Controller design under safety specifications for a class of bounded hybrid automata

Controller design under safety specifications for a class of bounded hybrid automata

Daniel Hoehener* Domitilla Del Vecchio†

October 16, 2016

Abstract

Motivated by driver-assist systems that warn the driver before taking control action, we study the safety problem for a class of bounded hybrid automata. We show that for this class there exists a least restrictive safe feedback controller that has a simple structure and can be computed efficiently online. The theoretical results are then used to design driver-assist systems for rear-end and merging collision scenarios.

1 INTRODUCTION

Driving a motor vehicle still presents with more than 1.5 million injuries in 2013 an important health risk. While a significant decrease in fatalities was achieved from 1975-2007 thanks to passive safety systems such as anti-lock braking systems, seat belts, etc., the number of fatalities remained stagnant over the last ten years, [1]. This, together with advances in sensing and communication technology, led to a shift from passive to active safety systems, such as forward collision warning and lane keeping systems. These features have large potential benefits, for instance it is estimated that forward collision warning systems could prevent more than 90% of all injuries resulting from rear-end crashes [2]. The complexity of active safety systems creates however the need for advanced tools for formal verification of safety specifications, [6].

Using the theory of hybrid automata it was that one can define controllers of hybrid systems that satisfy given safety specifications, see [8] and the references therein. Such controllers are called provably safe. Ideally, provably safe controllers should also be least restrictive, which means in the context of a driver-assist system that the controller constrains the possible actions of the human driver as little as possible. Due to the computational complexity of the task, the design of provably safe, least restrictive controllers remains a challenge and can in general only be done approximately, see for instance [9, 3, 11]. However it has been shown that a number of ground transportation systems have the so-called input-output order preserving property, in which case exact solutions are possible, see [4, 12, 5] and the references therein. The main focus of this paper is the extension of these results to hybrid automata that have both controlled and uncontrolled mode transitions, continuous control and disturbance inputs and possibly non-zero dwell time. For this purpose we introduce bounded hybrid automata which,

*Department of Mechanical Engineering, MIT, 77 Massachusetts Avenue, Cambridge, MA
†Department of Mechanical Engineering, MIT, 77 Massachusetts Avenue, Cambridge, MA

similar to order-preserving continuous systems, admit enveloping output trajectories. We show that for the class of bounded hybrid automata there exists a provably safe and least restrictive feedback controller that can be computed efficiently online. We also provide sufficient conditions for boundedness of a hybrid automaton. The results are illustrated with two application examples. The first example is a forward collision avoidance system that is allowed to override the driver to avoid a collision but only after first warning the driver and allowing for a delay between warning and override. The second example is concerned with a similar collision avoidance system but for the case of a two vehicle collision scenario at a traffic merging.
The application examples are described in detail in Section 2. The mathematical model is introduced in Section 3 followed by the solution algorithm in Section 4. A class of bounded hybrid automata is presented in Section 5 and numerical results are provided in Sections 6.

2 MOTIVATING EXAMPLES

2.1 Forward collision avoidance with warning

Consider two vehicles as illustrated in Fig. 1, where the following vehicle (FV) is equipped with a driver-assist system. FV uses on-board sensors in order to measure its own velocity, as well as relative position and speed of the lead vehicle (LV). This system has three states, x_r the relative position of LV with respect to FV, v_f the velocity of FV and LV's velocity v_l. Using standard longitudinal dynamics for FV, where ι_f denotes actuation input, and considering the acceleration d_l of LV as a bounded disturbance, i.e. $d_l \in [d_l^\ell, d_l^u]$, the dynamics of this system are given by

$$\begin{pmatrix} \dot{x}_r \\ \dot{v}_f \\ \dot{v}_l \end{pmatrix} = \begin{pmatrix} v_l - v_f \\ \iota_f - Av_f^2 - a_{rs} \\ d_l \end{pmatrix} =: \bar{f}^{FC}(x_r, v_f, v_l, \iota_f, d_l), \tag{1}$$

where A represents air drag and a_{rs} incorporates deceleration due to rolling resistance and slope of the road, see [10].

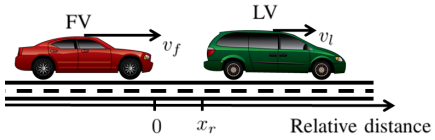


Figure 1: Following vehicle (FV) and lead vehicle (LV) in the corresponding coordinate frame.

A forward collision occurs in this context when

$$x_r \in]-\infty, b_{FC}[=: B_{FC}, \tag{2}$$

where $b_{FC} > 0$ represents the minimum allowed separation between the vehicles. The driver-assist system operating on FV has the capability of overriding the human driver's input d_f, with its own actuation input u_f, i.e. the actuation input ι_f of FV is d_f unless the driver is overridden by the driver-assist system in which case it is u_f. We require that the driver-assist system can override the

driver only after 1) issuing a warning; 2) allowing for a fixed reaction time T_{RT}; 3) driver disobeys the warning. Disobeying the warning here means that the driver's input is outside a given range D_W. More formally, the system has three modes of operation, inactive, warned and override, see Fig. 2. The system dynamics change in every mode in the sense that the input ι_f comes either from the human driver, in which case it is modeled as a bounded disturbance or the input comes from the driver-assist system and represents a control. The switch from inactive to warned is controlled by the driver-assist system while warned to override depends on the driver's input and is uncontrolled. Finally, to ensure that the driver has time T_{RT} to react to the warning, the system has to remain for at least T_{RT} in the warned mode, i.e. the warned mode has a minimum *dwell time* ω_m of T_{RT}. Assuring that x_r will never enter B_{FC} is therefore a safety problem for a hybrid automaton with controlled and uncontrolled mode transitions and non zero minimum dwell time. In this paper we present an approach that allows to find a control strategy for such a hybrid automaton that guarantees safety and overrides the driver as late as possible.

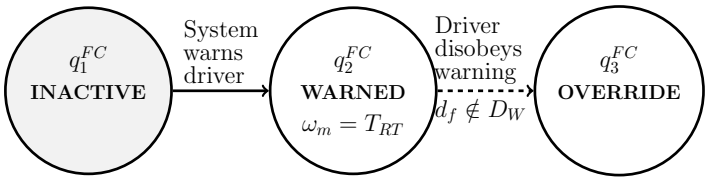


Figure 2: Finite state machine corresponding to the modes of operation of the forward collision avoidance system with events that trigger the mode transitions. The mode WARNED has minimum dwell time $\omega_m > 0$.

2.2 Two vehicle conflict resolution with warning

Consider a two vehicle conflict scenario, see Fig. 3, where the incubant vehicle (IV) follows the main road and the entering vehicle (EV) merges into that road. Modeling the dynamics of both vehicles using standard longitudinal dynamics, see above, we have a system with four states, the position along the path of both IV and EV denoted by x_i and x_e and the corresponding velocities given by v_i and v_e. Moreover, each of the vehicles has an independent actuation input denoted by ι_i and ι_e respectively. Defining

$$\bar{f}^{MC}(x, v, \iota) = (v, \iota - Av^2 - a_{rs})^T, \tag{3}$$

where A and a_{rs} are defined as above, the complete system dynamics are given by

$$(\dot{x}_i, \dot{v}_i, \dot{x}_e, \dot{v}_e) = (\bar{f}^{MC}(x_i, v_i, \iota_i)^T, \bar{f}^{MC}(x_e, v_e, \iota_e)^T).$$

A collision occurs when both vehicles are in the merging zone at the same time which can be formalized as

$$(x_i, x_e) \in]b_i^\ell, b_i^u[\times]b_e^\ell, b_e^u[=: B_{MC},$$

where the intervals $]b_i^\ell, b_i^u[$, $]b_e^\ell, b_e^u[$ represent the location of the merging zone along IV's and EV's path. Here we are assuming that there exists an intelligent roadside infrastructure which communicates with both vehicles and has the possibility to override each vehicle individually. As in the previous section we

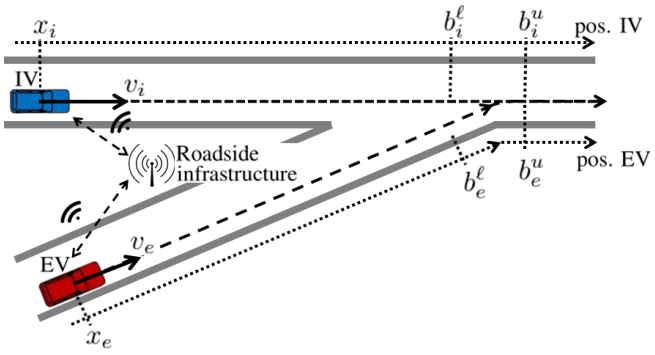


Figure 3: Incubant vehicle IV and entering vehicle EV in the corresponding coordinate frame. The conflict area is given by the set $]b_i^\ell, b_i^u[\times]b_e^\ell, b_e^u[$.

require that the system can override a driver only after 1) issuing a warning; 2) allowing for a fixed reaction time T_{RT}; 3) driver disobeys the warning. Both vehicles can therefore be seen as independent hybrid automata with modes of operation as those depicted in Fig. 2. The main difference to the previous case is that both vehicles have to pass a conflict zone and therefore there are two orders of passage, IV before EV and the other way around. Since it is desirable that the driver-assist system announces its plan to the drivers, we require in addition to 1)-3) that if the systems warns or overrides at least one driver then it has to be able to guarantee a fixed order of passage. This last requirement corresponds to assuring the avoidance of at least one of the sets

$$B_{MC}^{\ell u} \coloneqq]b_i^\ell, \infty[\times]-\infty, b_e^u[, \quad \text{and} \quad B_{MC}^{u\ell} \coloneqq]-\infty, b_i^u[\times]b_e^\ell, \infty[. \tag{4}$$

That is, the driver-assist system should choose the less restrictive order of passage and then guarantee this order independent of what the drivers do. This problem can be formulated as a safety problem on a parallel composition of hybrid automata. Formal definitions and a computationally efficient solution are provided in the following sections.

3 MATHEMATICAL MODEL AND PROBLEM STATEMENT

In this section we provide the formal problem statement. We start with few preliminary notions then provide the main system model and end the section with the problem statement and an illustration on the motivating examples.

