[2] Let $\tau.\mathsf{ltime}$ be T. Since the update action does not change s, $\tau_k.\mathsf{lstate} \lceil s = \tau_{k+1}.\mathsf{fstate} \lceil s$ for each $k \in \{0, \ldots, n-1\}$. As the differential equations are time invariant, $(\tau \downarrow s)$ is a solution of $d(s) = f_l(s, g(l, x_1))$. We define the function $\gamma : [0, T] \to \mathcal{X}$ as $\forall\, t \in [0, T]$, $\gamma(t) \triangleq (\tau \downarrow s)(t)$. We have to show that $\gamma(T) \in I_l$. Suppose, for the sake of contradiction, that there exists $t^* \in [0, T]$, such that

[2] $\tau_1 \frown \tau_2$ is the trajectory obtained by concatenating τ_2 at the end of τ_1.

$\gamma(t^*) \notin I_l$. By the definition of I_l, there exists i such that $F_{li}(\gamma(0)) \geq 0$ and $F_{li}(\gamma(t^*)) < 0$. We pick one such i and fix it for the remainder of the proof. Since F_{li} and γ are continuous, from intermediate value theorem, we know that there exists a time t_1 before t^* where F_{li} vanishes and that there is some finite time $\epsilon > 0$ after t_1 when F_{li} is strictly negative. Formally, there exists $t_1 \in [0, t^*)$ and $\epsilon > 0$ such that for all $t \in [0, t_1]$, $F_{li}(\gamma(t)) \geq 0$ and $F_{li}(\gamma(t_1)) = 0$ and for all $\delta \in (0, \epsilon]$, $F_{li}(\gamma(t_1 + \delta)) < 0$.

Case 1: $x_1 \in I_l \setminus C_i$. Since $F_{li}(\gamma(t_1)) = 0$, by definition, $\gamma(t_1) \in \partial I_i$. But from the value of $F_{li}(\gamma(t))$ where t is near to t_1, we get that $\frac{\partial F_{li}}{\partial t}(t_1) = \frac{\partial F_{li}}{\partial s}(\gamma(t_1)) \cdot f_l(\gamma(t_1), g(l, x_1)) < 0$. This contradicts condition (a).

Case 2: $x_1 \in C_i$. Since for all $t \in [0, t_1]$, $F_{li}(\gamma(t)) \geq 0$ and $F_{li}(\gamma(t_1)) = 0$, we get that for all $t \in [0, t_1]$, $\gamma(t) \in I_l$ and $\gamma(t_1) \in \partial I_i$. So from condition (b) and (c), we get $c_i \leq \|\gamma(t_1) - x_1\| = \left\| \int_0^{t_1} f_l(\gamma(t), g(l, x_1)) dt \right\| \leq b_i t_1$. That is, $t_1 \geq \frac{c_i}{b_i}$. But we know that $t_1 < t^* \leq T$ and periodicity of Control actions $T \leq \Delta_1 + \Delta_2$. Combining these, we get $\Delta_1 + \Delta_2 > \frac{c_i}{b_i}$ which contradicts condition (d). ■

For PCHAs with certain properties, the following lemma provides sufficient conditions for the existence of the bounds b_j and c_j which satisfy the bounded distance and bounded speed conditions of Lemma 2.

Lemma 3. *For a given $l \in L$, let $U_l = \{g(l, s) \mid l \in \mathcal{L}, s \in I_l\} \subseteq \mathcal{U}$ and suppose I_l is compact and f_l is continuous in $I_l \times U_l$. The bounded distance and bounded speed conditions (of Lemma 2) are satisfied if $C_j \subset I_l$ satisfies the following conditions:*

$$C_j \text{ is closed} \tag{1}$$

$$C_j \cap \partial I_j = \emptyset \tag{2}$$

Proof. From the continuity of F_{lj}, we can assume, without loss of generality, that $\partial I_j \neq \emptyset$. This is because if $\partial I_j = \emptyset$, then for all $s \in \mathcal{X}$, it must be either $F_{lj}(s) > 0$ or $F_{lj}(s) < 0$, that is, F_{lj} is not needed to describe I_l. In addition, the case where $C_j = \emptyset$ is trivial since conditions (b) and (c) of Lemma 2 are satisfied for any arbitrary large c_j and arbitrary small b_j. So for the rest of the proof, we assume that $\partial I_j \neq \emptyset$ and $C_j \neq \emptyset$. Since I_l is compact and C_j and ∂I_j are closed, C_j and ∂I_j are also compact. Consider a function $G_j : \partial I_j \to \mathbb{R}$ defined by

$$G_j(s) = \min_{s_0 \in C_j} \|s - s_0\|$$

where $\|\cdot\|$ is a norm on $\mathbb{R}^n$. Due to the continuity of $\|\cdot\|$ and the compactness and nonemptyness of C_j, G_j is continuous and since $C_j \cap \partial I_j = \emptyset$, we get that for all $s \in \partial I_j, G_j(s) > 0$. Since ∂I_j is compact and nonempty, G_j attains its minimum in ∂I_j. So there exists $c_j > 0$ such that $\min_{s \in \partial I_j} G_j(s) \geq c_j$.

Next, consider a function $H_j : I_l \to \mathbb{R}$ defined by

$$H_j(s) = \max_{s_0 \in C_j} \|f_l(s, g(l, s_0))\|.$$

Using the continuity of f_l, the compactness and nonemptyness of C_j and I_l and the same argument as above, we can conclude that there exists $b_j \geq 0$ such that $\max_{s \in I_l} H_j(s) \leq b_j$. ■

Theorem 1 combines the above lemmas and provides sufficient conditions for invariance of $\mathcal{I}$.

Theorem 1. *Consider a* PCHA $\mathcal{A}$ *and a set* $\mathcal{I} \subseteq Q_{\mathcal{A}}$. *Suppose* $Q_{0\mathcal{A}} \subseteq \mathcal{I}$, $\mathcal{A}$ *satisfies control invariance condition of Lemma 1, and conditions (a)-(d) of Lemma 2 for each* $l \in \mathcal{L}_{\mathcal{A}}$. *Then* $\mathsf{Reach}_{\mathcal{A}} \subseteq \mathcal{I}$.

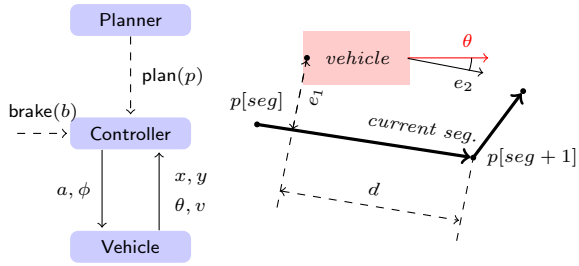
Proof. The proof follows directly from Lemma 1 and Lemma 2 since if conditions (a)-(d) of Lemma 2 are satisfied for any $l \in \mathcal{L}$, then condition (b) of Lemma 1 is satisfied. ■

Although the PCHA of Figure 1 has one action of each type, Theorem 1 can be extended for periodically controlled hybrid systems with arbitrary number of input and internal actions. Given the sets I_l and a semi-algebraic subset C_j, checking condition (a) and finding the c_j and b_j which satisfy conditions (b) and (c) can be formulated as a sum-of-squares optimization problem (provided that C_j and $I_l \setminus C_j$ are basic semi-algebraic sets) or proving emptiness of some certain semi-algebraic sets for PCHAs with polynomial vector-fields. We are currently exploring the possibility of automatically checking these conditions using SOSTOOLS [13] and QEPCAD [3].

4 System Model

In this section, we describe a subsystem of an autonomous ground vehicle (Alice) consisting of the physical vehicle and the controller (see, Figure 3(a)). Vehicle captures its the position, orientation, and the velocity of the vehicle on the plane. Controller receives information about the state of the vehicle and periodically computes the input steering (ϕ) and the acceleration (a). Controller also receives an infinite[3] sequence of waypoints from a Planner and its objective is to compute a and ϕ such that the vehicle (a) remains within a certain bounded distance e_{max} of the planned path, and (b) makes progress towards successive waypoints at a target speed. Property (a) together with the assumption (possibly guaranteed by Planner) that all planned paths are at least e_{max} distance away from obstacles, imply that the Vehicle does not collide with obstacles. While the Vehicle makes progress towards a certain waypoint, the subsequent waypoints may change owing to the discovery of new obstacles, short-cuts, and changes in the mission plan. Finally, the Controller may receive an externally triggered brake input, to which it must react by slowing the vehicle down.

[3] The verification technique can be extended in an obvious way to handle the case where the vehicle has to follow a finite sequence of waypoints and halt at the end.




```
variables
output x:ℝ:= x0; y:ℝ:= y0;                                  2
  θ:ℝ:= θ0; v:ℝ:= v0
input a, φ: ℝ                                               4

trajectories                                                6
evolve d(x) = v cos(θ)
  d(y) = v sin(θ)                                           8
  if |u.φ| ≤ φmax
    then d(θ) = v/L tan(φ)                                  10
    else d(θ) = v/L tan(φ/|φ| φmax) fi
  if v > 0 ∨ a ≥ 0                                          12
    then d(v) = a
    else d(v) = 0  fi                                       14
```

Fig. 3. (a) Planner-Controller system. (b) Deviation & disorientation. (c) Vehicle.

4.1 Vehicle

The Vehicle automaton of Figure 3 specifies the dynamics of the autonomous ground vehicle with acceleration (a) and steering angle (ϕ) as inputs. It has two parameters: (a) $\phi_{max} \in (0, \frac{\pi}{2}]$ is the physical limit on the steering angle, and (b) L is the wheelbase. The main output variables of Vehicle are (a) x and y coordinates of the vehicle with respect to a global coordinate system, (b) orientation θ of the vehicle with respect to the positive direction of the x axis, and (c) vehicle's velocity v. These variables evolve according to the differential equations of lines 7–14. Two aspects of this Vehicle model are noteworthy: (i) In determining the orientation of the vehicle, if the input steering angle ϕ is greater than the maximum limit ϕ_{max} then the maximum steering in the correct direction is applied. (ii) The acceleration can be negative only if the velocity is positive, and therefore the vehicle cannot move backwards. This vehicle model does require bounds on minimum and maximum acceleration, however, the controller ensures that the input acceleration is always within such a bound.

4.2 Controller

Figure 4 shows the SHIOA specification of the Controller automaton which reads the state of the Vehicle periodically and issues acceleration and steering outputs to achieve the aforementioned goals.

Controller is parameterized by: (a) the sampling period $\Delta \in \mathbb{R}_+$, (b) the target speed $v_T \in \mathbb{R}_{\geq 0}$, (c) proportional control gains $k_1, k_2 > 0$, (d) a constant $\delta > 0$ relating the maximum steering angle and the speed, (e) maximum and braking accelerations $a_{max} > 0$ and $a_{brake} < 0$. Restricting the maximum steering angle instead of the maximum steering rate is a simplifying but conservative assumption. Given a constant relating the maximum steering rate and the speed, there exists δ as defined above which guarantees that the maximum steering rate requirement is satisfied.

A *path* is an infinite sequence of points $p_1, p_2, \ldots$ where $p_i \in \mathbb{R}^2$, for each i. The main state variables of Controller are the following: (a) *brake* and *new_path*

are command variables which store the information received through the most recent brake (On or Off) and plan (a path) actions. (b) *path* is the current path being followed by Controller, (c) *seg* is the index of the last waypoint visited in the current *path*. That is, $seg + 1$ is the index of the current waypoint. The straight line joining $path[seg]$ and $path[seg + 1]$ is called the *current segment*. (d) *deviation* e_1 is the signed perpendicular distance from the current position of the vehicle to the current segment (see, Figure 3(b)). (e) *disorientation* e_2 is the difference between the current orientation of the vehicle (θ) and the angle of the current segment. (f) *waypoint-distance* d is the signed distance of the vehicle to the current waypoint measured parallel to the current segment.

signature
  input plan(p:Seq[$\mathbb{R}^]$); brake($b : On, Off$)
  internal main

variables
  input x, y, θ, v: $\mathbb{R}$
  output a, ϕ: $\mathbb{R} := (0, 0)$
  internal $brake$: $\{On, Off\} := Off$
    $path$: Seq[$\mathbb{R}^2$] := $arbitrary$
    new_path: Seq[$\mathbb{R}^2$] := $path$
    seg: $\mathbb{N} := 1$
    $e_1, e_2, d : \mathbb{R} := [e_{1,0}, e_{2,0}, d_0]$
    now: $\mathbb{R} := 0$; $next$:$\mathbb{R}_{\geq 0} := 0$

transitions
  input plan(p)
  eff $new_path := p$

  input brake(b)
  eff $brake := b$

  internal main
  pre $now = next$
  eff $next := now + \Delta$
  if $path \neq new_path \vee d \leq 0$ **then**
    if $path \neq new_path$
      then $seg := 1$; $path := new_path$
    elseif $d \leq 0$
      then $seg := seg + 1$ **fi**

    let $\boldsymbol{p} = \begin{bmatrix} path[seg+1].x - path[seg].x \\ path[seg+1].y - path[seg].y \end{bmatrix}$

    $\boldsymbol{q} = \begin{bmatrix} path[seg+1].y - path[seg].y \\ -(path[seg+1].x - p[seg].x) \end{bmatrix}$

    $\boldsymbol{r} = \begin{bmatrix} path[seg+1].x - x \\ path[seg+1].y - y) \end{bmatrix}$

    $e_1 := \frac{1}{\|\boldsymbol{q}\|} \boldsymbol{q} \cdot \boldsymbol{r}$
    $e_2 := \theta - \angle \boldsymbol{p}$
    $d := \frac{1}{\|\boldsymbol{p}\|} \boldsymbol{p} \cdot \boldsymbol{r}$
  fi

  let $\phi_d = -k_1\ e_1 - k_2\ e_2$
  $\phi = \frac{\phi_d}{|\phi_d|} \min(\delta \times v, |\phi_d|)$

  if $brake = On$ **then** $a := a_{brake}$
  elseif $brake = Off \wedge v < v_T$
    then $a := a_{max}$
  else $a := 0$ **fi**

trajectories
  $d(now) = 1$
  $d(e_1) = v \sin(e_2)$
  $d(e_2) = \frac{v}{L} \tan(\phi)$
  $d(d) = -v \cos(e_2)$
  stop when $now = next$

Fig. 4. Controller with parameters $v_T, k_1, k_2 \in \mathbb{R}_{\geq 0}$, $\delta, \Delta \in \mathbb{R}_+$ and $a_{brake} < 0$.