3.1 Preliminaries

Throughout this paper $n, m, s \in \mathbb{N}$ stand for natural numbers and for a map $f\colon X \to Y$ we abbreviate $f(X) \coloneqq \{f(x) \mid x \in X\}$. Similarly, if $F\colon X \rightsquigarrow Y$ is a set-valued map we write $F(X) \coloneqq \bigcup_{x\in X} F(x)$. The sets of piecewise continuous and continuous signals with images in Y are denoted by $\mathcal{S}(Y)$ and $\mathcal{C}(Y)$ respectively.
Partially ordered sets play an important role in this paper. Their definition is recalled next.

Definition 1. A tuple $(S, \preceq)$ is a *partially-ordered set* if for all $s_1, s_2, s_3 \in S$ we have i) $s_1 \preceq s_1$; ii) $s_1 \preceq s_2$ and $s_2 \preceq s_1$ implies that $s_1 = s_2$; iii) $s_1 \preceq s_2$ and $s_2 \preceq s_3$ implies that $s_1 \preceq s_3$.

Definition 2. Let $(S, \preceq)$ be a partially ordered subset of a Euclidean and $\Delta \subset S$ be a closed, convex, pointed cone. The partial order $\preceq$ is *induced* by Δ if for all $s_1, s_2 \in S$,

$$s_1 \preceq_\Delta s_2 \iff s_2 - s_1 \in \Delta.$$

If a partial order is induced by a cone Δ we use the abbreviations

$$\begin{aligned} [\![s, \infty]\!] &\coloneqq s + \Delta, \quad [\![-\infty, s]\!] \coloneqq s - \Delta, \\ [\![s_1, s_2]\!] &\coloneqq (s_1 + \Delta) \cap (s_2 - \Delta). \end{aligned} \tag{5}$$

Example 1. The component-wise partial order on $\mathbb{R}^n$ is induced by the cone $\mathbb{R}^n_+$. Moreover, for any partially ordered set $(S, \preceq)$, $(\mathcal{S}(S), \preceq')$ is a partially ordered set where for all $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{S}(S)$,

$$\mathbf{x}_1 \preceq' \mathbf{x}_2 \iff \mathbf{x}_1(t) \preceq \mathbf{x}_2(t) \; \forall t \in \mathbb{R}_+.$$

Notice also that if $\preceq$ is an induced partial order then the same is true for $\preceq'$.

In the rest of the paper, unless indicated otherwise, all partial orders are denoted by $\preceq$. Next we introduce hybrid trajectories.

Definition 3. A *hybrid time trajectory* $\tau = \{I_j\}_{j=0}^N$ is a finite or infinite sequence of intervals in $\mathbb{R}_+$ such that

i) $I_j = [\tau_j, \tau'_j]$ for $j < N$ and if $N < \infty$, $I_N = [\tau_N, \tau'_N]$ or $I_N = [\tau_N, \tau'_N[$;

ii) for all $j < N$, $\tau_j \leq \tau'_j = \tau_{j+1}$.

The set of all hybrid time trajectories is denoted by $\mathcal{T}$. The number of intervals in the sequence $\tau \in \mathcal{T}$ is denoted by $\langle \tau \rangle$ for and $t \in \mathbb{R}_+$, $t \in \tau$ abbreviates that there exists $j \in \mathbb{N}$ such that $t \in I_j$. Each $\tau \in \mathcal{T}$ is linearly ordered, i.e. $t \preceq t'$ for $t \in I_k$ and $t' \in I_l$ if $k \leq l$ and $t \leq t'$. As we work here with autonomous dynamics, without loss of generality we make the convention that $\tau_0 = 0$.

Definition 4. Let the set S be given. A *hybrid trajectory* in S is a tuple $(\tau, \mathbf{z})$ where $\tau = \{I_j\}_{j=0}^N \in \mathcal{T}$ and $\mathbf{z} = \{\mathbf{z}_j\}_{j=0}^N$ is a family of signals such that for all j, $\mathbf{z}_j \colon I_j \to S$. The set of all hybrid trajectories in S is $\mathcal{HT}(S)$.

For $(\tau, \mathbf{z}) \in \mathcal{HT}(S)$, $\mathbf{z}(t) \coloneqq \{\mathbf{z}_j(t) \mid t \in I_j\}$. We end by defining continuous hybrid trajectories.

Definition 5. Let the set S be given. The hybrid trajectory $(\tau, \mathbf{z}) \in \mathcal{HT}(S)$ is *continuous* if for every $t \in \mathbb{R}_+$,

i) $\mathbf{z}(t)$ is a singleton;

ii) for $z \in \mathbf{z}(t)$ and all $\epsilon > 0$ there exists $\delta > 0$ such that for all $t' \in]t - \delta, t + \delta[\cap \mathbb{R}_+$ and $z' \in \mathbf{z}(t')$, $\|z - z'\| < \epsilon$.

Remark 1. With every continuous hybrid trajectory $(\tau, \mathbf{z}) \in \mathcal{HT}(S)$ one can associate a continuous signal $\tilde{\mathbf{z}} \colon \mathbb{R}_+ \to S$ such that $\{\tilde{\mathbf{z}}(t)\} = \mathbf{z}(t)$ for all $t \in \mathbb{R}_+$.

3.2 Hybrid system model

As mathematical model we use a hybrid automaton with dwell time defined as follows.

Definition 6. A *hybrid automaton* with dwell time is a collection $H = (Q, X, Y, \mathcal{E}, U, D, R, f, \mathrm{Inv}, G, h)$ where Q is a finite set of discrete *modes*, $X \subset \mathbb{R}^n$ is the continuous *state space*, $Y \subset \mathbb{R}^r$ is the *output space*, $\mathcal{E} \subset Q \times Q$ represents the set of *discrete control inputs*, $U \subset \mathbb{R}^m$ is the set of *continuous control inputs*, $D \subset \mathbb{R}^s$ is the set of *disturbance inputs*, $R\colon Q \times \mathcal{E} \to Q$ is the *mode reset map*, $f\colon Q \times X \times U \times D \to X$ are the continuous *system dynamics*, $\mathrm{Inv}\colon Q \rightsquigarrow \mathbb{R}_+ \times D$ is a set-valued map with open images that represent the *invariance set*, $G\colon Q \rightsquigarrow \mathcal{E}$ is set-valued and represents a *guard condition* and $h\colon X \to Y$ is the *output map*.

Throughout this paper H denotes a hybrid automaton and Q, X, Y, $\mathcal{E}$, U, D, R, f, Inv, G, h are its components.

Definition 7. An *execution* of the hybrid automaton H starting at $(\omega, q, x) \in \mathbb{R}_+ \times Q \times X$ is a hybrid trajectory $(\tau, \mathbf{w}, \mathbf{q}, \mathbf{x}, \mathbf{y}, \mathbf{e}, \mathbf{u}, \mathbf{d}) \in \mathcal{HT}(\mathbb{R}_+ \times Q \times X \times Y \times \mathcal{E} \times U \times D)$ such that

i) $(\mathbf{w}(0), \mathbf{q}(0), \mathbf{x}(0)) = (\omega, q, x)$;

ii) For all j such that $\tau_j < \tau'_j$, $\mathbf{q}_j$ and $\mathbf{e}_j$ are constant and

$$\begin{pmatrix} \dot{\mathbf{w}}_j(t) \\ \dot{\mathbf{x}}_j(t) \end{pmatrix} = \begin{pmatrix} 1 \\ f(\mathbf{q}_j(t), \mathbf{x}_j(t), \mathbf{u}_j(t), \mathbf{d}_j(t)) \end{pmatrix} \quad \forall t \in I_j,$$
$$(\mathbf{w}_j(t), \mathbf{d}_j(t)) \in \mathrm{Inv}(\mathbf{q}_j(t)) \quad \forall t \in [\tau_j, \tau'_j[;$$

iii) For all $j > 0$, $\mathbf{q}_j(\tau_j) = R(\mathbf{q}_{j-1}(\tau_{j-1}), \mathbf{e}_j(\tau_j))$, $(\mathbf{w}_j(\tau_j), \mathbf{x}_j(\tau_j)) = (0, \mathbf{x}_{j-1}(\tau'_{j-1}))$ and either $\Big(\mathbf{w}_{j-1}(\tau'_{j-1}), \mathbf{d}_j(\tau_j)\Big) \notin \mathrm{Inv}(\mathbf{q}_{j-1}(\tau'_{j-1}))$ or $\mathbf{e}_j(\tau_j) \in G(\mathbf{q}(\tau'_{j-1}))$;

iv) For all j, $\mathbf{y}_j(t) = h(\mathbf{x}_j(t))$ for all $t \in I_j$.

The *hybrid state space* is $\mathcal{X} \coloneqq \mathbb{R}_+ \times Q \times X$ and we denote its elements by $\xi \coloneqq (\omega, q, x) \in \mathcal{X}$. Each component of an execution χ is a hybrid trajectory and we write $(\tau, \mathbf{w})$ for *dwell time*, $(\tau, \mathbf{q})$ and $(\tau, \mathbf{x})$ denote the discrete and continuous state trajectory respectively. The output trajectory is $(\tau, \mathbf{y})$ and discrete, continuous and disturbance inputs are denoted by $(\tau, \mathbf{e})$, $(\tau, \mathbf{u})$ and $(\tau, \mathbf{d})$. The set of executions of H is denoted by $\mathscr{H}$ and $\mathscr{H}(\xi) \subset \mathscr{H}$ is the set of executions starting at $\xi \in \mathcal{X}$. Moreover, if $\bar{\chi} \in \mathscr{H}$ then its components are also denoted with a bar, i.e. $\bar{\chi} = (\bar{\tau}, \bar{\mathbf{w}}, \bar{\mathbf{q}}, \bar{\mathbf{x}}, \bar{\mathbf{y}}, \bar{\mathbf{e}}, \bar{\mathbf{u}}, \bar{\mathbf{d}})$. We use an analogous convention for χ^*, χ', etc.

Definition 8. Let the controlled hybrid automata $H^j = (Q^j, X^j, Y^j, \mathcal{E}^j, U^j, D^j, R^j, f^j, \mathrm{Inv}^j, G^j, h^j)$, $j \in \{1, 2\}$, be given. Their *parallel composition* $H \coloneqq H^1 \parallel H^2$ is defined as the collection $H = (Q, X, Y, \mathcal{E}, U, D, R, f, \mathrm{Inv}, G, h)$ where $S = S^1 \times S^2$ for $S \in \{Q, X, Y, \mathcal{E}, U, D\}$ and $g = (g^1, g^2)^T$ for $g \in \{R, f, \mathrm{Inv}, G, h\}$.

3.3 Controllers

We assume that the controller observes the hybrid state space $\mathcal{X}$ fully.

Definition 9. A *feedback controller* for H is a set-valued map $\pi\colon \mathcal{X} \rightsquigarrow \mathcal{E} \times U$. The set of *closed loop causal executions* is

$$\mathscr{H}_\pi \coloneqq \Big\{(\tau, \mathbf{w}, \mathbf{q}, \mathbf{x}, \mathbf{y}, \mathbf{e}, \mathbf{u}, \mathbf{d}) \in \mathscr{H} \;\Big|\; \forall j \in \{0, \dots, \langle\tau\rangle\},$$
$$(\mathbf{e}_{j+1}(t), \mathbf{u}_{j+1}(t)) \in \pi(\mathbf{w}_j(t), \mathbf{q}_j(t), \mathbf{x}_j(t)) \text{ if } t \in \tilde{I}_j \text{ and } (e^0, \mathbf{u}_j(t)) \in \pi(\mathbf{w}_j(t), \mathbf{q}_j(t), \mathbf{x}_j(t)) \; \forall t \in I_j \setminus \tilde{I}_j \Big\},$$

where $\tilde{I}_j = \{\tau_j'\}$ if $(\mathbf{q}_j(\tau_j'), \mathbf{q}_{j+1}(\tau_{j+1})) \in \mathcal{E}$ and $\tilde{I}_j = \emptyset$ otherwise. Moreover, $e^0 \in \mathcal{E}$ is a void input without influence on the dynamics. The set of feedback controllers of H is $\mathscr{F}$.

Remark 2. The focus of this paper are safety problems, see Section 3.5. In this context the restriction to feedback controllers rather than controllers that depend on the entire state history is not restrictive as was shown in [8, Prop. 2].

It is also useful to define for any $\bar{\mathscr{H}} \subset \mathscr{H}$ and any $(\tau, \bar{\mathbf{d}}) \in \mathcal{HT}(D)$ the set

$$\bar{\mathscr{H}}^{\bar{\mathbf{d}}} \coloneqq \left\{(\tau, \mathbf{w}, \mathbf{q}, \mathbf{x}, \mathbf{y}, \mathbf{e}, \mathbf{u}, \mathbf{d}) \in \bar{\mathscr{H}} \;\middle|\; \forall j \in \{0, \dots, \langle\tau\rangle\}, \mathbf{d}_j(t) = \bar{\mathbf{d}}_j(t) \; \forall t \in I_j\right\}.$$

3.4 Properties of hybrid automata

Definition 10. Let H and $\pi \in \mathscr{F}$ be given. Then π has *continuous executions* if i) for all $\chi \in \mathscr{H}_\pi$, $(\tau, \mathbf{y})$ is continuous; ii) for all $(\omega, q, x) \in \mathcal{X}$, $\chi \in \mathcal{H}_\pi(\omega, q, x)$, all $t \in \mathbb{R}_+$ and $\epsilon > 0$ there exists $\delta > 0$ such that for all $(\tilde{\omega}, \tilde{x})$ satisfying $\|(\omega, x) - (\tilde{\omega}, \tilde{x})\| \leq \delta$ there exists $\tilde{\chi} \in \mathscr{H}_\pi(\tilde{\omega}, q, \tilde{x})$ such that $\|\mathbf{y}(t) - \tilde{\mathbf{y}}(t)\| \leq \epsilon$.

Intuitively a continuous hybrid automaton has outputs that depend continuously on the initial condition and on time. Notice that by Remark 1 we can consider the outputs of continuous hybrid systems as elements of $\mathcal{C}(Y)$.

Definition 11. Let H be given. Then H is *uniformly tightly bounded with respect to control* if $(Y, \preceq)$ has an induced partial order and there exist $\pi^\ell, \pi^u \in \mathscr{F}$ with continuous executions such that for all $\xi \in \mathcal{X}$, $(\tau, \mathbf{d}) \in \mathcal{HT}(D)$ and all $\chi \in \mathscr{H}^{\mathbf{d}}(\xi)$, $\chi^\ell \in \mathscr{H}^{\mathbf{d}}_{\pi^\ell}(\xi)$, $\chi^u \in \mathscr{H}^{\mathbf{d}}_{\pi^u}(\xi)$ we have that $\mathbf{y}^\ell(t) \preceq \mathbf{y}(t) \preceq \mathbf{y}^u(t)$ for all $t \in \mathbb{R}_+$.

Definition 12. Let the hybrid automaton H be uniformly tightly bounded with respect to control and $\pi^\ell, \pi^u \in \mathscr{F}$ be as in Definition 11. Then H is *bounded* if for all $\xi \in \mathcal{X}$ there exist $\mathbf{y}^{\ell u}_\xi, \mathbf{y}^{u\ell}_\xi \in \mathcal{C}(Y)$ such that

(i) $\forall\, \chi^\ell \in \mathscr{H}_{\pi^\ell}(\xi)$ and all $\chi^u \in \mathscr{H}_{\pi^u}(\xi)$, $\mathbf{y}^\ell \preceq \mathbf{y}^{\ell u}_\xi$ and $\mathbf{y}^{u\ell}_\xi \preceq \mathbf{y}^u$;

(ii) $\forall\, T \in \mathbb{R}_+$, $\epsilon > 0$ there exist $(\underline{\tau}, \underline{\mathbf{d}}), (\bar{\tau}, \bar{\mathbf{d}}) \in \mathcal{HT}(D)$ such that for all $\bar{\chi} \in \mathscr{H}^{\bar{\mathbf{d}}}_{\pi^\ell}(\xi)$ and all $\underline{\chi} \in \mathscr{H}^{\underline{\mathbf{d}}}_{\pi^u}(\xi)$, $\left\|\mathbf{y}^{\ell u}_\xi(t) - \bar{\mathbf{y}}(t)\right\| + \left\|\mathbf{y}^{u\ell}_\xi(t) - \underline{\mathbf{y}}(t)\right\| \leq \epsilon \; \forall t \in [0, T]$.

In Section 5 we discuss conditions guaranteeing that hybrid automata are bounded and show that the application examples satisfy these conditions.

3.5 Problem formulation

The problem we are considering has two main components, the hybrid automaton H and a so-called *bad set* $\mathcal{B}$. The bad set $\mathcal{B}$ contains all "unsafe" system configurations and has to be avoided. We consider the following cases:

i) H is a continuous and bounded hybrid automaton where the partial order on Y is induced. The bad set is for some $b \in Y$ given by $\mathcal{B} = \text{int}\, [\![b, \infty]\!]$;

ii) $H = H^1 \parallel H^2$ is the parallel composition of continuous and bounded hybrid automata H^1 and H^2 where Y^1 and Y^2 are equipped with induced partial orders. The bad set is $\mathcal{B} = \text{int}\, [\![b^1, \infty]\!] \times \text{int}\, [\![-\infty, b^2]\!]$, for $b^j \in Y^j$.

We say that $\pi \in \mathscr{F}$ is *safe* for $\xi \in \mathcal{X}$ if

$$\mathbf{y}(\mathbb{R}_+) \cap \mathcal{B} = \emptyset \; \forall \chi \in \mathscr{H}_\pi(\xi). \tag{6}$$

The *safe set* $\mathcal{W}(\mathcal{B})$ is the set of initial conditions for which there exists a safe feedback controller, that is,

$$\mathcal{W}(\mathcal{B}) \coloneqq \{\xi \in \mathcal{X} \mid \exists \pi \in \mathscr{F} \text{ s.t. (6) holds}\}.$$

Definition 13. Let $\pi \in \mathscr{F}$ be safe for all $\xi \in \mathcal{W}(\mathcal{B})$. Then π is a *least restrictive safety supervisor* if there exists no $\pi' \in \mathscr{F} \setminus \{\pi\}$ that is safe for all $\xi \in \mathcal{W}(\mathcal{B})$ and satisfies

$$\pi(\xi) \subset \pi'(\xi) \quad \forall \xi \in \text{int}\, \mathcal{W}(\mathcal{B}).$$

Problem 1. Find a least restrictive safety supervisor $\pi \in \mathscr{F}$.

Least restrictiveness of safety supervisors corresponds to the requirement that these controllers should not impose restrictive conditions on the hybrid dynamics as long as the system state is in the interior of the safe set.

3.6 Illustration on application example

Consider the forward collision avoidance warning system described in Section 2.1. The set of modes Q_{FC} of the corresponding hybrid system H_{FC} contains the three system modes depicted in Figure 2. The continuous state of the system is $x^{FC} \coloneqq (x_r, v_f, v_l)$ and the system output is x_r, thus the output map $h_{FC}(x^{FC}) = x_r$. We assume that the override control input u_f is bounded and set $U_{FC} \coloneqq [u_f^m, u_f^M]$. The disturbance input has two bounded components (d_f, d_l) hence we define $D_{FC} \coloneqq [d_f^m, d_f^M] \times [d_l^m, d_l^M]$. Controlled discrete transitions can happen in mode q_1^{FC}, see Figure 2, which implies that $\mathcal{E}_{FC} \coloneqq \left\{(q_1^{FC}, q_2^{FC}), e_0\right\}$, where e_0 is a void input that can be used before the first controlled mode transition. The guard condition ensures that controlled mode transitions do in fact only occur in mode q_1^{FC}, i.e.

$$G_{FC}(q_j^{FC}) \coloneqq \begin{cases} \{(q_1^{FC}, q_2^{FC})\} & \text{if } j \in \{1, 2\}, \\ \emptyset & \text{otherwise.} \end{cases}$$