The brake(b) action is an externally controlled input action which informs the Controller about the application of an external brake ($b = On$) or the removal of the brake ($b = Off$). When brake(b) occurs, b is recorded in the command variable *brake*. The plan(p) action is controlled by the external Planner (not presented in this paper) and it informs the Controller about a newly planned path p. When this action occurs, the path p is recorded in the variable *new_path*. The main action occurs once every Δ time starting from time 0. This action updates the values of the variables e_1, e_2, d, *path*, *seg*, a and ϕ as follows:

A. If *new_path* (obtained from the planner) is different from *path* then *seg* is set to 1 and *path* is set to *new_path*.
B. If *new_path* is the same as *path* and the waypoint-distance d is less than or equal to 0, then *seg* is set to $seg + 1$ (line 29). For both of the above cases several temporary variables are computed which are in turn used to update e_1, e_2, d as specified in Lines 33-35; otherwise these variables remain unchanged.
C. The steering output to the vehicle ϕ is computed using proportional control law and it is restricted to be at most δ times the velocity of the vehicle. This constraint is enforced for the mechanical protection of the steering. The steering output ϕ is set to the minimum of $-k_1e_1 - k_2e_2$ and $v \times \delta$ (line 39).
D. The acceleration output a is computed using bang bang control law. If *brake* is *On* then a is set to the braking deceleration a_{brake}; otherwise, it executes a_{max} until the vehicle reaches the target speed, at which point a is set to 0.

Along a trajectory, the evolution of the variables are specified by the differential equations on lines 50-51. These differential equations are derived from the update rules described above and the differential equations governing the evolution of x, y, θ and v.

Complete System Let $\mathcal{A}$ be the composition of the Controller and the Vehicle automata. The continuous state of $\mathcal{A}$ is defined by the valuations of $x, y, \theta, v, e_1, e_2$, and d of Vehicle and Controller. For convenience, we define a single derived variable s of type $\mathcal{X} = \mathbb{R}^7$ encapsulating all these variables. The discrete state of $\mathcal{A}$ is defined by the valuations of $brake, path$ and seg of Controller. A derived variable loc of type $\mathcal{L} = \texttt{Tuple}[\{On, Off\}, \texttt{Seq}[\mathbb{R}^2], \mathbb{N}]$ is defined encapsulating all these variables. It can be checked easily that the composed automaton $\mathcal{A}$ is a PCHA. Appendix A describes the variables, actions, state transition functions of the corresponding PCHA.

5 Analysis of the System

Overview. The informally stated goals of the system translate to the following subgoals:

A. (*safety*) At all reachable states of $\mathcal{A}$, the deviation (e_1) of the vehicle is upper-bounded by e_{max}, where e_{max} is determined in terms of system parameters.
B. (*segment progress*) There exist certain threshold values of deviation, disorientation, and waypoint-distance such that from any state $\mathbf{x}$ with greater deviation, disorientation and waypoint-distance, the vehicle reduces its deviation and disorientation with respect to the current segment, while making progress towards its current waypoint.
C. (*waypoint progress*) The vehicle reaches successive waypoints.

First, in Sections 5.1 and 5.2, we define a family $\{\mathcal{I}_k\}_{k\in\mathbb{N}}$ of subsets of $Q_{\mathcal{A}}$ and using Lemma 2 we conclude that they are invariant with respect to the control-free execution fragments of $\mathcal{A}$. From the specification of main action, we see that

the continuous state changes only occur if $path \neq new_path$ or waypoint-distance $d \leq 0$. Hence, using Theorem 1, we conclude that any execution fragment starting in $\mathcal{I}_k$ remains within $\mathcal{I}_k$, provided that path and current segment do not change.

In Section 5.3, we establish the segment progress property (B). Finally, in Section 5.4, we prove an invariance of $\mathcal{I}_k$, for a chosen k, and derive geometric properties of planner paths that can be followed by $\mathcal{A}$ safely. These geometric properties specify the minimum length of a path segment and the relationship between the segment length and the maximum difference between consecutive segment orientations and are derived from the segment progress property. An invariance of $\mathcal{I}_k$ provides a proof certificate that $\mathcal{A}$ satisfies the safety property (A) and the waypoint progress property (C).

5.1 Family of Invariants

We define, for each $k \in \mathbb{N}$, the set $\mathcal{I}_k$ which bounds the deviation of the vehicle e_1 to be within $[-\epsilon_k, \epsilon_k]$. This bound on deviation alone, of course, does not give us an inductive invariant. If the deviation is ϵ_k and the vehicle is highly disoriented, then it would violate $\mathcal{I}_k$. Thus, $\mathcal{I}_k$ also bounds the disorientation such that the steering angle computed based on the proportional control law is within $[-\phi_k, \phi_k]$. To prevent the vehicle from not being able to turn at low speed and to guarantee that the execution speed of the controller is fast enough with respect to the speed of the vehicle, $\mathcal{I}_k$ also bounds the speed of the vehicle. $\mathcal{I}_k$ is defined in terms of $\epsilon_k, \phi_k \geq 0$ as $\mathcal{I}_k \triangleq \{\mathbf{x} \in Q \mid \forall i \in \{1, \ldots 6\}, F_{k,i}(\mathbf{x}.s) \geq 0\}$ where $F_{k,1}, \ldots, F_{k,6} : \mathbb{R}^7 \to \mathbb{R}$ are defined as follows:

$$F_{k,1}(s) = \epsilon_k - s.e_1; \quad F_{k,2}(s) = \epsilon_k + s.e_1; \tag{3}$$

$$F_{k,3}(s) = \phi_k + k_1 s.e_1 + k_2 s.e_2; \quad F_{k,4}(s) = \phi_k - k_1 s.e_1 - k_2 s.e_2; \tag{4}$$

$$F_{k,5}(s) = v_{max} - s.v; \quad F_{k,6}(s) = \delta s.v - \phi_b. \tag{5}$$

Here $v_{max} = v_T + \Delta a_{max}$ and $\phi_b > 0$ is an arbitrary constant. As we shall see shortly, the choice of ϕ_b affects the minimum speed of the vehicle and also the requirements of a brake action. We examine a state $\mathbf{x} \in \mathcal{I}_k$, that is, $F_{k,i}(\mathbf{x}.s) \geq 0$ for any $i \in \{1, \ldots 6\}$. $F_{k,1}(s), F_{k,2}(s) \geq 0$ means $s.e_1 \in [-\epsilon_k, \epsilon_k]$. $F_{k,3}(s), F_{k,4}(s) \geq 0$ means that the steering angle computed based on the proportional control law is in the range $[-\phi_k, \phi_k]$. Further, if $\phi_k \leq \phi_{max}$, then the computed steering satisfies the physical constraint of the vehicle. If, in addition, we have $\phi_b \geq \phi_k$ and $F_{k,6}(s) \geq 0$, then the vehicle actually executes the computed steering command. $F_{k,5}(s) \geq 0$ means that the speed of the vehicle is at most v_{max}. The sets $\mathcal{I}_k$, projected onto the (e_1, e_2) plane, for different values of the parameters ϵ_k and ϕ_k are shown in Figure 5.

For each $k \in \mathbb{N}$, we define

$$\theta_{k,1} = \frac{k_1}{k_2}\epsilon_k - \frac{1}{k_2}\phi_k \tag{6}$$

$$\theta_{k,2} = \frac{k_1}{k_2}\epsilon_k + \frac{1}{k_2}\phi_k \tag{7}$$

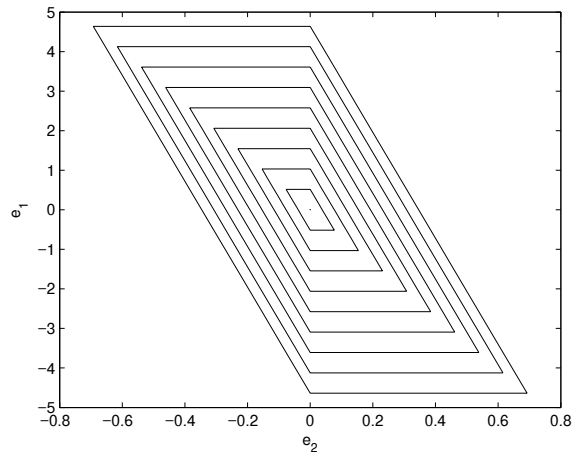


Fig. 5. The set $\mathcal{I}_k$ for different values of ϵ_k and ϕ_k, projected onto the e_1, e_2 plane.

That is, $\theta_{k,1}$ and $\theta_{k,2}$ are the values of e_2 at which the proportional control law yields the steering angle of ϕ_k and $-\phi_k$, respectively, given that the value of e_1 is $-\epsilon_k$. From the above definitions, we make the following observations about the boundary of the $\mathcal{I}_k$ sets: for any $k \in \mathbb{N}$ and $\mathbf{x} \in \mathcal{I}_k$, $\mathbf{x}.e_2 \in [-\theta_{k,2}, \theta_{k,2}]$, $F_{k,1}(\mathbf{x}.s) = 0$ implies $\mathbf{x}.e_2 \in [-\theta_{k,2}, -\theta_{k,1}]$, $F_{k,2}(\mathbf{x}.s) = 0$ implies $\mathbf{x}.e_2 \in [\theta_{k,1}, \theta_{k,2}]$, $F_{k,3}(\mathbf{x}.s) = 0$ implies $\mathbf{x}.e_2 \in [-\theta_{k,2}, \theta_{k,1}]$, and $F_{k,4}(\mathbf{x}.s) = 0$ implies $\mathbf{x}.e_2 \in [-\theta_{k,1}, \theta_{k,2}]$.

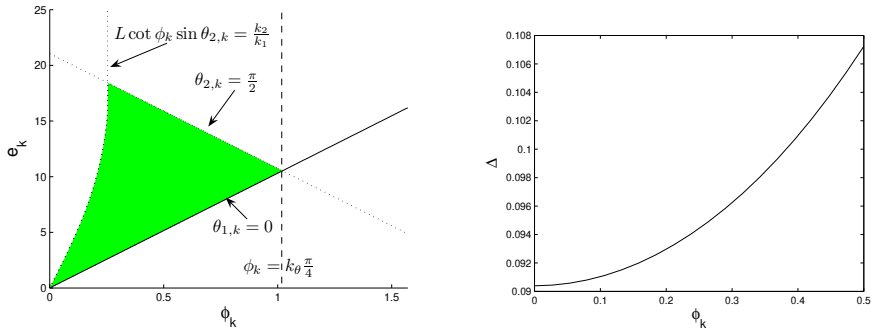
We assume that ϕ_b and all the $\epsilon_k's$ and ϕ_k's satisfy the following assumptions that are derived from physical and design constraints on the controller. The region in the ϕ_k,ϵ_k plane which satisfies Assumption 1 is shown Figure 6.

Assumption 1. *(Vehicle and controller design)*

(a) $\phi_k \leq \phi_b \leq \phi_{max}$ *and* $\phi_k < \frac{\pi}{2}$
(b) $0 \leq \theta_{k,1} \leq \theta_{k,2} < \frac{\pi}{2}$
(c) $L \cot \phi_k \sin \theta_{k,2} < \frac{k_2}{k_1}$
(d) $\Delta \leq \frac{c}{b}$ *where* $c = \frac{1}{\sqrt{k_1^2+k_2^2}}(\phi_k - \tilde{\phi})$, $b = v_{max}\sqrt{\sin^2\theta_{k,2} + \frac{1}{L^2}\tan^2(\tilde{\phi})}$ *and* $\tilde{\phi} = \cot^{-1}\left(\frac{k_2}{k_1 L \sin\theta_{k,2}}\right)$ [4].