In the WARNED mode transitions happen when the driver's input d_f is outside the open set $D_W \subset [d_f^m, d_f^M]$ after a dwell time $\omega \geq T_{RT}$. This is modeled with the following invariance set:

$$\mathrm{Inv}_{FC}(q) \coloneqq [0, T_{RT}[\times D_{FC} \cup [T_{RT}, \infty[\times D_W \times [d_l^m, d_l^M],$$

if $q = q_2^{FC}$ and $\mathrm{Inv}(q) \coloneqq \mathbb{R}_+ \times D_{FC}$ otherwise. Since the mode graph depicted in Fig. 2 is a chain, the mode reset map can be defined as $R(q_j^{FC}, \mathcal{E}) = \{q_{j+1}\}$ if $j \in \{1, 2\}$ and $R(q_3^{FC}, \mathcal{E}) = \{q_3^{FC}\}$. The continuous dynamics are given in (1) where the input ι_f depends on the mode. We have

$$f^{FC}(q_j^{FC}, x^{FC}, u_f, d_f, d_l) \coloneqq \begin{cases} \bar{f}^{FC}(x^{FC}, d_f, d_l) & \text{if } j \in \{1, 2\}, \\ \bar{f}^{FC}(x^{FC}, u_f, d_l) & \text{if } j = 3. \end{cases}$$

Recall that the bad set for this problem has already been defined in (2). Thus the order on Y_{FC} is induced by $\mathbb{R}_+$. Solving Problem 1 corresponds in this case to designing a feedback controller that maintains a large enough relative distance x_r for all possible inputs of the drivers of both vehicles.
Consider next the two vehicle conflict situation described in Section 2.2. By using the vehicle dynamics $\bar{f}^{MC}$, the finite state machine depicted in Fig. 2 and D_W^ℓ, D_W^u to replace D_W in the above definition of the invariance set, we can define the hybrid automata H^ℓ and H^u. Here H^ℓ represents a driver-assist system that provides a braking warning and H^u one that provides an acceleration warning. To design a controller for the two vehicle conflict scenario we consider the hybrid automaton $H^{MC} \coloneqq H_i \parallel H_e$ where H_i and H_e are hybrid automata corresponding to IV and EV respectively. We then have to solve the following two problems:

1) $H_i = H^\ell$, $H_e = H^u$ and the bad set is $B_{MC}^{\ell u}$;

2) $H_i = H^u$, $H_e = H^\ell$ and the bad set is $B_{MC}^{u\ell}$.

Since it is clear that $B_{MC}^{\ell u}$ and $B_{MC}^{u\ell}$ defined by (4) correspond to the case when the order of Y_i is induced by $\mathbb{R}_-$ and $\mathbb{R}_+$ respectively, the two problems fit the framework introduced in Section 3.5.

4 PROBLEM SOLUTION

In this section we present the solution of Problem 1. We first describe the feedback controllers that solve the problem. Then we show how these controllers can be implemented efficiently and finally conclude the section by describing the solution algorithm for the application examples described in Section 2. Proofs of all theoretical results are provided in the Appendix.

4.1 Control strategy

For any hybrid system H, bad set $\mathcal{B} \subset Y$ and feedback controller $\pi \in \mathscr{F}$ the corresponding *capture set* $C_\pi(\mathcal{B})$ is defined by

$$C_\pi(\mathcal{B}) \coloneqq \{\xi \in \mathcal{X} \mid \exists \chi \in \mathscr{H}_\pi(\xi) \text{ s.t. } \mathbf{y}(\mathbb{R}_+) \cap \mathcal{B} \neq \emptyset\}.$$

The set $C_\pi(\mathcal{B})$ represents the set of states for which $\pi \in \mathscr{F}$ is not safe. It is convenient to define for every $q \in Q$ the *mode dependent capture set*

$$C_\pi(q; \mathcal{B}) \coloneqq \{(\omega, x) \in \mathbb{R}_+ \times X \mid (\omega, q, x) \in C_\pi(\mathcal{B})\}.$$

In addition, using the notion of capture set, the discrete inputs that are admissible and safe are given by the set

$$\mathcal{E}_\pi(\omega, q, x; \mathcal{B}) \coloneqq (G(q) \cup \{e_0\}) \setminus \left(\{q\} \times \left\{q' \in Q \;\middle|\; (\omega, q', x) \in C_\pi(\mathcal{B})\right\}\right).$$

In the case of a continuous and bounded hybrid system we have the following result.

Theorem 1. *Let H be uniformly tightly bounded with respect to control. Moreover $\mathcal{B} = \operatorname{int} [\![b, \infty]\!]$ for some $b \in Y$ and $\pi^\ell \in \mathscr{F}$ be as in Definition 11. Then $\bar{\pi} \in \mathscr{F}$ given by*

$$\bar{\pi}(\omega, q, x) \coloneqq \begin{cases} \pi^\ell(\omega, q, x) & \text{if } (\omega, x) \in \overline{C_{\pi^\ell}(q; \mathcal{B})}, \\ \mathcal{E}_{\pi^\ell}(\omega, q, x; \mathcal{B}) \times U & \text{otherwise,} \end{cases}$$

is a least restrictive safety supervisor and $\mathcal{W}(\mathcal{B}) = C_{\pi^\ell}(\mathcal{B})^c$.

The case when H is the parallel composition of bounded hybrid automata is similar.

Theorem 2. *Let $H = H^1 \parallel H^2$ where for all $j \in \{1, 2\}$, H^j is uniformly tightly bounded with respect to control. Furthermore let $\mathcal{B} = \operatorname{int} [\![b^1, \infty]\!] \times \operatorname{int} [\![-\infty, b^2]\!]$ where $b^j \in Y^j$ for $j \in \{1, 2\}$. Finally let $\pi^\uparrow \coloneqq \left(\pi_1^\ell, \pi_2^u\right)^T \in \mathscr{F}$ where π_j^ℓ and π_j^u denote the feedback controllers of each system H^j from Definition 11. Then $\bar{\pi} \in \mathscr{F}$ defined by*

$$\bar{\pi}(\omega, q, x) \coloneqq \begin{cases} \pi^\uparrow(\omega, q, x) & \text{if } (\omega, x) \in \overline{C_{\pi^\uparrow}(q; \mathcal{B})}, \\ \mathcal{E}_{\pi^\uparrow}(\omega, q, x; \mathcal{B}) \times U & \text{otherwise,} \end{cases}$$

is a least restrictive safety supervisor and $\mathcal{W}(\mathcal{B}) = C_{\pi^\uparrow}(\mathcal{B})^c$.

4.2 Characterization of capture set

The implementation of the least restrictive safety supervisors obtained in Theorems 1 and 2 requires the computation of the corresponding capture, respectively safe sets. Here we show that these capture sets have a simple characterization for bounded hybrid automata.

Theorem 3. *Let H be a continuous and bounded hybrid system. Moreover let $\mathcal{B}$ be as in Theorem 1. Then*

$$\mathcal{W}(\mathcal{B}) = \left\{\xi \in \mathcal{X} \;\middle|\; \mathbf{y}_\xi^{\ell u}(\mathbb{R}_+) \cap \mathcal{B} = \emptyset\right\},$$

where $\mathbf{y}_\xi^{\ell u}$ is as in Definition 12.

The case when H the parallel composition of bounded hyrid automata is similar.

Theorem 4. *Let $H = H^1 \parallel H^2$ where for $j \in \{1, 2\}$, H^j is continuous and bounded. Moreover let $\mathcal{B}$ be as in Theorem 2. Then*

$$\mathcal{W}(\mathcal{B}) = \left\{\xi = (\xi_1, \xi_2) \in \mathcal{X} \;\middle|\; (\mathbf{y}_{\xi_1}^{\ell u}, \mathbf{y}_{\xi_2}^{u \ell})(\mathbb{R}_+) \cap \mathcal{B} = \emptyset\right\},$$

where $\mathbf{y}_{\xi_j}^{\ell u}$ and $\mathbf{y}_{\xi_j}^{u \ell}$ are as in Definition 12 for $j \in \{1, 2\}$.

4.3 Solution algorithm

The least restrictive safety supervisors from Theorem 1 and 2 are set-valued maps which means that they provide a set of safe inputs rather than a specific safe input. These safety supervisors should therefore be understood as actual supervisors of the system. To be precise consider the logic diagram of Fig. 4. Here (u^p, d^p) corresponds to the plant input which might be driver and disturbance inputs in a driver assist system. Then the safety supervisor checks if the plant input is within the set of safe inputs and overrides the plant input if and only if this is the case.

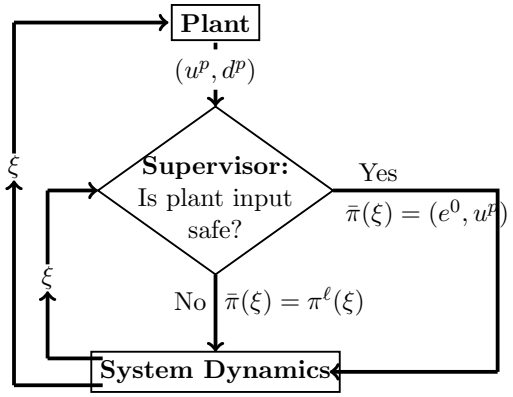


Figure 4: Finite state machine corresponding to the modes of operation of the forward collision avoidance driver-assist system with events that trigger the mode transitions. The mode WARNED has non-zero minimum dwell time τ.

Since the actual implementation of the safety supervisor will check the safety of the plant input in discrete time, we use a fixed time step $\Delta t > 0$ and perform a forward Euler approximation in order to compute the state that would result by applying the plant input (u^p, d^p). To check whether this state is in $\mathcal{W}(\mathcal{B})$ we then use either Theorem 3 or Theorem 3. Pseudo code for the case of a bounded hybrid automaton is provided in Algorithm 1.

5 A class of bounded hybrid automata

As stated in Section 3.5 our main assumption is that the hybrid automaton H is continuous and bounded. In this section we describe a class of hybrid automata that has these properties.