If the vehicle is forced to slow down too much at the boundary of an $\mathcal{I}_k$ by the brakes, then it may not be able to turn enough to remain inside $\mathcal{I}_k$. Thus, in verifying the above properties we need to restrict our attention to *good executions* in which brake inputs do not occur at low speeds and are not too persistant. This is formalized by the next definition.

[4] Using assumption 1(d), it can be shown that $\tilde{\phi} < \phi_k$ so $\frac{c}{b} > 0$.



(a) (b)

Fig. 6. (a) The set of $(\epsilon_k,\ \phi_k)$ which satisfies assumptions 1 (c) and (d) and are represented by the green region. (b) The relationship between the maximum bound on Δ and ϕ_k for $\epsilon_k = \frac{1}{k_1}\phi_k$.

Definition 2. *A* good execution *is an execution α that satifies: if a* brake(On) *action occurs at time t then (a) $\alpha(t).v > \frac{\phi_b}{\delta} + \Delta|a_{brake}|$, (b)* brake$(Off)$ *must occur within time $t + \frac{1}{|a_{brake}|}(\alpha(t).v - \frac{\phi_b}{\delta} - \Delta|a_{brake}|)$.*

For the remainder of this section we only consider good executions. A state $\mathbf{x} \in Q_{\mathcal{A}}$ is reachable if there exists a good execution α with $\alpha.lstate = \mathbf{x}$.

5.2 Invariance Property

We fix a $k \in \mathbb{N}$ for the remainder of the section and denote $\mathcal{I}_k, F_{k,i}$ as $\mathcal{I}$ and F_i, respectively, for $i \in \{1,\ldots,6\}$. As in Lemma 2, we define $I = \{s \in \mathcal{X} \mid F_i(s) \geq 0\}$ and for each $i \in \{1,\ldots,6\}$, $\partial I_i = \{s \in \mathcal{X} \mid F_i(s) = 0\}$ and let the functions $f_1, f_2, \ldots, f_7 : \mathbb{R}^7 \times \mathbb{R}^2 \to \mathbb{R}$ describe the evolution of x, y, θ, v, e_1, e_2 and d, respectively. We prove that I satisfies the control-free invariance condition of Lemma 1 by applying Lemma 2.

First, we define the sets $C_1, \ldots, C_6$ and show that all the assumptions in Lemma 2 are satisfied. The proof does not involve solving differential equations but requires algebraic simplification of the expressions defining the vector fields and the boundaries $\{\partial I_i\}_{i\in\{1,\ldots 6\}}$ of the invariant set.

$$C_1 = C_2 = \emptyset \tag{8}$$

$$C_3 = \{s \in I \mid -k_1 s.e_1 - k_2 s.e_2 \leq 0 \vee L\cot(-k_1 s.e_1 - k_2 s.e_2)\sin\theta_{k,2} \geq \frac{k_2}{k_1}\} \tag{9}$$

$$C_4 = \{s \in I \mid -k_1 s.e_1 - k_2 s.e_2 \geq 0 \vee L\cot(k_1 s.e_1 + k_2 s.e_2)\sin\theta_{k,2} \geq \frac{k_2}{k_1}\} \tag{10}$$

$$C_5 = \{s \in I \mid s.v \leq v_T\} \tag{11}$$

$$C_6 = \{s \in I \mid s.v \geq \frac{\phi_b}{\delta} + \Delta|a_{brake}|\} \tag{12}$$

From the definition of a good execution (Definition 2), we show that when the value of the variable *brake* is *On*, the speed of the vehicle is at least $\frac{\phi_b}{\delta}+\Delta|a_{brake}|$.

Lemma 4. *At any reachable state* $\mathbf{x}$ *of* $\mathcal{A}$*, if* $\mathbf{x}.brake = On$ *then* $\mathbf{x}.v \geq \frac{\phi_b}{\delta} + \Delta|a_{brake}|$.

Proof. Consider an arbitrary execution fragment, $\alpha = \tau_0 a_1 \tau_1 a_2 \ldots$ and an arbitrary $i \in \mathbb{N}$ such that $(\tau_i \downarrow brake)(0) = On$. Since the initial value of the variable *brake* is *Off*, there must exists $j \leq i$ such that a_j is a $\mathsf{brake}(On)$ action and for any natural number $m \in [j, i]$, a_m is not a $\mathsf{brake}(Off)$ action. Let $(\tau_{j-1}.\mathsf{lstate}) \lceil v = v_b$. Since a_j is a $\mathsf{brake}(On)$ action which does not affect v, we get $(\tau_j.\mathsf{fstate}) \lceil v = v_b$. From Definition 2, $v_b > \frac{\phi_b}{\delta} + \Delta|a_{brake}|$ and there must exists $k > i$ such that a_k is a $\mathsf{brake}(Off)$ action and $\sum_{m=j}^{k-1} \tau_m.\mathsf{ltime} \leq \frac{1}{|a_{brake}|}(v_b - \frac{\phi_b}{\delta} - \Delta|a_{brake}|)$. So for any $t \in dom(\tau_i)$, we get

$$
\begin{aligned}
(\tau_i \downarrow v)(t) &\geq v_b + \min_{s, s_0 \in \mathcal{X}, l \in \mathcal{L}} f_4(s, g(l, s_0))(t + \sum_{m=j}^{i-1} \tau_m.\mathsf{ltime}) \\
&\geq v_b + a_{brake}(\sum_{m=j}^{k-1} \tau_m.\mathsf{ltime}) = \frac{\phi_b}{\delta} + \Delta|a_{brake}|
\end{aligned}
$$

■

The next lemma shows that the subtangential, bounded distance and bounded speed conditions (of Lemma 2) are satisfied with the the sets $\{C_j\}_{j \in \{1,\ldots,6\}}$ defined in (8)-(12). The proof applies Lemma 3. The knowledge about the reachable state $\mathbf{x}$ of $\mathcal{A}$ with $\mathbf{x}.brake = On$, provided in Lemma 4, is needed to prove the subtangential condition for $j = 6$.

Lemma 5. *For each* $l \in \mathcal{L}$ *and* $j \in \{1, \ldots, 6\}$*, the subtangential, bounded distance, and bounded speed conditions (of Lemma 2) are satisfied.*

Proof. Since $C_1, C_2 = \emptyset$, we see that the bounded distance and bounded speed conditions are automatically satisfied for $j = 1, 2$ with any arbitrary large c_j and arbitrary small b_j. Now, consider an arbitrary $s_0 \in I$ and $s \in \partial I_1$. By definition, $F_1(s) = 0$. From the definition of $\theta_{k,1}$ and $\theta_{k,2}$ and Assumption 1(b), $s.e_2 \in [-\theta_{k,2}, -\theta_{k,1}] \subset (-\frac{\pi}{2}, 0]$. In addition, since $s \in I$, $F_6(s) = \delta s.v - \phi_b \geq 0$ and since $\delta > 0$ and $\phi_b \geq 0$, $s.v \geq 0$. Thus,

$$
\frac{\partial F_1}{\partial s}(s) \cdot f(s, g(l, s_0)) = -\frac{de_1}{dt} = -s.v \sin(s.e_2) \geq 0
$$

For $j = 2$, the subtangential condition can be proved in a similar way.

To prove the bounded distance and the bounded speed conditions for $j = 3, \ldots, 6$, we apply Lemma 3. Let $\mathcal{U}_I = \{g(l, s) \mid l \in \mathcal{L},\ s \in I\}$. From the definition of I, we get that for any $s_0 \in I$, $-k_1 s_0.e_1 - k_2 s_0.e_2 \in [-\phi_k, \phi_k] \subset (-\frac{\pi}{2}, \frac{\pi}{2})$. Therefore, f is continuous in $I \times \mathcal{U}_I$.

In addition, it can be easily checked that the projection of I onto the (e_1, e_2, v) space is compact and for any $j \in \{3, \ldots, 6\}$, C_j is closed. Since the only variables involved in proving the control-free invariance condition of Lemma 1 are e_1, e_2 and v whose evolution along a trajectory can be described without other variables, from the proof of Lemma 2 and Lemma 3, we see that the requirement that I is compact can be relaxed to the requirement the projection of I onto the (e_1, e_2, v) space is compact. Hence, from Lemma 3, to prove that conditions (a)-(c) of Lemma 2 hold, we only need to show that for any $l \in \mathcal{L}$, the following conditions are satisfied for each $j \in \{3, \ldots, 6\}$:

1. $C_j \cap \partial I_j = \emptyset$
2. For any $s_0 \in I \setminus C_j$ and $s \in \partial I_j$, $\frac{\partial F_j}{\partial s} \cdot f(s, g(l, s_0)) \geq 0$

Consider an arbitrary $s \in \partial I_3$. From the definition of I_3, $-k_1 s.e_1 - k_2 s.e_2 = \phi_k > 0$. So from Assumption 1(c), $L \cot(-k_1 s.e_1 - k_2 s.e_2) \sin\theta_{k,2} < \frac{k_2}{k_1}$. Therefore, $C_3 \cap \partial I_3 = \emptyset$. Pick an arbitrary $s_0 \in I \setminus C_3$. From the definition of I and C_3, $0 < -k_1 s_0.e_1 - k_2 s_0.e_2 \leq \phi_k$ and $L \cot(-k_1 s_0.e_1 - k_2 s_0.e_2) \sin\theta_{k,2} < \frac{k_2}{k_1}$. Combining this with Assumption 1(a), we get $0 < -k_1 s_0.e_1 - k_2 s_0.e_2 \leq \frac{\pi}{2}$ and $|-k_1 s_0.e_1 - k_2 s_0.e_2| \leq \phi_{max}$. In addition, since $s_0 \in I$, $F_6(s_0) \geq 0$ and so $\delta s_0.v \geq \phi_b \geq \phi_k \geq |-k_1 s_0.e_1 - k_2 s_0.e_2|$, and since $s \in I$, $s.v \geq 0$. Therefore, we can conclude that

$$\frac{ds.e_2}{dt} = \frac{s.v}{L} \tan(-k_1 s_0.e_1 - k_2 s_0.e_2) \geq 0$$

and from Assumption 1(b), $s.e_2 \in [-\theta_{k,2}, \theta_{k,1}] \subset (-\frac{\pi}{2}, 0]$. So we get

$$\begin{aligned}\frac{ds.e_1}{ds.e_2} &= L \cot(-k_1 s_0.e_1 - k_2 s_0.e_2) \sin(s.e_2) \\ &\geq -L \cot(-k_1 s_0.e_1 - k_2 s_0.e_2) \sin\theta_{k,2} \\ &> -\frac{k_2}{k_1}.\end{aligned}$$

Thus,

$$\frac{\partial F_3}{\partial s} \cdot f(s, g(l, s_0)) = k_2 \frac{ds.e_2}{dt} + k_1 \frac{ds.e_1}{dt} = \frac{ds.e_2}{dt} \left(k_2 + k_1 \frac{ds.e_1}{ds.e_2} \right) \geq 0.$$

This completes the proof for $j = 3$.

For $j = 4$, we can follow the previous proof to show that $C_4 \cap \partial I_4 = \emptyset$, $\frac{ds.e_2}{dt} \leq 0$ and $\frac{ds.e_1}{ds.e_2} > -\frac{k_2}{k_1}$, and so

$$\forall s_0 \in I \setminus C_4, \frac{\partial F_4}{\partial s} \cdot f(s, g(l, s_0)) \geq 0.$$

Next, consider an arbitrary $s \in \partial I_5$. From the definition of ∂I_5, $s.v = v_{max}$. Since $a_{max}, \Delta > 0$, $v_{max} = v_T + \Delta a_{max} > v_T$. Therefore, $C_5 \cap \partial I_5 = \emptyset$. Pick

an arbitrary $s_0 \in I \setminus C_5$. From the definition of I and C_5, $v_T < s_0.v \leq v_{max}$. Therefore, we can conclude that

$$\frac{\partial F_5}{\partial s} \cdot f(s, g(l, s_0)) = \begin{cases} -a_{brake} \\ 0 \end{cases} \geq 0.$$

This completes the proof for $j = 5$.

Finally, consider an arbitrary $s \in \partial I_6$. From the definition of ∂I_6, $s.v = \frac{\phi_b}{\delta}$. Since $\Delta, |a_{brake}| > 0$, $\frac{\phi_b}{\delta} < \frac{\phi_b}{\delta} + \Delta|a_{brake}|$. Therefore, $C_6 \cap \partial I_6 = \emptyset$. Consider an arbitrary $s_0 \in I \setminus C_6$. From Lemma 4 and the definition of f_4, we see that $f_4(s, g(l, s_0)) = a_{brake}$ only if $s_0.v \geq \frac{\phi_b}{\delta} + \Delta|a_{brake}|$. But since $s_0 \in I \setminus C_6$, from the definition of I and C_6, $s_0.v < \frac{\phi_b}{\delta} + \Delta|a_{brake}|$. Therefore, $f_4(s, g(l, s_0))$ is either 0 or a_{max} and so we can conclude that

$$\frac{\partial F_6}{\partial s} \cdot f(s, g(l, s_0)) = f_4(s, g(l, s_0)) \geq 0.$$

■

From the definition of each C_j, we can derive the lower bound c_j on the distance from C_j to I and the upper bound b_j on the length of the vector field f where the control variable u is evaluated when the continuous state $s \in C_j$. Using these bounds and Assumption 1(d) we proof the sampling rate condition.

Lemma 6. *For each $l \in \mathcal{L}$, the sampling rate condition (of Lemma 2) is satisfied.*

Proof. For each $j \in \{1, \ldots, 6\}$, we want to find c_j and b_j which satisfy condition (b) and (c) of Lemma 2. First, we note that for $j = 1, 2$, $C_j = \emptyset$, so c_j can be arbitrary large and b_j can be arbitrary small and therefore any $\Delta \in \mathbb{R}_+$ satisfies the sampling rate condition of Lemma 2. For $j = 5, 6$, it can be easily shown that $c_5 = \Delta a_{max}$, $b_5 = a_{max}$, $c_6 = \Delta|a_{brake}|$ and $b_6 = |a_{brake}|$; thus, $\frac{c_j}{b_j} = \Delta$. That is, Δ can be an arbitrary large number if we only consider $j = 1, 2, 5, 6$. So we only have to consider $j = 3, 4$. From Assumption 1(c), there exists

$$\tilde{\phi} = \cot^{-1}\left(\frac{k_2}{k_1 L \sin\theta_{k,2}}\right) < \phi_k.$$

Using symmetry, we get that for $j = 3$ and $j = 4$, the shortest distance between $\mathcal{U}_j$ and ∂I_j is then given by

$$c_j = \min_{s \in \partial I_j, s_0 \in \mathcal{U}_j} \|s - s_0\| = \frac{1}{\sqrt{k_1^2 + k_2^2}}(\phi_k - \tilde{\phi}).$$

Since $\forall s \in I, s.e_2 \in [-\theta_{k,2}, \theta_{k,2}] \subset (-\frac{\pi}{2}, \frac{\pi}{2})$, we have

$$\begin{aligned} b_j &= \max_{s \in I, s_0 \in \mathcal{U}_j} \|f(s, g(l, s_0))\| \\ &\leq v_{max}\sqrt{\sin^2\theta_{k,2} + \frac{1}{L^2}\tan^2(\tilde{\phi})} \end{aligned}$$

From Assumption 1(d), we see that $\Delta \leq \min_{j\in\{1,\ldots,6\}} \frac{c_j}{b_j}$. ■

Thus, all assumptions in the hypothesis of Lemma 2 are satisfied; from Theorem 1 we obtain that good execution fragments of $\mathcal{A}$ preserve invariance of $\mathcal{I}$, provided that the path and current segment do not change over the fragment.

Theorem 2. *For any* plan*-free execution fragment β starting at a state $\mathbf{x} \in \mathcal{I}$ and ending at $\mathbf{x}' \in Q_{\mathcal{A}}$, if $\mathbf{x}.path = \mathbf{x}.new_path$ and $\mathbf{x}.seg = \mathbf{x}'.seg$, then $\mathbf{x}' \in \mathcal{I}$.*

Proof. From Lemmas 5-6, we see that all the conditions in Lemma 2 are satisfied. Thus, we can conclude that the control-free invariance condition of Lemma 1 is satisfied. In addition, from the specification of main action, we see that a discrete transition in the continuous state s only occurs when $path \neq new_path$ (i.e. a new path is received) or $s.d \leq 0$ (i.e. the vehicle has reached the end of the current segment). Hence, if a closed execution β does not contain a plan action, $\beta.\mathsf{fstate} \lceil path = \beta.\mathsf{fstate} \lceil new_path$ and $\beta.\mathsf{lstate} \lceil seg = \beta.\mathsf{fstate} \lceil seg$, then a discrete transition in the continuous state s does not occur in β. Applying Theorem 1, we get the desired result.

5.3 Segment Progress

In this section, we establish the segment progress property. First, we prove the progress property over a pasted trajectory τ between any two main actions. That is, suppose right after an occurrence of a main action, $\mathbf{x} \in \mathcal{I}_k$ for some $k \in \mathbb{N}$. Then, right before an occurrance of the next main action, $\mathbf{x} \in \mathcal{I}_{k+1}$ where $\mathcal{I}_{k+1} \subseteq \mathcal{I}_k$ and if k is less than some threshold k^*, then $\mathcal{I}_{k+1}$ is strictly contained in $\mathcal{I}_k$. Next, in Lemma 9, we compute the bound d^* on the maximum change in the value of d over τ. Given the progress property over τ and the bound d^*, we can then establish the segment progress property (B) defined at the beginning of Section 5. That is, starting from a state $\mathbf{x}$ and ending at $\mathbf{x}'$, if $\mathbf{x} \in \mathcal{I}_k$, then $\mathbf{x}' \in \mathcal{I}_{k+n}$ where an integer $n \geq 0$ depends $\mathbf{x}.d - \mathbf{x}'.d$ and the system parameters, provided that path and current segment do not change. Furthermore, if $\mathbf{x}.d - \mathbf{x}'.d$ is large enough, then n is strictly positive.

We further assume that for any natural number k, ϕ_k satisfies the following assumption.

Assumption 2. *(Controller design)* $\frac{\tan\phi_k}{2L} v_{max} \Delta \leq \frac{\pi}{2}$

First, we solve the differential equation which describes the evolution of e_1 and e_2 along τ. From periodicity of main actions we see that $dom(\tau) = [0, \Delta]$. Define the functions $e_1, e_2, v, v_{avg} : dom(\tau) \to \mathbb{R}$ as follows: $e_1(t) = (\tau \downarrow e_1)(t)$, $e_2(t) = (\tau \downarrow e_2)(t)$, $v(t) = (\tau \downarrow v)(t)$ and $v_{avg}(t) = \frac{1}{t}\int_0^t v(t')dt'$. From the state models of the Vehicle and the Controller specified in Figure 3 and Figure 4, since ϕ and a are constant along τ, the solution to the differential equations can be

solved analytically and are given by

$$
\begin{aligned}
e_1(t) &= \begin{cases} e_1(0) + L\cot\phi\cos e_2(0) - L\cot\phi\cos e_2(t) & \text{if } \phi \neq 0 \\ e_1(0) + v_{avg}(t)t\sin e_2(0) & \text{otherwise} \end{cases} \\
e_2(t) &= e_2(0) + \tfrac{\tan\phi}{L} v_{avg}(t)t
\end{aligned} \tag{13}
$$

where $\phi = \tau.\mathsf{fstate} \lceil \phi$ and $a = \tau.\mathsf{fstate} \lceil a$.

The following lemma provides a bound on the change in e_1 over τ and on the change in ϕ between two consecutive main actions assuming that a discrete transition in the continuous state s does not occur.

Lemma 7. *Suppose $\tau.\mathsf{fstate} \in \mathcal{I}_k$ for some $k \in \mathbb{N}$. Then, $|e_1(0) - e_1(\Delta)| \leq \Delta_e$ and $|(k_1 e_1(0) + k_2 e_2(0)) - (k_1 e_1(\Delta) + k_2 e_2(\Delta))| \leq \Delta_\phi$ where $\Delta_e = v_{max}\Delta$ and $\Delta_\phi = v_{max}\Delta\left(k_1 + k_2 \frac{\tan\phi_k}{L}\right)$.*

Proof. From (13), we see that $|e_1(\Delta) - e_1(0)| \leq v_{max}\Delta$ and $|e_2(\Delta) - e_1(0)| \leq \frac{\tan\phi_k}{L} v_{max}\Delta$. So

$$
\begin{aligned}
|(k_1 e_1(0) + k_2 e_2(0)) - (k_1 e_1(\Delta) + k_2 e_2(\Delta))| &\leq k_1 |e_1(\Delta) - e_1(0)| + k_2 |e_2(\Delta) - e_2(0)| \\
&\leq k_1 v_{max}\Delta + k_2 \frac{\tan\phi_k}{L} v_{max}\Delta
\end{aligned}
$$

■

The next lemma proves the desired progress property over τ

Lemma 8. *Suppose $\tau.\mathsf{fstate} \in \mathcal{I}_k$ for some $k \in \mathbb{N}$. Then $\tau.\mathsf{lstate} \in \mathcal{I}_{k+1}$ whose parameters ϵ_{k+1} and ϕ_{k+1} are given by*

$$\epsilon_{k+1} = \epsilon_k - a_k \tag{14}$$

$$\phi_{k+1} = \phi_k - b_k \tag{15}$$

where $a_k, b_k \geq 0$ and are given by

$$a_k = \epsilon_k - \max\left(\epsilon'_{k+1}, \frac{1}{k_1}\phi'_{k+1}\right) \tag{16}$$

$$b_k = \phi_k - \max(\phi'_{k+1}, \varphi) \tag{17}$$

$$\epsilon'_{k+1} = \begin{cases} \max\left(\epsilon_k - \xi_k, \epsilon^*_k\right) & \textit{if } \epsilon_k > \epsilon^*_k \\ \epsilon_k & \textit{otherwise} \end{cases} \tag{18}$$

$$\phi'_{k+1} = \begin{cases} \max\left(\phi_k - \psi_k, \phi^*_k\right) & \textit{if } \phi_k > \phi^*_k \\ \phi_k & \textit{otherwise} \end{cases} \tag{19}$$

$$\epsilon^*_k = \epsilon'_k + v_{max}\Delta \tag{20}$$

$$\phi^*_k = \phi'_k + k_1 v_{max}\Delta + k_2 \frac{\tan\phi_k}{L} v_{max}\Delta \tag{21}$$

$$\xi_k = -2L \max_{\phi\in[-\phi_k,\phi_k]} \cot\phi \sin\left(-\frac{k_1}{k_2}\epsilon^*_k - \frac{1}{k_2}\phi + \frac{\tan\phi}{2L}v_{max}\Delta\right)\sin\left(\frac{\tan\phi}{2L}\frac{\phi_b}{\delta}\Delta\right) \tag{22}$$

$$\psi_k = \frac{k_2}{L}\tan\phi^*_k\frac{\phi_b}{\delta}\Delta - 2k_1 L\cot\phi^*_k \sin\theta_{k,2}\sin\left(\frac{\tan\phi_k}{2L}v_{max}\Delta\right) \tag{23}$$

$$\epsilon'_k = \max_{\tilde{\phi}\in[-\phi_k,\phi_k]}\left(-\frac{1}{k_1}\tilde{\phi} + \frac{k_2}{k_1}\frac{\tan\tilde{\phi}}{2L}v_{max}\Delta\right) \tag{24}$$

$$\phi'_k = \max\left(\tan^{-1}\sqrt{\frac{2k_1L^2\delta}{k_2\phi_b\Delta}\sin\theta_{k,2}\sin\left(\frac{\tan\phi_k}{2L}v_{max}\Delta\right)}, \Delta_\phi\right) \tag{25}$$

where φ is the minimum value of ϕ_{k+1} such that ϵ'_{k+1} and ϕ_{k+1} satisfy Assumption 1(d). Define k^* to be the minimum value of k such that $\epsilon_k \leq \epsilon^*_k$ or $\phi_k \leq \phi^*_k$. (If for any k, $\epsilon_k > \epsilon^*_k$ and $\phi_k > \phi^*_k$, just pick an arbitrary natural number k^*.) Then, for any $k < k^*$, a_k and b_k are strictly positive, that is, $I_{k+1} \subsetneq I_k$.

Proof. Since by definition $\epsilon_{k+1} \geq \epsilon'_{k+1}$ and $\phi_{k+1} \geq \phi'_{k+1}$, we see that if $|\tau.\mathsf{lstate} \lceil e_1| \leq \epsilon'_{k+1}$ and $|k_1(\tau.\mathsf{lstate} \lceil e_1) + k_2(\tau.\mathsf{lstate} \lceil e_2)| \leq \phi'_{k+1}$, then $\tau.\mathsf{lstate} \in \mathcal{I}_{k+1}$. To show that ϵ_{k+1} and ϕ_{k+1} satisfy assumption 1 and that $a_k, b_k \geq 0$, we use the following observations: (a) $\psi_k \geq 0$ and $\xi_k \geq 0$ and thus, $\epsilon'_{k+1} \leq \epsilon_k$ and $\phi'_{k+1} \leq \phi_k$, (b) given ϕ'_{k+1}, $\frac{1}{k_1}\phi'_{k+1}$ is the minimum value of ϵ_{k+1} such that ϵ_{k+1} and ϕ'_{k+1} satisfies assumption 1, (c) given ϵ'_{k+1}, φ is the minimum value of ϕ_{k+1} such that ϵ'_{k+1} and ϕ_{k+1} satisfies assumption 1, and (d) φ decreases as ϵ'_{k+1} decreases. With these observations and the assumption that ϵ_k and ϕ_k satisfy assumption 1, it can be easily checked that (a) $\epsilon_{k+1} \leq \epsilon_k$ and $\phi_{k+1} \leq \phi_k$, (b) if $\epsilon_k > \epsilon^*_k$ and $\phi_k > \phi^*_k$, then $\epsilon'_{k+1} < \epsilon_k$ and $\phi'_{k+1} < \phi_k$, and (c) if $\epsilon_{k+1} \neq \epsilon'_{k+1}$, then $\phi_{k+1} = \phi'_{k+1}$ and if $\phi_{k+1} \neq \phi'_{k+1}$, then $\epsilon_{k+1} = \epsilon'_{k+1}$. Thus, we can conclude that ϵ_{k+1} and ϕ_{k+1} satisfy assumption 1 and that if $\epsilon_k > \epsilon^*_k$ and $\phi_k > \phi^*_k$, then $\epsilon_{k+1} < \epsilon_k$ and $\phi_{k+1} < \phi_k$.