5.1 Discrete dynamics

It is natural to consider the set of modes Q of a hybrid automaton H together with the possible mode transitions as a directed graph. To be precise, one can consider the graph $(Q, \mathcal{A})$, where Q represents the set of vertices of the graph and the arcs $\mathcal{A}$ are given by

$$\mathcal{A} \coloneqq \left\{ (q, q') \in Q \times Q \;\middle|\; q' \in R(q, \mathcal{E}) \wedge q \neq q' \right\}.$$

Algorithm 1: Supervisor for bounded hybrid automaton

Input: Current state ξ and plant input (u^p, d^p)
Output: Discrete and continuous inputs (ε, u)
  Compute $\chi^{pred} \in \mathscr{H}^{d^p}_{u^p}(\xi)$;
  $\xi^{pred} \leftarrow \big(\mathbf{w}^{pred}(\Delta t), \mathbf{q}^{pred}(\Delta t), \mathbf{x}^{pred}(\Delta t)\big)$;
  if $\xi^{pred} \in \left\{ \xi \in \mathcal{X} \;\middle|\; \mathbf{y}^{\ell u}_{\xi}(\mathbb{R}_+) \cap \mathcal{B} = \emptyset \right\}$ **then**
    $(\varepsilon, u) \leftarrow (\emptyset, u^p)$;
  else
    if $(\emptyset, u^p) \in \pi^{\ell}(\xi)$ **then**
      $(\varepsilon, u) \leftarrow (\emptyset, u^p)$;
    else
      $(\varepsilon, u) \leftarrow \pi^{\ell}(\xi)$;
    end if
  end if
  return (ε, u);

Definition 14. For a mode $q \in Q$ the set of its *successors* is $\mathscr{S}(q) \coloneqq \{q' \in Q \mid \exists (q, q') \in \mathcal{A}\}$. A *leaf* is a mode q such that $\mathscr{S}(q) = \emptyset$. A *controlled mode* is a mode q such that $(q, q') \in \mathcal{E}$ for all $q' \in \mathscr{S}(q)$. The set of controlled modes is denoted by $Q_{\mathcal{E}}$, Q_L is the set of leafs and $Q_D \coloneqq Q \setminus (Q_{\mathcal{E}} \cup Q_L)$.

Definition 15. A *simple path* is a sequence $\{q_0, \ldots, q_N\} \subset Q$ such that for all $j \in \{0, \ldots, N-1\}$, $(q_j, q_{j+1}) \in \mathcal{A}$ and $q_j \neq q_k$ for all $j \neq k$.

We will impose the following assumption on $(Q, \mathcal{A})$.

Assumption 1. i) $\mathcal{E} \subset \mathcal{A}$; ii) $(Q, \mathcal{A})$ forms a simple path; iii) for all $q \in Q_{\mathcal{E}}$, $\mathrm{Inv}(q) = \mathbb{R}_+ \times D$ and $G(q) = \{q\} \times \mathscr{S}(q)$; iv) for $q \in Q_L$, $\mathrm{Inv}(q) = \mathbb{R}_+ \times D$ and $G(q) = \emptyset$; v) for all $q \in Q_D$, $q \notin R(q, \mathcal{E})$ and $G(q) = \mathcal{E}$.

Condition i) ensures that each discrete control input corresponds to a specific mode transition. Requirement ii) reflects the hierarchy between different operating modes. Moreover together with iv) and v) it guarantees that there are finitely many mode transitions since every mode can be visited at most once. Conditions iii)-v) restrict the discrete dynamics according to the three classes of modes $Q_{\mathcal{E}}$, Q_L and Q_D. The notation $q \preceq q'$ means that either $q = q'$ or there exists a simple path from q to q'.

5.2 Continuous dynamics

The following is a standard assumptions on the dynamics.

Assumption 2. i) For all $(q, u, d) \in Q \times U \times D$ the mapping $x \mapsto f(q, x, u, d)$ is Lipschitz on X and for all $(q, x) \in Q \times X$ the mapping $(u, d) \mapsto f(q, x, u, d)$ is continuous; ii) the map $h \colon X \to Y$ is continuous.

Proposition 1. *Let H be a hybrid automaton satisfying Assumptions 1-2. Then H is non-blocking, has no Zeno executions and is continuous.*

The proof of this result uses standard arguments from hybrid systems theory, see for instance [7], and is therefore omitted.

In order to obtain a sufficient condition for boundedness of a hybrid automaton we use the notion of order preserving systems.
For each $q \in Q$, the continuous system $\Sigma(q) = (X, Y, f(q,\cdot,\cdot,\cdot), h, U, D)$ characterizes the continuous dynamics within the mode. Thanks to Assumption 2, for all $x \in X$, $\mathbf{u} \in \mathcal{S}(U)$ and $\mathbf{d} \in \mathcal{S}(D)$ there exist corresponding trajectories $\mathbf{x}^{q,x,\mathbf{u},\mathbf{d}} \in \mathcal{C}(X)$, $\mathbf{y}^{q,x,\mathbf{u},\mathbf{d}} \in \mathcal{C}(Y)$ satisfying $\mathbf{x}^{q,x,\mathbf{u},\mathbf{d}}(0) = x$ and

$$\begin{cases} \dot{\mathbf{x}}^{q,x,\mathbf{u},\mathbf{d}}(t) = f(q, \mathbf{x}^{q,x,\mathbf{u},\mathbf{d}}(t), \mathbf{u}(t), \mathbf{d}(t)) \quad \forall t \in \mathbb{R}_+, \\ \mathbf{y}^{q,x,\mathbf{u},\mathbf{d}}(t) = h(\mathbf{x}^{q,x,\mathbf{u},\mathbf{d}}(t)) \quad \forall t \in \mathbb{R}_+. \end{cases}$$

Definition 16. Let $q \in Q$, X, Y, U and D be partially ordered sets. Then $\Sigma(q)$ is *order preserving* with respect to control and disturbance if for all $\mathbf{d} \in \mathcal{S}(D)$ and $\mathbf{u} \in \mathcal{S}(U)$,

(i) $x_1 \preceq x_2,\ \mathbf{u}_1 \preceq \mathbf{u}_2 \implies \mathbf{x}^{q,x_1,\mathbf{u}_1,\mathbf{d}} \preceq \mathbf{x}^{q,x_2,\mathbf{u}_2,\mathbf{d}}$;

(ii) $x_1 \preceq x_2,\ \mathbf{d}_1 \preceq \mathbf{d}_2 \implies \mathbf{x}^{q,x_1,\mathbf{u},\mathbf{d}_1} \preceq \mathbf{x}^{q,x_2,\mathbf{u},\mathbf{d}_2}$;

(iii) $x_1 \preceq x_2 \implies h(x_1) \preceq h(x_2)$.

5.3 Bounded hybrid automata

Next we provide sufficient conditions for a hybrid automaton to be bounded.

Theorem 5. *Let H be a hybrid automaton satisfying Assumption 1-2 and such that X, Y, U and D are sets with induced partial orders. Then H is continuous and bounded if in addition the following conditions are satisfied*

(i) there exist $u^\ell, u^u \in \mathbb{R}^m$ such that $U = [\![u^\ell, u^u]\!]$;

(ii) there exist $d^\ell, d^u \in \mathbb{R}^s$ such that $D = [\![d^\ell, d^u]\!]$;

(iii) for all $q \in Q_D$ there exist $T^q \in \mathbb{R}_+$, $d_q^{\omega,\ell}, d_q^\ell, d_q^{\omega,u}, d_q^u \in D$ such that $d_q^{\omega,\ell} \preceq d_q^\ell$, $d_q^{\omega,u} \succeq d_q^u$ and $\mathrm{Inv}(q) = \Big([0, T^q[\times \mathrm{int}\,[\![d_q^{\omega,\ell}, d_q^{\omega,u}]\!]\Big) \cup \big([T^q, \infty[\times \mathrm{int}\,[\![d_q^\ell, d_q^u]\!]\big)$;

(iv) for all $q \in Q$, the continuous system $\Sigma(q)$ is order preserving with respect to control and disturbance;

(v) for all $x \in X$, $\mathbf{u} \in S(U)$, $\mathbf{d} \in S(D)$ and all $q, \tilde{q} \in Q$ such that $\tilde{q} \preceq q$,

$$\mathbf{y}^{q,x,u^\ell,\mathbf{d}} \preceq \mathbf{y}^{\tilde{q},x,u^\ell,\mathbf{d}},\ \mathbf{y}^{\tilde{q},x,u^u,\mathbf{d}} \preceq \mathbf{y}^{q,x,u^u,\mathbf{d}},$$
$$\mathbf{y}^{\tilde{q},x,\mathbf{u},d_q^\ell} \preceq \mathbf{y}^{q,x,\mathbf{u},d_q^{\omega,\ell}},\ \mathbf{y}^{q,x,\mathbf{u},d_q^{\omega,u}} \preceq \mathbf{y}^{\tilde{q},x,\mathbf{u},d_q^u},$$

where $d_q^j = d_q^{\omega,j} = d^j$, $j \in \{\ell, u\}$, if $q \in Q_\mathcal{E} \cup Q_L$.

The proof of this result is provided in the Appendix and is based on the explicit forms of the extremal trajectories provided in following Corollaries.

Corollary 1. *Let H be as in Theorem 5. Then $\pi^\ell, \pi^u \in \mathscr{F}$ defined by*

$$\pi^\ell(\omega, q, x) \coloneqq \begin{cases} \{(q, \mathscr{S}(q))\} \times \{u^\ell\} & \text{if } q \in Q_{\mathcal{E}}, \\ \{(e_0, u^\ell)\} & \text{otherwise}, \end{cases}$$

$$\pi^u(\omega, q, x) \coloneqq \begin{cases} \{(q, \mathscr{S}(q))\} \times \{u^u\} & \text{if } q \in Q_{\mathcal{E}}, \\ \{(e_0, u^u)\} & \text{otherwise}, \end{cases}$$

are extremal feedback controllers as in Defintion 11.

Corollary 2. *Let H be as in Theorem 5 and $\pi^\ell, \pi^u \in \mathscr{F}$ be as in Corollary 1. Then for all $(\omega, q, x) \in \mathbb{R}_+ \times Q \times X$ we can set $\bar{q} \in Q \setminus (Q_{\mathcal{E}} \cup Q_L)$ to be such that $q \preceq \bar{q}$ and $\bar{q} \preceq q'$ for all $q' \in \{\tilde{q} \in Q_D \mid q \preceq \tilde{q}\}$ and $\bar{\omega} = \omega$ if $q = \bar{q}$ and $\bar{\omega} = 0$ otherwise. Defining the signals $\mathbf{d}^\ell, \mathbf{d}^u \in \mathcal{S}(D)$ by*

$$\mathbf{d}^\ell(t) \coloneqq \begin{cases} d_{\bar{q}}^{\omega,\ell} & \text{if } t \leq T^{\bar{q}} - \bar{\omega}, \\ d_{\bar{q}}^{\ell} & \text{otherwise}, \end{cases}$$

$$\mathbf{d}^u(t) \coloneqq \begin{cases} d_{\bar{q}}^{\omega,u} & \text{if } t \leq T^{\bar{q}} - \bar{\omega}, \\ d_{\bar{q}}^{u} & \text{otherwise}, \end{cases}$$

$\mathbf{y}^{\ell u} \coloneqq \mathbf{y}^{\bar{q},x,u^\ell,\mathbf{d}^u}$ and $\mathbf{y}^{u\ell} \coloneqq \mathbf{y}^{\bar{q},x,u^u,\mathbf{d}^\ell}$ are bounds as in Definition 12.