So what remain to be proved are $|\tau.\mathsf{lstate} \lceil e_1| \leq \epsilon'_{k+1}$ and $|k_1(\tau.\mathsf{lstate} \lceil e_1) + k_2(\tau.\mathsf{lstate} \lceil e_2)| \leq \phi'_{k+1}$. From Theorem 2, $\tau.\mathsf{lstate} \in \mathcal{I}_k$. Thus, we can

conclude that $\phi'_{k+1} \leq \phi_k$ and $\epsilon'_{k+1} \leq \epsilon_k$. This completes the proof for the second case of (18) and (19).

Next, we prove the first case of (19). Let $\phi_f = -k_1 e_1(0) - k_2 e_2(0)$ and $\phi_l = -k_1 e_1(\Delta) - k_2 e_2(\Delta)$. Suppose $|\phi_f| \geq \Delta_\phi$. From (13), we get that

$$\phi_l = -k_1 \left(e_1(0) + L\cot\phi_1 \cos(e_2(0)) - L\cot\phi_1 \cos(e_2(\Delta))\right) - k_2 \left(e_2(0) + \frac{\tan\phi_f}{L} v_{avg}\Delta\right)$$

where v_{avg} is the average speed of the vehicle over τ. Substituting $e_1(0) = -\frac{k_2}{k_1} e_2(0) - \frac{1}{k_1}\phi_f$, we get

$$\phi_l = \phi_f - \left(\frac{k_2}{L}\tan\phi_f v_{avg}\Delta + 2k_1 L\cot\phi_f \sin(\frac{1}{2}(e_2(0) + e_2(\Delta))) \sin\left(\frac{\tan\phi_f}{2L} v_{avg}\Delta\right)\right).$$

Since $\tau.\mathsf{fstate}, \tau.\mathsf{lstate} \in \mathcal{I}_k$, from the definition of $\theta_{k,2}$, we see that $|e_2(0)|, |e_2(\Delta)| \leq \theta_{k,2}$. So $\frac{1}{2}|e_2(0) + e_2(\Delta)| \leq \theta_{k,2}$. In addition, from Lemma 2 and the definition of F_5 and F_6, we know that $\frac{\phi_b}{\delta} \leq v_{avg} \leq v_{max}$. From Lemma 8, we get that ϕ_f and ϕ_l have the same sign. So it is easy to show that

$$|\phi_l| \leq |\phi_f| - \left(\frac{k_2}{L}\tan|\phi_f|\frac{\phi_b}{\delta}\Delta - 2k_1 L\cot|\phi_f|\sin\theta_{k,2}\sin\left(\frac{\tan\phi_k}{2L} v_{max}\Delta\right)\right).$$

Define the function $\Psi : [0, \phi_k] \to \mathbb{R}$ by

$$\Psi(\phi) = \frac{k_2}{L}\tan\phi\frac{\phi_b}{\delta}\Delta - 2k_1 L\cot\phi\sin\theta_{k,2}\sin\left(\frac{\tan\phi_k}{2L} v_{max}\Delta\right).$$

That is $\psi_k = \Psi(\phi_k^*)$. It can be easily checked that with assumption 2, $\Psi(\phi)$ increases with ϕ and vanishes when $\phi = \tan^{-1}\sqrt{\frac{2k_1 L^2\delta}{k_2\phi_b\Delta}\sin\theta_{k,2}\sin\left(\frac{\tan\phi_k}{2L} v_{max}\Delta\right)}$ which does not exceed ϕ'_k defined in (25). For $\phi > \phi'_k$, $\Psi(\phi) > 0$. From Lemma 7, we also know that for any $\phi_f \in [-\phi_k, \phi_k]$,

$$|\phi_l| \leq |\phi_f| + k_1 v_{max}\Delta + k_2\frac{\tan\phi_k}{L} v_{max}\Delta.$$

Since $\phi_k^* > \phi'_k$, we arrive at the following conclusion:

$$|\phi_l| \leq \begin{cases} |\phi_f| - \psi_k & \text{if } |\phi_f| > \phi_k^* \\ \phi_k^* & \text{if } \phi'_k \leq |\phi_f| \leq \phi_k^* \\ |\phi_f| + k_1 v_{max}\Delta + k_2\frac{\tan\phi_k}{L} v_{max}\Delta & \text{if } |\phi_f| < \phi'_k \end{cases}$$

Thus, $|\phi_l| \leq \max(\phi_k - \psi_k, \phi_k^*)$.

Finally, we prove the first case of (18). From (13), we get that

$$e_1(\Delta) = e_1(0) + 2L\cot\phi_1 \sin\left(e_2(0) + \frac{\tan\phi_f}{2L} v_{avg}\Delta\right)\sin\left(\frac{\tan\phi_f}{2L} v_{avg}\Delta\right).$$

Note that the case where $\phi_f = 0$ is also captured by this equation as $\lim_{\phi_f \to 0} 2L \cot \phi_f \sin\left(\frac{\tan \phi_f}{2L} v_{avg} \Delta\right) = v_{avg}\Delta$. Define the function $\Xi : [0, \epsilon_k] \to \mathbb{R}$ by

$$\Xi(\epsilon) = -2L \max_{\phi \in [-\phi_k, \phi_k]} \cot \phi \sin\left(-\frac{k_1}{k_2} e - \frac{1}{k_2}\phi + \frac{\tan \phi}{2L} v_{max} \Delta\right) \sin\left(\frac{\tan \phi}{2L} \frac{\phi_b}{\delta} \Delta\right).$$

That is $\xi_k = \Xi(\epsilon_k^*)$. It can be easily checked that with assumption 2, $\Xi(\epsilon) > 0$ for any $\epsilon > \epsilon_k'$ and that if $e_1(0) \geq \epsilon_k'$, then $e_2(0) \leq -\frac{k_1}{k_2}\epsilon_k' - \frac{1}{k_2}\phi_f$ and so $2L \cot \phi_f \sin\left(e_2(0) + \frac{\tan \phi_f}{2L} v_{avg}\Delta\right) \sin\left(\frac{\tan \phi_f}{2L} v_{avg}\Delta\right) \leq -\xi_k$. Using symmetry, we can derive similar lower bound for the case where $e_1(0) \leq -\epsilon_k'$. From Lemma 7, we also know that

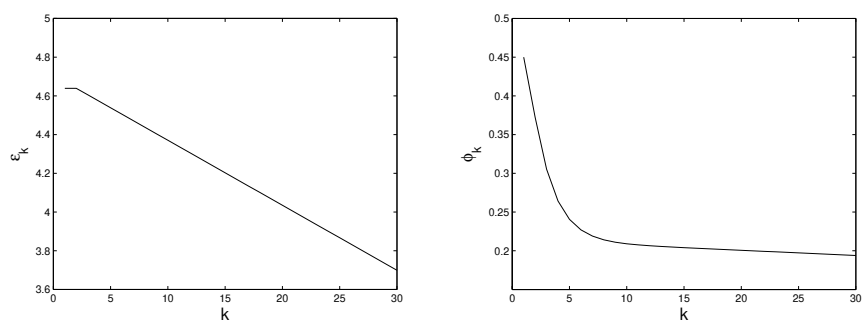
$$|e_1(\Delta)| \leq |e_1(0)| + v_{max}\Delta$$

So we arrive at the following conclusion:

$$|e_1(\Delta)| \leq \begin{cases} |e_1(0)| - \xi_k & \text{if } |e_1(0)| > \epsilon_k^* \\ \epsilon_k^* & \text{if } \epsilon_k' \leq |e_1(0)| \leq \epsilon_k^* \\ |e_1(0)| + v_{max}\Delta & \text{if } |e_1(0)| < \epsilon_k' \end{cases}$$

Thus, $|e_1(\Delta)| \leq \max(\epsilon_k - \xi_k, \epsilon_k^*)$. ■

The plot showing the progress in the deviation and disoriantation is shown in Figure 7.



(a) (b)

Fig. 7. The progress in deviation and disorientation. (a) The relationship between ϵ_k and k. (b) The relationship between ϕ_k and k

The following lemma provides the value of the bound d^* on the maximum change in the value of d over τ

Lemma 9. *Suppose* $\tau.\mathsf{fstate} \in \mathcal{I}_k$ *for some* $k \in \mathbb{N}$*. For any* $t \in dom(\tau)$*,* $|(\tau \lceil d)(t) - \tau.\mathsf{fstate} \lceil d| \leq d^*$ *where* $d^* = v_{max}\Delta$*.*

Proof. From Theorem 2, the definition of F_5 and F_6 and the definition of f_7 which describes the evolution of d, we get that $\max_{s,s_0 \in I} \|f_7(s, g(l, s_0))\| \leq v_{max}$. Since $dom(\tau) = [0, \Delta]$, we get $|(\tau \downarrow d)(t) - \tau.\mathsf{fstate} \lceil d| \leq \max_{s,s_0 \in I} \|f_7(s, g(l, s_0))\|\Delta \leq v_{max}\Delta$.

Using Lemma 8 and Lemma 9, we establish the relationship between the progress of $\mathcal{I}_k$ and the decrease in the value of d.

Lemma 10. *For each* $k \in \mathbb{N}$*, starting from any reachable state* $\mathbf{x} \in \mathcal{I}_k$ *such that* $\mathbf{x}.d > v_{max}\Delta$*,* $\mathbf{x}.path = \mathbf{x}.new_path$ *and* $\mathbf{x}.next = \mathbf{x}.now$*, any* plan*-free execution fragment* β *with* $\beta.\mathsf{ltime} = \Delta$ *satisfies* $\beta.\mathsf{lstate} \in \mathcal{I}_{k+1}$ *and* $\beta.\mathsf{lstate} \lceil d \geq \mathbf{x}.d - v_{max}\Delta$*.*

Proof. Since $\mathbf{x}.next = \mathbf{x}.now$ and $\beta.\mathsf{ltime} = \Delta$, we see that β can be written as $\beta = \beta'$ or $\beta = \beta'\mathsf{main}\tau_j\mathsf{brake}(b_j)\tau_{j+1}\mathsf{brake}(b_{j+1})\ldots\tau_n$ where β' is an execution fragment with exactly one main action a_i which occurs at time 0 and is immediately followed by a main action in the execution, $\beta'.\mathsf{ltime} = \Delta$ and $\tau_j, \ldots \tau_n$ are point trajectories. Let τ be the pasted trajectory of all the trajectories after a_i in β'. Then, τ is a pasted trajectory of all the trajectories between two main actions and so Lemma 8 and Lemma 9 apply. Since the main action a_i occurs at time 0 in β and brake action does not affect the value of s, we see that $\tau_{i-1}.\mathsf{lstate} \lceil s = \mathbf{x}.s$. So $\tau_{i-1}.\mathsf{lstate} \lceil d > v_{max}\Delta > 0$ and hence a_i does not change the value of s. That is, $\tau.\mathsf{fstate} = \mathbf{x} \in \mathcal{I}_k$. From Lemma 8, we get that $\beta'.\mathsf{lstate} \in \mathcal{I}_{k+1}$. In addition, from Lemma 9, we see that $\beta'.\mathsf{lstate} \lceil d \geq \mathbf{x}.d - v_{max}\Delta$. Since $\mathbf{x}.d > v_{max}\Delta$, we get $\beta'.\mathsf{lstate} \lceil d > 0$. Therefore, the main action following β' does not change the value of s. In addition, since brake action only affects the *brake* variable, we see that $\beta.\mathsf{lstate} \lceil s = \beta'.\mathsf{lstate} \lceil s$. Hence, we can conclude that $\beta.\mathsf{lstate} \in \mathcal{I}_{k+1}$ and $\beta.\mathsf{lstate} \lceil d \geq \mathbf{x}.d - v_{max}\Delta$.

Finally, we conclude the section by establishing the segment progress property (B) defined at the beginning of Section 5.