It is not difficult to check that the hybrid systems H_{FC}, H^ℓ and H^u introduced in Section 3.6 satisfy the conditions of Theorem 5 if the sets D_W, D_W^ℓ and D_W^u are open intervals. It is then straightforward to obtain least restrictive safety supervisors for both the forward collision and the two vehicle conflict scenarios by using Theorem 1-4 and Corollary 1-2.

6 SIMULATION RESULTS

Simulation results were obtained by using Algorithm 1 for the application examples of Section 2. All algorithms were implemented in MATLAB and run on a 2.6 GHz dual core computer.

6.1 Forward collision avoidance with warnings: Capture sets

Consider the scenario described in Section 2.1. To compute the capture set of this problem we use Theorem 3 and Corollary 2. The set $C(B_{FC}) \coloneqq \mathcal{W}(B_{FC})^c$ of this problem is a subset of $\mathbb{R}^3$. For better visualization we plot two dimensional slices of this set that correspond to the fixed LV speed 120km/h. Moreover we use $v_r \coloneqq v_l - v_f$ to denote the relative velocity of LV with respect to FV. Fig. 5 shows the mode dependent capture sets. By Corollary 1 it is clear that the mode dependent capture set for q_1^{FC} and q_2^{FC} are equal when $\omega = 0$. The mode dependent capture set corresponding to q_3^{FC} on the other hand is considerably smaller as in this case FV can be controlled by the supervisor. The minimum dwell time ω_m has an important impact on the size of the mode dependent capture set in modes q_1^{FC} and q_2^{FC}, as is shown in Fig. 6. As expected, the larger ω_m the bigger the capture set. Notice that the dwell time ω has a similar effect when the system is in mode q_2^{FC}. In this case, the bigger ω, the smaller the mode dependent capture set.

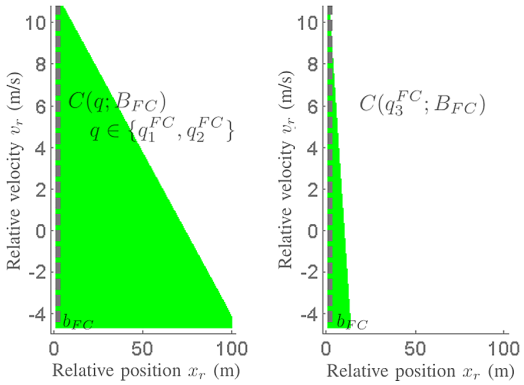


Figure 5: Slices of the mode dependent capture set $C(q; B_{FC})$ where $v_l = 33\frac{1}{3}m/s$, $\omega = 0s$ and $\omega_m = T_{RT} = 1s$.

6.2 Two vehicle conflict scenario

For the two vehicle conflict scenario described in section 2.2 we simulated the position of IV and EV under the control of the safety supervisor given in Theorem 2, see Fig. 7. As mentioned in Section 2.2, the case when IV passes the merging zone first corresponds to the bad set $B_{MC}^{u\ell}$. The set $B_{MC}^{\ell u}$ corresponds to the case when EV is first to pass. In the simulation depicted in Fig. 7 only the case when IV passes first is safe. Finally recall that warned drivers obey the warning when their actuation input belongs to the set D_W^{ℓ} or D_W^{u} depending on whether they got an acceleration or a braking warning. In the simulation example of Fig. 7, EV disobeys the warning and is therefore eventually overridden by the driver-assist system.

7 CONCLUSIONS AND FUTURE WORK

In this paper we considered the safety problem for bounded hybrid automata and designed a corresponding safe and least restrictive feedback controller. In addition we showed that for a special class of bounded hybrid automata this feedback controller has a simple form and is efficiently computable online. Finally we showed that driver-assist systems that warn drivers before they override them can be modeled within this class of hybrid systems.

The applicability of our approach is mainly restricted by the fact that we consider bad sets that are cones. Moreover, it is in general difficult to check whether a given hybrid automaton is bounded and to find the appropriate enveloping trajectories. It would therefore be interesting to investigate possible relaxations of the conditions of Theorem 5. From a practitioners point of view it would be interesting to investigate approaches to decide whether the driver is complying with the warning other than the hard threshold used here. Finally, another interesting problem would be to to study how to give the control back to the driver after a safety intervention.

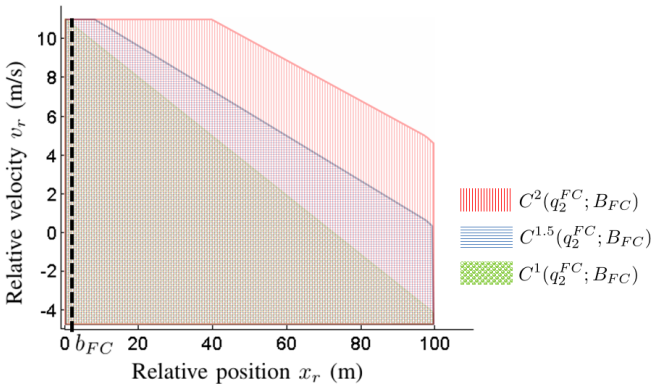


Figure 6: The figure shows superposed mode dependent capture sets for the mode q_2^{FC} and $\omega_m \in \{1s, 1.5s, 2s\}$. We have $C^1(q_2^{FC}; B_{FC}) \subset C^{1.5}(q_2^{FC}; B_{FC}) \subset C^2(q_2^{FC}; B_{FC})$ where $C^{T_{RT}}(q_2^{FC}; B_{FC})$ stands for the mode dependent capture set of a system with $\omega_m = T_{RT}$.

A Proofs of the safety results

In the following we prove Theorem 1 and 2. We start with a few helpful lemmas.

Lemma 1. *Let H be a continuous hybrid system, $\pi \in \mathscr{F}$ and $\mathcal{B} \subset Y$ open. Then for all $q \in Q$, $C_\pi(q; \mathcal{B})$ is open.*

Proof. Fix an arbitrary $q \in Q$ and $(\omega, x) \in C_\pi(q; \mathcal{B})$. We show that there exists $\delta > 0$ such that

$$(\tilde{\omega}, \tilde{x}) \in C_\pi(q; \mathcal{B}) \quad \forall (\tilde{\omega}, \tilde{x}) \in (\omega, x) + \delta B, \tag{7}$$

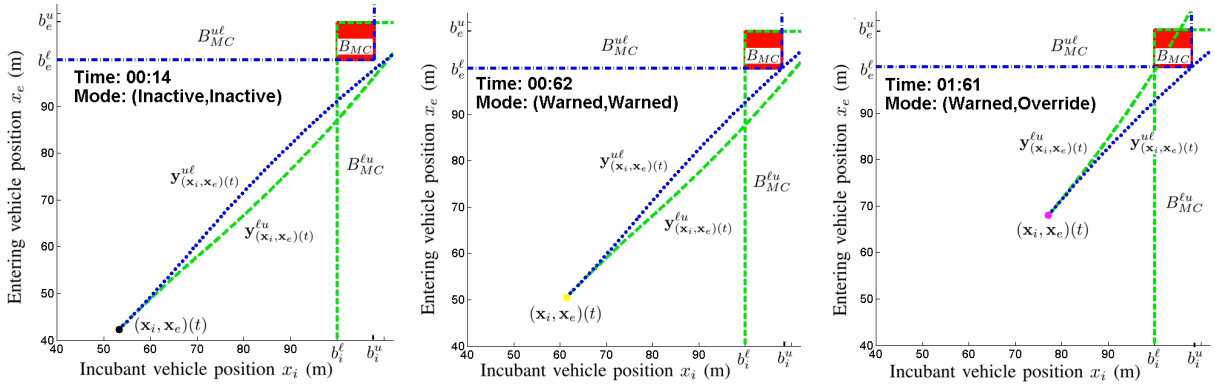
where B denotes an open ball. Since $(\omega, x) \in C_\pi(q; \mathcal{B})$, there exist $t \in \mathbb{R}_+$ and $\chi \in \mathscr{H}_\pi(\omega, q, x)$ such that $\mathbf{y}(t) \in \mathcal{B}$. By openness of $\mathcal{B}$ there exists $\epsilon > 0$ such that $\mathbf{y}(t) + \epsilon B \subset \mathcal{B}$. Hence, by Definition 10, there exists $\delta > 0$ such that for all $(\tilde{\omega}, \tilde{x}) \in (\omega, x) + \delta B$ there exists $\tilde{\chi} \in \mathscr{H}_\pi(\tilde{\omega}, q, \tilde{x})$ such that $\|\tilde{\mathbf{y}}(t) - \mathbf{y}(t)\| < \epsilon$ and therefore $\tilde{\mathbf{y}}(t) \in \mathcal{B}$ which implies (7). □

Lemma 2. *Let H be a continuous hybrid automaton, $\mathcal{B} \subset Y$ open and $M \in \mathbb{N}$. Furthermore let $\{\pi_j\}_{j=1}^M$, $\{\mathcal{B}_j\}_{j=1}^M$ be such that $\pi_j \in \mathscr{F}$ and $\mathcal{B} \subset \mathcal{B}_j$ for all j. Then $\bar{\pi} \in \mathscr{F}$ given by*

$$\bar{\pi}(\omega, q, x) := \begin{cases} \pi_j(\omega, q, x) \\ \text{if } (\omega, x) \in \partial C_j(q) \cap \left(\bigcap_{k<j} \overline{C_k(q)}\right) \cap \left(\bigcap_{l>j} C_l(q)\right), \\ \mathcal{E}_{\pi_1,\dots,\pi_M}(\omega, q, x; \mathcal{B}_1, \dots, \mathcal{B}_M) \times U \qquad \text{otherwise,} \end{cases}$$

is safe for all $(\omega, q, x) \in \left(\bigcap_{j=1}^M C_j\right)^c$, where $C_j := C_{\pi_j}(\mathcal{B}_j)$, $C_j(q) := C_{\pi_j}(q; \mathcal{B}_j)$ and

$$\mathcal{E}_{\pi_1,\dots,\pi_M}(\omega, q, x; \mathcal{B}_1, \dots, \mathcal{B}_M) := (G(q) \cup \{e_0\}) \setminus \left\{(q, q') \;\middle|\; (\omega, q', x) \in \textstyle\bigcap_{j=1}^M C_j\right\}.$$



(a) (b) (c)

Figure 7: The plots show a sequence of positions for a simulation with two vehicles approaching a merging zone B_{MC}. In (a), the hybrid state is in $\mathcal{W}(B_{MC}^{\ell u})^c$ but in $\mathcal{W}(B_{MC}^{u\ell})$. In (b) the state hits the boundary of the safe set $\mathcal{W}(B_{MC}^{u\ell})$ and the safety supervisor warns both drivers. IV complies with the warning while EV disobeys and is eventually overridden by the system, (c).