Lemma 11. *For each* $k \in \mathbb{N}$*, starting from any reachable state* $\mathbf{x} \in \mathcal{I}_k$*, any reachable state* $\mathbf{x}'$ *is in* $\mathcal{I}_{k+n}$ *where* $n = \max(\lfloor \frac{\mathbf{x}.d - \mathbf{x}'d}{v_{max}\Delta} \rfloor - 1, 0)$*, provided that path and current segment do not change.*

Proof. Consider an arbitrary closed execution fragment β starting at $\mathbf{x}$ and ending at $\mathbf{x}'$. Since by assumption, β is a plan-free execution fragment such that $\beta.\mathsf{lstate} \lceil path = \beta.\mathsf{fstate} \lceil new_path$ and $\beta.\mathsf{lstate} \lceil seg = \beta.\mathsf{fstate} \lceil seg$, from Theorem 2, we know that $\beta.\mathsf{lstate} \in \mathcal{I}_k$. This completes the proof for the case where $\lfloor \frac{\mathbf{x}.d - \mathbf{x}'d}{v_{max}\Delta} \rfloor - 1 \leq 0$.

Next, consider the case where $\lfloor \frac{\mathbf{x}.d - \mathbf{x}'.d}{v_{max}\Delta} \rfloor - 1 > 0$. From the structure of a PCHA, we see that $next = now$ every Δ time. So, the first state in β such that $next = now$ occurs no later than time Δ. Using Lemma 9, we see that at this state, $d \geq \mathbf{x}.d - v_{max}\Delta$. Applying Lemma 10 and using an invariance of $\mathcal{I}_k$ for any

k proved in Theorem 2, we get that $\beta_1.\mathsf{lstate} \in \mathcal{I}_{k+n}$ where $n = \lfloor \frac{\mathbf{x}.d - v_{max}\Delta - \mathbf{x}'.d}{v_{max}\Delta} \rfloor$. ■

Figure 8 shows a sequence of shrinking $\mathcal{I}_k$'s visited by $\mathcal{A}$ in making progress towards a waypoint.

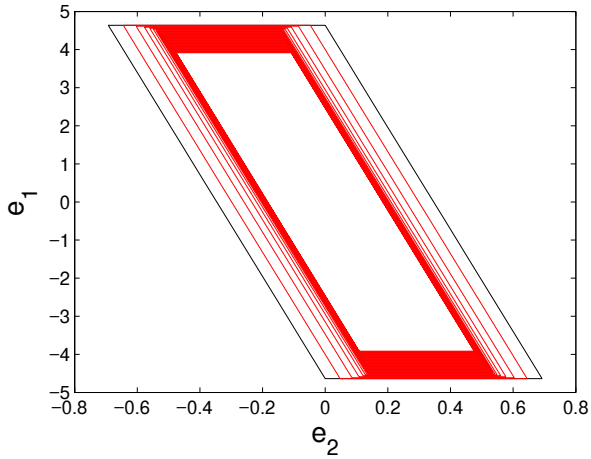


Fig. 8. $\mathcal{I}_k$ in black, $\mathcal{I}_{k+i}$ in red for $i > 0$.

5.4 Safety and Waypoint Progress: Identifying Safe Planner Paths

In this section, we derive a sufficient condition on planner paths that can be safely followed with respect to a chosen set $\mathcal{I}_k$ whose parameters $\epsilon_k \in [0, e_{max}]$ and $\phi_k \in [0, \phi_{max}]$ satisfy Assumption 1. The choice of $\mathcal{I}_k$ is made such that it is the smallest invariant set containing the the initial state $Q_{0\mathcal{A}}$. Then, we prove an invariance of $\mathcal{I}_k$ and conclude that the safety and waypoint progress properties (A) and (C) defined at the beginning of Section 5 are satisfied.

The proof is structured as follows. First, we consider an execution fragment where path does not change and starting with waypoint-distance not shorter than some threshold D^*. Lemma 12 uses the progress property established in Section 5.3 to prove that this execution fragment preserves $\mathcal{I}_k$. Then, in Lemma 13 and Lemma 14, we show that right after a path is changed, the waypoint-distance is not shorter than D^* and the state of $\mathcal{A}$ remains in $\mathcal{I}_k$. Using these results, Lemma 15 concludes that an execution fragment which updates the path exactly once by the first main action preserves $\mathcal{I}_k$. Finally, we use Lemma 12 and Lemma 15 to conclude the section that $\mathcal{I}_k$ is an invariant of $\mathcal{A}$ and with this result, we conclude that the system satisfies the safety and waypoint progress properties (A) and (C) defined at the beginning of Section 5.

The following assumption provides sufficient conditions for planner paths that can be safely followed. The key idea in the condition is: *longer path segments can be succeeded by sharper turns*. Following a long segment, the vehicle reduces its deviation and disorientation by the time it reaches the end, and thus, it is possible for the vehicle to turn more sharply at the end without breaking an invariance of $\mathcal{I}_k$.

Assumption 3. *(Planner paths) Let $p_0, p_1, \ldots$ be a planner path; for $i \in \{0, 1, \ldots\}$, let λ_i be the length of the segment $\overline{p_i p_{i+1}}$ and σ_i be the difference in orientation of $\overline{p_i p_{i+1}}$ and that of $\overline{p_{i+1} p_{i+2}}$. Then,*

(a) $\lambda_i \geq 2 v_{max} \Delta + \epsilon_k$.
(b) Let $n = k + \lfloor \frac{\lambda_i - \epsilon_k - 2 v_{max} \Delta}{v_{max} \Delta} \rfloor$. *Then, λ_i and σ_i satisfy the following conditions:*

$$\epsilon_{k+n} \leq \frac{1}{|\cos \sigma_i|} (\epsilon_k - v_{max} \Delta |\sin \sigma_i|) \tag{26}$$

$$\phi_{k+n} \leq \phi_k - k_1 v_{max} \Delta \sin |\sigma_i| - k_1 \epsilon_{k+n} (1 - \cos \sigma_i) - k_2 |\sigma_i| \tag{27}$$

where, given ϵ_k and ϕ_k, ϵ_j and ϕ_j are defined recursively for any $j > k$ by $\epsilon_j = \epsilon_{j-1} - a_{j-1}$ and $\phi_j = \phi_{j-1} - b_{j-1}$ where a_{j-1}, b_{j-1} are defined in Lemma 8.

The relationship between λ and the maximum value of σ which satisfies this assumption is shown in Figure 9.

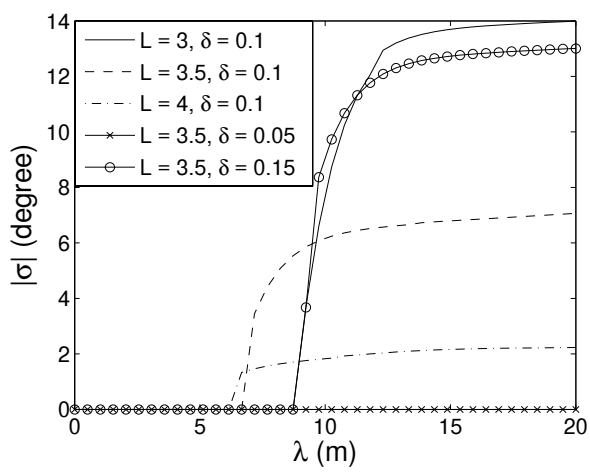


Fig. 9. Segment length vs. maximum difference between consecutive segment orientations, for different values of L and δ.

To establish that $\mathcal{I}_k$ is an invariant of $\mathcal{A}$, we further assume that (a) new planner paths begin at the current position, (b) Vehicle is not too disoriented

with respect to new paths, and (c) Vehicle speed is not too high as stated in Assumption 4.

Assumption 4. *(*plan *action and new path)*

(a) Any new path $p = p_1 p_2 \ldots$ satisfies $p_1 = [x_p, y_p]$ where x_p and y_p are the values of the variable x and y, respectively, when the path is received (i.e. when the plan *action occurs). That is, for any new input path, the path must begin at the current position of the vehicle.*

(b) Let v_p and θ_p be the speed and the orientation of the vehicle, respectively, when a plan *action occurs. Then,*

$$v_p < \frac{\epsilon_k}{\Delta\sqrt{1+\sin^2\theta_{k,2}}} - a_{max}\Delta$$

In addition, let $p = p_1 p_2 \ldots$ be the received path and let $\boldsymbol{p}$ be the vector which represents a straight line defined by p_1 and p_2. Then,

$$|\angle \boldsymbol{p} - \theta_p| \leq \frac{\phi_k}{k_2} - (v_p + a_{max}\Delta)\Delta\left(\frac{k_1}{k_2}\sqrt{1+\sin^2\theta_{k,2}} + \frac{\tan\phi_k}{L}\right).$$

First, we consider an execution fragment where path does not change and starting with a large enough waypoint-distance. The following lemma uses the progress property established in Section 5.3 to shows that before switching to the next segment, $\mathbf{x} \in \mathcal{I}_{k+n}$ where $n \geq 0$ depends on the segment length. Since we restrict the sharpness of the turn with respect to segment length (Assumption 3), we can then conclude that this execution fragment preserves $\mathcal{I}_k$.

Lemma 12. *Consider a* plan*-free execution fragment β starting at a state $\mathbf{x} \in \mathcal{I}_k$. Suppose $\mathbf{x}.path = \mathbf{x}.new_path$ and $\mathbf{x}.d \geq \lambda_1 - \epsilon_k - v_{max}\Delta$ where λ_1 is the length of the segment $\mathbf{x}.seg$. Then $\beta.\mathsf{lstate} \in \mathcal{I}_k$.*

Proof. First, observe that β can be written as $\beta = \beta_1 a_1 \beta_2 a_2 \ldots \beta_m$ where for any i, a_i is a main action and β_i is a plan-free execution fragment such that $\beta_i.\mathsf{lstate} \lceil path = \beta_i.\mathsf{fstate} \lceil new_path$ and $\beta_i.\mathsf{lstate} \lceil seg = \beta_i.\mathsf{fstate} \lceil seg$. From Lemma 2, we get that for any i, if $\beta_i.\mathsf{fstate} \in \mathcal{I}_k$, then $\beta.\mathsf{lstate} \in \mathcal{I}_k$. So, suppose $\beta_1.\mathsf{fstate} \in \mathcal{I}_k$, $\beta_1.\mathsf{fstate} \lceil path = \beta_1.\mathsf{fstate} \lceil new_path$ and $\beta_1.\mathsf{fstate} \lceil d \geq \lambda_1 - \epsilon_k - v_{max}\Delta$. We only need to show that for any $i > 1$, $\beta_i.\mathsf{fstate} \in \mathcal{I}_k$.

Consider the base case $i = 2$. If $\beta_2.\mathsf{fstate} \lceil seg = \beta_1.\mathsf{lstate} \lceil seg$, then a_1 does not change the continuous state s, and so $\beta_2.\mathsf{fstate} \in \mathcal{I}_k$. Otherwise, $\beta_2.\mathsf{fstate} \lceil seg = \beta_1.\mathsf{fstate} \lceil seg + 1$. But from the update rule of the variable seg and Lemma 9, it can be easily shown that $-v_{max}\Delta < \beta_1.\mathsf{lstate} \lceil d \leq 0$. Applying Lemma 11, we get that $\beta_1.\mathsf{lstate} \in \mathcal{I}_{k+n}$ where $n = \lfloor \frac{\lambda_1 - \epsilon_k - 2v_{max}\Delta}{v_{max}\Delta} \rfloor$ because by Assumption 3(a), $\lambda_1 - \epsilon_k - 2v_{max}\Delta > 0$.

Let $\mathbf{x}_1 = \beta_1.\mathsf{lstate}$ and $\mathbf{x}_2 = \beta_2.\mathsf{fstate}$ and let σ_1 be the difference between the orientation of $\beta_1.\mathsf{fstate} \lceil seg$ and $\beta_1.\mathsf{fstate} \lceil seg + 1$. From the update rule for e_1 and the definition of $\boldsymbol{p}$, $\boldsymbol{q}$ and $\boldsymbol{r}$ in Figure 4, it can be shown that $\mathbf{x}_2.e_1 = \mathbf{x}_1.d \sin\sigma_1 + \mathbf{x}_1.e_1 \cos\sigma_1$. But since $\beta_1.\mathsf{lstate} \in \mathcal{I}_{k+n}$, from the definition

of $\mathcal{I}_{k+n}$, $|\mathbf{x}_1.e_1| \leq \epsilon_{k+n}$. Therefore, using the bounds on $\mathbf{x}_1.d$ provided earlier in the proof, we get $|\mathbf{x}_2.e_1| \leq v_{max}\Delta|\sin\sigma_1|+\epsilon_{k+n}|\cos\sigma_1|$. Hence, from Assumption 3(b), $|\mathbf{x}_2.e_1| \leq \epsilon_k$, that is, $F_1(\mathbf{x}_2.s), F_2(\mathbf{x}_2.s) \geq 0$.

Next, we prove that $F_3(\mathbf{x}_2.s), F_4(\mathbf{x}_2.s) \geq 0$. From the definition of $\mathcal{I}_{k+n}$, we know that $-\frac{k_1}{k_2}\mathbf{x}_1.e_1 - \frac{1}{k_2}\phi_{k+n} \leq \mathbf{x}_1.e_2 \leq -\frac{k_1}{k_2}\mathbf{x}_1.e_1 + \frac{1}{k_2}\phi_{k+n}$. From the update rule for e_2, it can be easily shown that $\mathbf{x}_2.e_2 = \mathbf{x}_1.e_2 - \sigma_1$. Thus, we get that $-\frac{k_1}{k_2}\mathbf{x}_1.e_1 - \frac{1}{k_2}\phi_{k+n} - \sigma_1 \leq \mathbf{x}_2.e_2 \leq -\frac{k_1}{k_2}\mathbf{x}_1.e_1 + \frac{1}{k_2}\phi_{k+n} - \sigma_1$. Using the bounds on $\mathbf{x}_2.e_1$, $\mathbf{x}_2.e_2$ and $\mathbf{x}_1.d$, we can derive that $k_1\mathbf{x}_2.e_1 + k_2\mathbf{x}_2.e_2 \leq k_1 v_{max}\Delta\sin|\sigma_1| + k_1\epsilon_{k+n}(1-\cos\sigma_1) + \phi_{k+n} + k_2|\sigma_1|$ and $k_1\mathbf{x}_2.e_1 + k_2\mathbf{x}_2.e_2 \geq -k_1 v_{max}\Delta\sin|\sigma_1| - k_1\epsilon_{k+n}(1-\cos\sigma_1) - \phi_{k+n} - k_2|\sigma_1|$. That is,

$$|k_1\mathbf{x}_2.e_1 + k_2\mathbf{x}_2.e_2| \;\leq\; k_1 v_{max}\Delta\sin|\sigma_1| + k_1\epsilon_{k+n}(1-\cos\sigma_1) + \phi_{k+n} + k_2|\sigma_1|$$

Therefore, Assumption 3(b) guarantees that $|k_1\mathbf{x}_2.e_1 + k_2\mathbf{x}_2.e_2| \leq \phi_k$. That is, $F_3(\mathbf{x}_2.s), F_4(\mathbf{x}_2.s) \geq 0$. In addition, since a main action does not affect v, $F_5(\mathbf{x}_2.s) = F_5(\mathbf{x}_1.s)$ and $F_6(\mathbf{x}_2.s) = F_6(\mathbf{x}_1.s)$, so $F_5(\mathbf{x}_2.s), F_6(\mathbf{x}_1.s) \geq 0$.

Therefore, by definition of $\mathcal{I}_k$, we get $\beta_2.\mathsf{fstate} \in \mathcal{I}_k$. In addition, from the bounds on $\mathbf{x}_1.d$ and $\mathbf{x}_1.e_1$, it can be easily shown that $\beta_2.\mathsf{fstate} \lceil d \geq \lambda_2 - \epsilon_k - v_{max}\Delta$ where λ_2 is the length of the segment $\beta_2.\mathsf{fstate} \lceil seg$.

Next, consider an arbitrary $i \geq 2$ and assume that $\beta_{i-1}.\mathsf{fstate} \in \mathcal{I}_k$ and if $i = 2$ or $i > 2$ and $\beta_{i-1}.\mathsf{fstate} \lceil seg \neq \beta_{i-2}.\mathsf{lstate} \lceil seg$, then $\beta_{i-1}.\mathsf{fstate} \lceil d \geq \lambda_{i-1} - \epsilon_k - v_{max}\Delta$ where λ_{i-1} is the length of the segment $\beta_{i-1}.\mathsf{fstate} \lceil seg$. Simply following the previous proof for $i = 2$, we get $\beta_i.\mathsf{fstate} \in \mathcal{I}_k$ and if $\beta_i.\mathsf{fstate} \lceil seg \neq \beta_{i-1}.\mathsf{lstate} \lceil seg$, then $\beta_i.\mathsf{fstate} \lceil d \geq \lambda_i - \epsilon_k - v_{max}\Delta$ where λ_i is the length of the segment $\beta_i.\mathsf{fstate} \lceil seg$.

By mathematical induction, we conclude the proof that for any $i > 1$, $\beta_i.\mathsf{fstate} \in \mathcal{I}_k$. ■

The next two lemmas show that Assumption 4 is sufficient to guarantee that if a path is changed, then all the assumptions in the Lemma 12 are satisfied.

Lemma 13. *For each state $\mathbf{x}, \mathbf{x}' \in Q$ such that $\mathbf{x}.path \neq \mathbf{x}.new_path$, if $\mathbf{x} \in \mathcal{I}_k$ and $\mathbf{x} \xrightarrow{\mathsf{main}} \mathbf{x}'$, then $\mathbf{x}'.d \geq \lambda - v_{max}\Delta > 0$ where λ is the length of the first segment of $\mathbf{x}.new_path$.*

Proof. Consider an arbitrary execution $\alpha = \tau_0 a_1 \tau_1 a_2 \ldots$. Pick an arbitrary natural number i such that a_i is a main action and let $\mathbf{x} = \tau_{i-1}.\mathsf{lstate}$ and $\mathbf{x}' = \tau_i.\mathsf{fstate}$. We want to show that if $\mathbf{x} \lceil path \neq \mathbf{x} \lceil new_path$, then $\mathbf{x}'.d \geq \lambda - v_{max}\Delta > 0$. Notice that $\mathbf{x}.path \neq \mathbf{x}.new_path$ if and only if there exists a natural number $j < i$ such that a_j is a plan action and for any natural number $k \in \{j+1, \ldots, i-1\}$, a_k is not a main action. Using Assumptions 4(a), we get $\langle \tau_j.\mathsf{fstate} \lceil x, \tau_j.\mathsf{fstate} \lceil y \rangle = p_{i,1}$ where $p_{i,1}$ is the first waypoint in $\mathbf{x}.new_path$. Since main action occurs every Δ time, the time between a_i and a_j is at most Δ. Therefore, from Lemma 2, the definition of F_5 and F_6 and the definition of f_1 and f_2 which describe the evolution of x and y, we see that $\|\langle \mathbf{x}.x, \mathbf{x}.y \rangle - p_{i,1}\| \leq v_{max}\Delta$. Furthermore, from Assumption 3(a), we know that $\lambda = \|p_{i,2} - p_{i,1}\| > v_{max}\Delta + \epsilon_k$ where $p_{i,2}$ is the second waypoint in p_i. Thus, $\mathbf{x}.d \geq \|p_{i,2} - p_{i,1}\| - \|\langle \mathbf{x}.x, \mathbf{x}.y \rangle - p_{i,1}\| \geq \lambda - v_{max}\Delta > 0$.

Lemma 14. *For each state $\mathbf{x}, \mathbf{x}' \in Q$ such that $\mathbf{x}.path \neq \mathbf{x}.new_path$, if $\mathbf{x} \in \mathcal{I}_k$ and $\mathbf{x} \overset{\mathsf{main}}{\rightarrow} \mathbf{x}'$, then $\mathbf{x}' \in \mathcal{I}_k$.*

Proof. Consider an arbitrary execution $\alpha = \tau_0 a_1 \tau_1 a_2 \ldots$. Pick an arbitrary natural number i such that a_i is a main action and let $\mathbf{x} = \tau_{i-1}.\mathsf{lstate}$ and $\mathbf{x}' = \tau_i.\mathsf{fstate}$. We want to show that if $\mathbf{x} \in \mathcal{I}_k$ and $\mathbf{x}.path \neq \mathbf{x}.new_path$, then $\mathbf{x}' \in \mathcal{I}_k$. So suppose $\mathbf{x} \in \mathcal{I}_k$. Notice that $\mathbf{x}.path \neq \mathbf{x}.new_path$ if and only if there exists a natural number $j < i$ such that a_j is a plan action and for any natural number $k \in \{j+1, \ldots, i-1\}$, a_k is not a main action. Let p_{j1} and p_{j2} be the first two waypoints of the new path. Consider a closed execution fragment $\beta = \tau_j a_{j+1} \ldots \tau_{i-1}$. From Assumption 4(a), we get that $p_{j1} = \tau_j.\mathsf{fstate} \lceil \langle x, y \rangle$. Since main action occurs every Δ time, we see that $\beta.\mathsf{ltime} \leq \Delta$. From the differential equations describing the evolution of x and y, we get that

$$|(\tau_j.\mathsf{fstate} \lceil x) - (\mathbf{x}.x)| \leq ((\tau_j.\mathsf{fstate} \lceil v) + a_{max}\Delta)\Delta$$
$$|(\tau_j.\mathsf{fstate} \lceil y) - (\mathbf{x}.y)| \leq \sin\theta_{k,2}((\tau_j.\mathsf{fstate} \lceil v) + a_{max}\Delta)\Delta$$

So from the definition of $\boldsymbol{r}$ in Figure 4, we get that

$$\|\boldsymbol{r}\| \leq (\tau_j.\mathsf{fstate} \lceil v) + a_{max}\Delta)\Delta\sqrt{1 + \sin^2\theta_{k,2}}$$

Using Assumption 4(b), we can conclude that $\|\boldsymbol{r}\| \leq \epsilon_k$. So from the update rule for e_1, $|\mathbf{x}'.e_1| \leq \|\boldsymbol{r}\|$ and so

$$|\mathbf{x}'.e_1| \leq (\tau_j.\mathsf{fstate} \lceil v) + a_{max}\Delta)\Delta\sqrt{1 + \sin^2\theta_{k,2}} \leq \epsilon_k, \tag{28}$$

that is $F_1(\mathbf{x}'.s), F_2(\mathbf{x}'.s) \geq 0$.

Similarly, from the differential equation describing the evolution of θ, we get that

$$|(\tau_j.\mathsf{fstate} \lceil \theta) - (\mathbf{x}.\theta)| \leq \frac{1}{L}\tan\phi_k((\tau_j.\mathsf{fstate} \lceil v) + a_{max}\Delta)\Delta$$

Using condition (1) of Assumption 4(b), we can conclude that

$$\begin{aligned}
|\angle\boldsymbol{p} - (\mathbf{x}.\theta)| &= |(\angle\boldsymbol{p} - (\tau_j.\mathsf{fstate} \lceil \theta)) + ((\tau_j.\mathsf{fstate} \lceil \theta) - (\mathbf{x}.\theta))| \\
&\leq |(\angle\boldsymbol{p}_i - (\tau_j.\mathsf{fstate} \lceil \theta))| + |((\tau_j.\mathsf{fstate} \lceil \theta) - (\mathbf{x}.\theta))| \\
&\leq \frac{\phi_k}{k_2} - \frac{k_1}{k_2}((\tau_j.\mathsf{fstate} \lceil v) + a_{max}\Delta)\Delta\sqrt{1 + \sin^2\theta_{k,2}}
\end{aligned}$$

So we get

$$|k_2\mathbf{x}'.e_2| \leq \phi_k - k_1((\tau_j.\mathsf{fstate} \lceil v) + a_{max}\Delta)\Delta\sqrt{1 + \sin^2\theta_{k,2}}$$

Combining this with (28), we get that

$$|k_1(\mathbf{x}'.e_1) + k_2(\mathbf{x}'.e_2)| \leq |k_1(\mathbf{x}'.e_1)| + |k_2(\mathbf{x}'.e_2)| \leq \phi_k,$$

that is, $F_3(\mathbf{x}'.s), F_4(\mathbf{x}'.s) \geq 0$.

In addition, since main action does not affect v, we see that $F_5(\mathbf{x}'.s) = F_5(\mathbf{x}.s)$ and $F_6(\mathbf{x}'.s) = F_6(\mathbf{x}.s)$, so $F_5(\mathbf{x}'.s), F_6(\mathbf{x}'.s) \geq 0$. Therefore, by definition of $\mathcal{I}_k$, we get that $\mathbf{x}' \in \mathcal{I}_k$. ■

Using the previous three lemmas, the following lemma concludes that an execution fragment which updates the path exactly once by the first main action preserves $\mathcal{I}_k$.

Lemma 15. *Consider a* plan*-free execution fragment* β *starting at a state* $\mathbf{x} \in \mathcal{I}_k$*. If* $\mathbf{x}.path \neq \mathbf{x}.new_path$*, then* $\beta.\mathsf{lstate} \in \mathcal{I}_k$*.*

Proof. β can be written as $\beta = \beta_1 \mathsf{main} \beta_2$ where $\beta_1 = \tau_0 \mathsf{brake} \tau_1 \mathsf{brake} \ldots \tau_n$ and β_2 is a plan-free execution fragment with $\beta_2.\mathsf{fstate} \lceil path = \beta_2.\mathsf{fstate} \lceil new_path$. Clearly, $\beta_1.\mathsf{lstate} \lceil path \neq \beta_1.\mathsf{lstate} \lceil new_path$. In addition, $\beta_1.\mathsf{fstate} \in \mathcal{I}_k$ and thus, from Theorem 2, $\beta_1.\mathsf{lstate} \in \mathcal{I}_k$. Applying Lemma 13 and Lemma 14, we see that $\beta_2.\mathsf{fstate} \lceil d \geq \lambda_1 - v_{max}\Delta \geq \lambda_1 - \epsilon_k - v_{max}\Delta$ and $\beta_2.\mathsf{fstate} \in \mathcal{I}_k$ where λ_1 is the length of the first segment of $\mathbf{x}.new_path$. Therefore, from Lemma 12, $\beta.\mathsf{lstate} \in \mathcal{I}_k$.