Proof. For any $\chi \in \mathscr{H}$, $(\mathbf{w},\mathbf{q},\mathbf{x})([0,t])$ denotes the hybrid state history, thus

$$(\mathbf{w},\mathbf{q},\mathbf{x})([0,t]) \coloneqq \{(\mathbf{w}(t),\mathbf{q}(t),\mathbf{x}(t)) \mid t \in [0,t]\}\,.$$

The set of all finite histories of the hybrid automaton H is denoted by $\mathscr{X}^*$. With this we can define *causal controllers* as maps $\pi\colon \mathscr{X}^* \to \mathcal{E} \times U$ and extend the notion of closed loop causal executions to the set

$$\mathscr{H}_\pi = \{\chi \in \mathscr{H} \mid \forall j \in \{0,\dots,\langle\tau\rangle\},$$
$$(\mathbf{e}_{j+1}(t),\mathbf{u}_{j+1}(t)) \in \pi((\mathbf{w},\mathbf{q},\mathbf{x})([0,t])) \text{ if } t \in \tilde{I}_j \text{ and } (\mathbf{e}_0,\mathbf{u}_j(t)) \in \pi((\mathbf{w},\mathbf{q},\mathbf{x})([0,t])) \;\forall t \in I_j \setminus \tilde{I}_j\Big\}\,.$$

Notice that feedback controllers are a particular case of causal controllers.
Next, consider the causal controller $\hat{\pi}\colon \mathscr{X}^* \to \mathcal{E} \times U$ defined by

$$\hat{\pi}((\mathbf{w},\mathbf{q},\mathbf{x})([0,t])) \coloneqq \begin{cases} \bar{\pi}(\mathbf{w}(t),\mathbf{q}(t),\mathbf{x}(t)) & \text{if } t \le \varepsilon_t, \\ \pi_{j_t}(\mathbf{w}(t),\mathbf{q}(t),\mathbf{x}(t)) & \text{otherwise,} \end{cases}$$

where

$$\varepsilon_t \coloneqq \inf\left\{ t' \in [0,t] \;\middle|\; (\mathbf{w},\mathbf{q},\mathbf{x})([t',t]) \subset \bigcap_{j=1}^{M} C_j \right\},$$

$$j_t \coloneqq \max\left\{ j \in \{1,\dots,M\} \;\middle|\; (\mathbf{w}(\varepsilon_t),\mathbf{x}(\varepsilon_t)) \in \partial C_j(\mathbf{q}(\varepsilon_t)) \cap \left(\bigcap_{k=1}^{M} \overline{C_k(\mathbf{q}(\varepsilon_t))} \right) \right\}.$$

We make the convention that $\varepsilon_t = t$ and $j_t = 1$ if the sets over which we take the infimum and the maximum are empty. Hence $\hat{\pi}$ is well-defined.

To prove the Lemma it is sufficient to show that

$$(\mathbf{w}(\mathbb{R}_+), \mathbf{q}(\mathbb{R}_+), \mathbf{x}(\mathbb{R}_+)) \cap \bigcap_{j=1}^{M} C_j = \emptyset \qquad \forall \chi \in \mathscr{H}_{\hat{\pi}} \left(\left(\bigcap_{j=1}^{M} C_j \right)^c \right). \tag{8}$$

Indeed, if (8) holds true, then it follows from the very definition of $\hat{\pi}$ that

$$\mathscr{H}_{\hat{\pi}} \left(\left(\bigcap_{j=1}^{M} C_j \right)^c \right) = \mathscr{H}_{\bar{\pi}} \left(\left(\bigcap_{j=1}^{M} C_j \right)^c \right).$$

Moreover, since clearly $\{(\omega, q, x) \mid h(x) \in \mathcal{B}\} \subset \bigcap_{j=1}^{M} C_j$, the statement of the Lemma follows from (8).
To show (8) we argue by contradiction and assume there exists $(\omega, q, x) \in \left(\bigcap_{j=1}^{M} C_j \right)^c$, $\chi \in \mathscr{H}_{\hat{\pi}}(\omega, q, x)$ and $t \in I_k \in \tau$ such that $(\mathbf{w}_k(t), \mathbf{x}_k(t)) \in \bigcap_{j=1}^{M} C_j(q_k(t))$.
We show first that this implies that

$$(\mathbf{w}_k(\tilde{t}), \mathbf{x}_k(\tilde{t})) \in \bigcap_{j=1}^{M} C_j(\mathbf{q}_k(\tau_k)) \quad \forall \tilde{t} \in [\tau_k, t]. \tag{9}$$

Indeed, if we assume to the contrary that there exists $\tilde{t} \in [\tau_k, t]$ such that $(\mathbf{w}_k(\tilde{t}), \mathbf{x}_k(\tilde{t})) \in \left(\bigcap_{j=1}^{M} C_\pi(\mathbf{q}_j(\tau_j)) \right)^c$ then by the continuity of $\mathbf{w}_k$ and $\mathbf{x}_k$, there exists $\bar{t} \in [\tilde{t}, t[$ such that for all $t' \in]\bar{t}, t]$, $(\mathbf{w}_k(t'), \mathbf{x}_k(t')) \in \bigcap_{j=1}^{M} C_j(\mathbf{q}_k(\tau_k))$ and

$$(\mathbf{w}_k(\bar{t}), \mathbf{x}_k(\bar{t})) \in \partial \left(\bigcap_{j=1}^{M} C_j(\mathbf{q}_k(\tau_k)) \right).$$

Hence $\bar{t} = \varepsilon_t$ and therefore $\hat{\pi}((\mathbf{w}, \mathbf{q}, \mathbf{x})([\bar{t}, \tilde{t}]) = \pi_{j_t}(\mathbf{w}(\tilde{t}), \mathbf{q}(\tilde{t}), \mathbf{x}(\tilde{t}))$ for all $\tilde{t} \in [\bar{t}, t]$. This is however impossible since

$$(\mathbf{w}(\bar{t}), \mathbf{x}(\bar{t})) \in \partial C_{j_t}(\mathbf{q}(\bar{t})) \subset C_{j_t}(\mathbf{q}(\bar{t}))^c,$$

and establishes (9).
Notice that if $k = 0$ then (9) achieves the desired contradiction. We consider therefore the case when $k > 0$ and show that (9) implies that

$$(\mathbf{w}_{k-1}(\tau'_{k-1}), \mathbf{x}_{k-1}(\tau'_{k-1})) \in \bigcap_{j=1}^{M} C_j(\mathbf{q}_{k-1}(\tau_{k-1})). \tag{10}$$

Indeed using (9), (10) follows immediately from the very definition of $\hat{\pi}$ and $\bar{\pi}$.
Repeating these arguments we deduce that $(\omega, q, x) = (\mathbf{w}_0(\tau_0), \mathbf{q}_0(\tau_0), \mathbf{x}_0(\tau_0)) \in \bigcap_{j=1}^{M} C_j$ which achieves the desired contradiction and ends the proof. □

Lemma 3. *Let H, $\mathcal{B}$ and π^ℓ be as in Theorem 1. Then*

$$\mathcal{W}(\mathcal{B}) = C_{\pi^\ell}(\mathcal{B})^c.$$

Proof. It is clear that the inclusion $\mathcal{W}(\mathcal{B}) \supset C_{\pi^\ell}(\mathcal{B})^c$ holds. It suffices therefore to prove that

$$\mathcal{W}(\mathcal{B}) \subset C_{\pi^\ell}(\mathcal{B})^c.$$

To show this, let $\xi \in \mathcal{W}(\mathcal{B})$ be arbitrary. Then there exists $\pi \in \mathscr{F}$ such that for all $(\tau, \mathbf{d}) \in \mathcal{HT}(D)$ and all $\chi \in \mathscr{H}_\pi^{\mathbf{d}}(\xi)$, $\mathbf{y}(t) \preceq b^\ell$ for all $t \in \mathbb{R}_+$. However, since H is uniformly tightly bounded with respect to control it follows that for all $\chi^\ell \in \mathscr{H}_{\pi^\ell}^{\mathbf{d}}(\xi)$, $\mathbf{y}^\ell \preceq \mathbf{y}$. We conclude that $\xi \in C_{\pi^\ell}(\mathcal{B})^c$. □

A similar statement also holds if H is the parallel composition of bounded hybrid automata.

Lemma 4. *Let $H = H^1 \parallel H^2$, $\mathcal{B}$, $\pi^\uparrow = (\pi_1^\ell, \pi_2^u)$ be as in Theorem 2. Then $\mathcal{W}(\mathcal{B}) = C_{\pi^\uparrow}(\mathcal{B})^c$.*

Proof. It is equivalent to prove that $\mathcal{W}(\mathcal{B})^c = C_{\pi^\uparrow}(\mathcal{B})$. Since in addition it is clear that $\mathcal{W}(\mathcal{B})^c \subset C_{\pi^\uparrow}(\mathcal{B})$ it suffices to show the opposite inclusion. Let $\xi \in C_{\pi^\uparrow}(\mathcal{B})$. Then there exist $\chi^\uparrow \in \mathscr{H}_{\pi^\uparrow}(\xi)$ and $t \in \mathbb{R}_+$ such that $\mathbf{y}^\uparrow(t) \in \mathcal{B}$ which implies that $\mathbf{y}_1^\uparrow(t) \succeq b^1$ and $\mathbf{y}_2^\uparrow(t) \preceq b^2$. Then since H^i is uniformly tightly bounded, for all $\chi \in \mathscr{H}^{\mathbf{d}^\uparrow}(\xi)$, $\mathbf{y}_1 \succeq \mathbf{y}_1^\uparrow$ and $\mathbf{y}_2 \preceq \mathbf{y}_2^\uparrow$. Hence $\mathbf{y}(\mathbb{R}_+) \cap \mathcal{B} \neq \emptyset$ and thus $\xi \in \mathcal{W}(\mathcal{B})^c$. □

This completes the preparations and we are ready to proof Theorem 1. The proof of Theorem 2 is analogous and therefore omitted.