Now, we establish an invariance of $\mathcal{I}_k$.

Theorem 3. *Suppose the initial state* $\mathbf{x}_0 \in \mathcal{I}_k$ *and* $\mathbf{x}_0.d \geq \lambda_1 - \epsilon_k - v_{max}\Delta$ *where* λ_1 *is the length of the first segment of the initial path. Then,* $\mathcal{I}_k$ *is an invariant of* $\mathcal{A}$*.*

Proof. Any execution α can be written as $\alpha = \beta_1 \mathsf{plan} \beta_2 \mathsf{plan} \ldots$ where β_1 is a plan-free execution fragment with $\beta_1.\mathsf{fstate} \lceil path = \beta_1.\mathsf{fstate} \lceil new_path$ and for any $i \geq 2$, β_i is a plan-free execution fragment with $\beta_i.\mathsf{fstate} \lceil path \neq \beta_i.\mathsf{fstate} \lceil new_path$. Since plan action does not affect the variable s, if $\beta_1.\mathsf{lstate} \in \mathcal{I}_k$, then $\beta_2.\mathsf{fstate} \in \mathcal{I}_k$ and using Lemma 15, we get that for any $i \geq 2$, $\beta_i.\mathsf{lstate} \in \mathcal{I}_k$. Thus, we only need to show that $\beta_1.\mathsf{lstate} \in \mathcal{I}_k$. But this is true from Lemma 12 since $\beta_1.\mathsf{fstate} \lceil d = \mathbf{x}_0.d \geq \lambda_1 - \epsilon_k - v_{max}\Delta$ and $\beta_1.\mathsf{fstate} \in \mathcal{I}_k$.

Since for any state $\mathbf{x} \in \mathcal{I}_k$, $|\mathbf{x}.e_1| \leq \epsilon_k \leq e_{max}$, invariance of $\mathcal{I}_k$ guarantees the safety property (A). For property (C), we note that for any state $\mathbf{x} \in \mathcal{I}_k$, there exists $v_{min} > 0$ such that $\mathbf{x}.v \geq v_{min} > 0$ and $|\mathbf{x}.e_2| \leq \theta_{k,2} < \frac{\pi}{2}$, that is, $\dot{d} = f_7(\mathbf{x}.s, u) \leq -v_{min} \cos\theta_{k,2} < 0$ for any $u \in \mathcal{U}$. Thus, it follows that the waypoint distance decreases and the vehicle makes progress towards its waypoint.

References

1. R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138(1):3–34, 1995.
2. N. P. Bhatia and G. P. Szegö. *Dynamical Systems: Stability Theory and Applications*, volume 35 of *Lecture notes in mathematics*. Springer-Verlag, Berlin; New York, 1967.

3. C. W. Brown. Qepcad b: a program for computing with semi-algebraic sets using cads. *SIGSAM Bull.*, 37(4):97–108, 2003.
4. J. W. Burdick, N. DuToit, A. Howard, C. Looman, J. Ma, R. M. Murray, and T. Wongpiromsarn. Sensing, navigation and reasoning technologies for the DARPA Urban Challenge. Technical report, DARPA Urban Challenge Final Report, 2007.
5. N. E. DuToit, T. Wongpiromsarn, J. W. Burdick, and R. M. Murray. Situational reasoning for road driving in an urban environment. In *International Workshop on Intelligent Vehicle Control Systems (IVCS)*, 2008.
6. T. A. Henzinger, P. W. Kopke, A. Puri, and P. Varaiya. What's decidable about hybrid automata? In *ACM Symposium on Theory of Computing*, pages 373–382, 1995.
7. D. K. Kaynar, N. Lynch, R. Segala, and F. Vaandrager. *The Theory of Timed I/O Automata*. Synthesis Lectures on Computer Science. Morgan Claypool, November 2005. Also available as Technical Report MIT-LCS-TR-917.
8. G. Lafferriere, G. J. Pappas, and S. Yovine. A new class of decidable hybrid systems. In *In Hybrid Systems : Computation and Control*, pages 137–151. Springer, 1999.
9. N. Lynch, R. Segala, and F. Vaandrager. Hybrid I/O automata. *Information and Computation*, 185(1):105–157, August 2003.
10. S. Mitra. *A Verification Framework for Hybrid Systems*. PhD thesis, Massachusetts Institute of Technology, Cambridge, MA 02139, September 2007.
11. S. Mitra, Y. Wang, N. Lynch, and E. Feron. Safety verification of model helicopter controller using hybrid Input/Output automata. In O. Maler and A. Pnueli, editors, *HSCC*, volume 2623 of *LNCS*, pages 343–358. Springer, 2003.
12. P. Prabhakar, V. Vladimerou, M. Viswanathan, and G. E. Dullerud. A decidable class of planar linear hybrid systems. In *Hybrid Systems: Computation and Control, 11th International Workshop, HSCC 2008, St. Louis, MO, USA, April 22-24, 2008. Proceedings*, volume 4981 of *LNCS*, pages 401–414. Springer, 2008.
13. S. Prajna, A. Papachristodoulou, and P. A. Parrilo. Introducing sostools: A general purpose sum of squares programming solver. In *In Proceedings of the 41st IEEE Conf. on Decision and Control*, pages 741–746, 2002.
14. V. Vladimerou, P. Prabhakar, M. Viswanathan, and G. E. Dullerud. Stormed hybrid systems. In *ICALP (2)*, volume 5126 of *LNCS*, pages 136–147. Springer, 2008.
15. T. Wongpiromsarn and R. M. Murray. Distributed mission and contingency management for the DARPA urban challenge. In *International Workshop on Intelligent Vehicle Control Systems (IVCS)*, 2008.

A Vehicle||Controller as a PCHA

Here we show that the composed automaton $\mathcal{A} = \mathsf{Vehicle}\|\mathsf{Controller}$ is a periodically controlled hybrid automaton. We define an automaton $\mathcal{A}'$ that is identical to $\mathcal{A}$ except that its variables, actions, and transition functions are renamed to match the definition of the generic PCHA of Figure 1.

Variables. $\mathcal{A}'$ has the following variables.

– a continuous variable $s \triangleq \langle x, y, \theta, v, e_1, e_2, d \rangle$ of type $\mathcal{X} = \mathbb{R}^7$.

- a discrete state variable $loc \triangleq \langle brake, path, seg \rangle$ of type $\mathcal{L} = \texttt{Tuple}[\{On, Off\}, \texttt{Seq}[\mathbb{R}^2], \mathbb{N}]$.
- a control variable is $u = \langle a, \phi \rangle$ of type $\mathcal{U} = \mathbb{R}^2$.
- two command variables $z_1 \triangleq brake$ of type $\mathcal{Z}_1 = \{On, Off\}$ and $z_2 = path$ of type $\mathcal{Z}_2 = \texttt{Seq}[\mathbb{R}^2]$.

Actions and transitions. $\mathcal{A}$ has two input update actions, $\mathsf{brake}(b)$ and $\mathsf{plan}(p)$, and the command variables z_1 and z_2 store the values b and p, respectively, when these actions occur.

An internal control action main occurs every Δ time, starting from time 0. That is, values of Δ_1 and Δ_2 as defined in a generic PCHA are $\Delta_1 = \Delta$ and $\Delta_2 = 0$. The control law function g and the state transition function h of $\mathcal{A}$ can be derived from the specification of main action in Figure 4. Let $g = \langle g_a, g_\phi \rangle$ where $g_a : \mathcal{L} \times \mathcal{X} \to \mathbb{R}$ and $g_\phi : \mathcal{L} \times \mathcal{X} \to \mathbb{R}$ represent the control law for a and ϕ, respectively, and are given by

$$g_a(l, s) = \begin{cases} a_{brake} & \text{if } l.brake = On \\ a_{max} & \text{if } l.brake = Off \ \wedge \ s_0.v < v_T \\ 0 & \text{otherwise} \end{cases}$$

$$g_\phi(l, s) = \frac{\phi_d}{|\phi_d|} \min(\delta \times s.v, |\phi_d|)$$

where $\phi_d = -k_1 s.e_1 - k_2 s.e_2$. Let $h = \langle h_{s,1}, \ldots, h_{s,7}, h_{l,1}, h_{l,2}, h_{l,3} \rangle$ where $h_{s,1}, \ldots, h_{s,7} : \mathcal{L} \times \mathcal{X} \times \mathcal{Z}_1 \times \mathcal{Z}_2 \to \mathbb{R}$ describe the discrete transition of x, y, θ, v, e_1, e_2 and d components of s, respectively, and $h_{l,1} : \mathcal{L} \times \mathcal{X} \times \mathcal{Z}_1 \times \mathcal{Z}_2 \to \{On, Off\}$, $h_{l,2} : \mathcal{L} \times \mathcal{X} \times \mathcal{Z}_1 \times \mathcal{Z}_2 \to \texttt{Seq}[\mathbb{R}^2]$ and $h_{l,3} : \mathcal{L} \times \mathcal{X} \times \mathcal{Z}_1 \times \mathcal{Z}_2 \to \mathbb{N}$ describe the discrete transition of *brake*, *path* and *seg*, respectively. Then, the function h is given by

$$h_{s,1}(l, s, z_1, z_2) = s.x, \ \ h_{s,2}(l, s, z_1, z_2) = s.y$$

$$h_{s,3}(l, s, z_1, z_2) = s.v, \ \ h_{s,4}(l, s, z_1, z_2) = s.\theta$$

$$h_{s,5}(l, s, z_1, z_2) = \begin{cases} s.e_1 & \text{if } l.path = z_2 \ \wedge \ s.d > 0 \\ \frac{1}{\|\boldsymbol{q}\|} \boldsymbol{q} \cdot \boldsymbol{r} & \text{otherwise} \end{cases}$$

$$h_{s,6}(l, s, z_1, z_2) = \begin{cases} s.e_2 & \text{if } l.path = z_2 \ \wedge \ s.d > 0 \\ s.\theta - \angle \boldsymbol{p} & \text{otherwise} \end{cases}$$

$$h_{s,7}(l, s, z_1, z_2) = \begin{cases} s.d & \text{if } l.path = z_2 \ \wedge \ s.d > 0 \\ \frac{1}{\|\boldsymbol{p}\|} \boldsymbol{p} \cdot \boldsymbol{r} & \text{otherwise} \end{cases}$$

$$h_{l,1}(l, s, z_1, z_2) = z_1, \ \ h_{l,2}(l, s, z_1, z_2) = z_2$$

$$h_{l,3}(l, s, z_1, z_2) = \begin{cases} 1 & \text{if } l.path \neq z_2 \\ l.seg + 1 & \text{if } l.path = z_2 \ \wedge \ s.d \leq 0 \\ l.seg & \text{otherwise} \end{cases}$$

where the temporary variable $\boldsymbol{p}$, $\boldsymbol{q}$ and $\boldsymbol{r}$ are computed as in the Controller specification based on the updated value of *path* and *seg*.

Trajectories. From the the state models of Vehicle and Controller automata specified on line 14 of Figure 3 and lines 48-50 of Figure 4, we see that $\mathcal{A}$ only has one state model. For any value of $l \in \mathcal{L}$, the continuous state s evolves according to the differential equation $\dot{s} = f(s, u)$ where $f = \langle f_1, f_2, \ldots, f_7 \rangle$ and $f_1, \ldots, f_7 : \mathcal{X} \times \mathcal{U} \to \mathbb{R}$ are associated with the evolution of the x, y, θ, v, e_1, e_2 and d components of s, respectively. Using the definition of the control law function g defined above, we can derive the following components of $f(s, g(l, s_0))$:

$$
\begin{aligned}
& f_1(s, g(l, s_0)) = s.v \cos(s.\theta), \;\; f_2(s, g(l, s_0)) = s.v \sin(s.\theta) \\
& f_3(s, g(l, s_0)) = f_6(s, g(l, s_0)) = \frac{s.v}{L} \tan(\frac{\phi_d}{|\phi_d|} \min(|\phi_d|, \delta s_0.v, \phi_{max})) \\
& f_4(s, g(l, s_0)) = \begin{cases} a_{brake} & \text{if } l.brake = On \;\wedge\; s.v > 0 \\ a_{max} & \text{if } l.brake = Off \;\wedge\; s_0.v < v_T \\ 0 & \text{otherwise} \end{cases} \\
& f_5(s, g(l, s_0)) = s.v \sin(s.e_2) \\
& f_7(s, g(l, s_0)) = -s.v \cos(s.e_2)
\end{aligned}
$$

where $\phi_d = -k_1 s_0.e_1 - k_2 s_0.e_2$.