Proof of Theorem 1 By Lemmas 2 and 3 it is clear that $\bar{\pi}$ is safe for all $(\omega, q, x) \in \mathcal{W}(\mathcal{B})$. We have to show that there exists no $\pi \in \mathscr{F} \setminus \{\bar{\pi}\}$ that is safe for all $\mathcal{W}(\mathcal{B})$ and such that for some $\xi \in \operatorname{int} \mathcal{W}(\mathcal{B})$, $\bar{\pi}(\xi) \subset \pi(\xi)$.
Fix $\pi \in \mathscr{F}$ that is safe for all $\xi \in \mathcal{W}(\mathcal{B})$. Then for all $\xi \in \operatorname{int} \mathcal{W}(\mathcal{B}) = \overline{C_{\bar{\pi}}(\mathcal{B})}^c$ it is clear that $\pi(\xi) \subset \mathcal{E}_\pi(\xi; \mathcal{B})$. Moreover, since by Lemma 3

$$C_{\bar{\pi}}(\mathcal{B}) = \mathcal{W}(\mathcal{B})^c \subset C_\pi(\mathcal{B}) \quad \forall \pi \in \mathscr{F},$$

it follows that $\bar{\pi}(\xi) \supset \pi(\xi)$ for all $\xi \in \operatorname{int} \mathcal{W}(\mathcal{B})$. □

B Characterization of safe set

In this paragraph we proof Theorem 3. The proof of Theorem 4 is analogous and therefore omitted.

Proof of Theorem 3 We start with the inclusion

$$\mathcal{W}(\mathcal{B}) \subset \left\{ \xi \in \mathcal{X} \;\middle|\; \mathbf{y}_\xi^{\ell u}(\mathbb{R}_+) \cap \mathcal{B} = \emptyset \right\}. \tag{11}$$

Let $\xi \in \mathcal{W}(\mathcal{B})$. Then in particular for all $(\tau, \mathbf{d}) \in \mathcal{HT}(D)$

$$\mathbf{y}(\mathbb{R}_+) \cap \mathcal{B} = \emptyset \qquad \forall \chi \in \mathscr{H}_{\pi^\ell}^{\mathbf{d}}(\xi). \tag{12}$$

We have to show that $\mathbf{y}_\xi^{\ell u}(\mathbb{R}_+) \cap \mathcal{B} = \emptyset$. We argue by contradiction and assume instead that there exists $\bar{t} \in \mathbb{R}_+$ such that $\mathbf{y}_\xi^{\ell u}(\bar{t}) \in \mathcal{B}$. Then since $\mathcal{B}$ is open, there exists $\epsilon > 0$ such that $\mathbf{y}_\xi^{\ell u}(\bar{t}) + [-\epsilon, \epsilon] \subset \mathcal{B}$. However then it follows from the properties of $\mathbf{y}_\xi^{\ell u}$ that there exist $(\bar{\tau}, \bar{\mathbf{d}}) \in \mathcal{HT}(D)$ and $\bar{\chi} \in \mathscr{H}_{\pi^\ell}^{\bar{\mathbf{d}}}(\xi)$

such that for all $t \in [0, \bar{t}]$, $\left\| \bar{y}(t) - \mathbf{y}_{\xi}^{\ell u}(t) \right\| \leq \epsilon$. This implies that $\bar{y}(\bar{t}) \in \mathcal{B}$ which contradict (12) and thus achieves the proof of (11).
To show the opposite inclusion it suffices by Lemma 3 to show that

$$\left\{ \xi \in \mathcal{X} \;\middle|\; \mathbf{y}_{\xi}^{\ell u}(\mathbb{R}_+) \cap \mathcal{B} = \emptyset \right\} \subset \left\{ \xi \in \mathcal{X} \mid \mathbf{y}(\mathbb{R}_+) \cap \mathcal{B} = \emptyset \; \forall \chi \in \mathscr{H}_{\pi^\ell}(\xi) \right\},$$

where π^ℓ is as in Definition 11. This follows readily from the properties of $\mathbf{y}_{\xi}^{\ell u}$ and the definion of $\mathcal{B}$. $\square$

C Sufficient condition for bounded hybrid automata

In this paragraph we provide a proof of Theorem 5.

Proof of Theorem 5 First notice that by Proposition 1 we only have to proof that H is bounded. First we show that H is uniformly tightly bounded with respect to control. Indeed we show that $\pi^\ell \in \mathscr{F}$ defined as in Corollary 1 is such that for all $(\tau, \mathbf{d}) \in \mathcal{HT}(D)$ and all $\xi \in \mathcal{X}$, $\chi \in \mathscr{H}^{\mathbf{d}}(\xi)$ and $\chi^\ell \in \mathscr{H}^{\mathbf{d}}_{\pi^\ell}(\xi)$, $\mathbf{y}^\ell \preceq \mathbf{y}$. Analogous arguments can be used to show that π^u defined in Corollary 1 has the properties of π^u in Definition 11.
Let $(\tau, \mathbf{d}) \in \mathcal{HT}(D)$ and all $\xi \in \mathcal{X}$ be arbitrary and χ, χ^ℓ be as above. First we show by induction that

$$\tau_N^{\ell'} \leq \tau'_N \quad \forall N \in \{0, \ldots, \langle \tau^\ell - 1 \rangle\}. \tag{13}$$

The case $N = 0$ is clear since $\tau_N^{\ell'} = 0$ if $q \in Q_{\mathcal{E}}$ and mode transitions are caused by $\mathbf{d}$ otherwise, see condition (iii) in Theorem 5.
Consider therefore the case $N \to N+1$. The other cases being trivial we can assume that $\mathbf{q}^\ell(\tau_{N+1}^\ell) \in Q_D$ and $\tau_{N+1} \in I_{N+1}^\ell$. However in this case it follows from the fact that $(Q, \mathcal{A})$ forms a simple path and again condition (iii) of Theorem 5 that the statement holds.
Next we show again by induction that for all

$$\mathbf{y}^\ell(t) \preceq \mathbf{y}(t) \quad \forall t \leq \tau_N^{\ell'}, \; \forall N \in \{0, \ldots, \langle \tau^\ell - 1 \rangle\}.$$

We start with the case $N = 0$. If $q \in Q_{\mathcal{E}}$ then there is no continuous evolution and the statement is trivial. On the other hand, if $q \in Q \setminus Q_{\mathcal{E}}$ then it follows from the previous arguments that $\tau_0^{\ell'} = \tau'_0$ and thus the statement is a consequence of the order preserving property of $\Sigma(q)$, see condition (iv) of Theorem 5.
Consider next the case $N \to N+1$. Using (13) the statement follows readily from the induction hypothesis, and conditions (iv)-(v) of Theorem 5. This completes the first part of the proof.
The second part of the proof consists in showing that $\mathbf{y}^{\ell u}$ and $\mathbf{y}^{u\ell}$ defined in Corollary 2 satisfy conditions (i)-(ii) of Definition 12. In fact, (ii) follows directly from the definition of $\mathbf{y}^{\ell u}$ and $\mathbf{y}^{u\ell}$, condition (iii) of Theorem 5 and Gronwall's lemma. Therefore it remains to show (i), i.e. we have to show that

$$\mathbf{y}^\ell \preceq \mathbf{y}_{\xi}^{\ell u} \quad \forall \chi^\ell \in \mathscr{H}_{\pi^\ell}(\xi), \; \forall \xi \in \mathcal{X}.$$

To do this let $\xi \in \mathcal{X}$ and $\chi^\ell \in \mathscr{H}_{\pi^\ell}(\xi)$ be arbitrary. Let $\bar{j} \in \{0, \ldots, \langle \tau^\ell \rangle - 1\}$ be such that $\mathbf{q}_j^\ell(\tau_j) = \bar{q}$ where $\bar{q}$ is as in Corollary 2. By the very definition of π^ℓ it is clear that $\tau_j = 0$. Thus the statement follows readily from conditions (iv)-(v) of Theorem 5. The proof is complete.

References

[1] *Traffic safety facts 2013*.

[2] *The use of forward collision avoidance systems to prevent and mitigate rear-end crashes*, 2015.

[3] A. Aswani, H. Gonzalez, S. Sastry, and C. Tomlin, *Provably safe and robust learning-based model predictive control*, Automatica, 49 (2013), pp. 1216 – 1226.

[4] D. Del Vecchio, M. Malisoff, and R. Verma, *A separation principle for a class of hybrid automata on a partial order*, in American Control Conference, 2009, pp. 3638–3643.

[5] R. Ghaemi and D. Del Vecchio, *Control for safety specifications of systems with imperfect information on a partial order*, IEEE Trans. Aut. Control, 59 (2014), pp. 982–995.

[6] P. Kafka, *The automotive standard ISO 26262, the innovative driver for enhanced safety assessment & technology for motor cars*, Procedia Engineering, 45 (2012), pp. 2 – 10.

[7] J. Lygeros, K. Johansson, S. Simic, J. Zhang, and S. Sastry, *Dynamical properties of hybrid automata*, IEEE Transactions on Automatic Control, 48 (2003), pp. 2–17.

[8] J. Lygeros, C. J. Tomlin, and S. Sastry, *Controllers for reachability specifications for hybrid systems*, Automatica, 35 (1999), pp. 349–370.

[9] I. Mitchell, A. Bayen, and C. Tomlin, *A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games*, IEEE Trans. Aut. Control, 50 (2005), pp. 947–957.

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

[11] V. A. Shia, Y. Gao, R. Vasudevan, K. D. Campbell, T. Lin, F. Borrelli, and R. Bajcsy, *Semiautonomous vehicular control using driver modeling*, IEEE Trans. Intell. Transp. Syst., 15 (2014), pp. 2696–2709.

[12] R. Verma and D. Del Vecchio, *Safety control in hidden mode hybrid systems*, IEEE Trans. Automatic Control, 57 (2012), pp. 62–77.