# Safety Control of Hidden Mode Hybrid Systems

Rajeev Verma, *Student Member, IEEE,* and Domitilla Del Vecchio, *Member, IEEE,*

***Abstract*—In this paper, we consider the safety control problem for Hidden Mode Hybrid Systems (HMHSs), which are a special class of hybrid automata in which the mode is not available for control. For these systems, safety control is a problem with imperfect state information. We tackle this problem by introducing the notion of non-deterministic discrete information state and by translating the problem to one with perfect state information. The perfect state information control problem is obtained by constructing a new hybrid automaton, whose discrete state is an estimate of the HMHS mode and is, as such, available for control. This problem is solved by computing the capture set and the least restrictive control map for the new hybrid automaton. Sufficient conditions for the termination of the algorithm that computes the capture set are provided. Finally, we show that the solved perfect state information control problem is equivalent to the original problem with imperfect state information under suitable assumptions. We illustrate the application of the proposed technique to a collision avoidance problem between an autonomous vehicle and a human driven vehicle at a traffic intersection.**

***Index Terms*—Mode estimation, dynamic feedback, multi-agent systems.**

## I. Introduction

Hidden Mode Hybrid Systems (HMHSs) are a special class of hybrid automata [29, 39], in which the mode is unknown and mode transitions are driven only by disturbance events. There are a large number of applications that can be well described by hybrid automata models, in which it is not realistic to assume knowledge of the mode. This is the case, for example, of intent-based conflict detection and avoidance for aircrafts, in which the intent of aircrafts in the environment is unknown and needs to be estimated (see [45] and the references therein). In robotic games such as RoboFlag [11, 16], the intents of non-team members are unknown and need to be identified to allow decisions toward keeping the home zone safe. Next generation warning and active safety systems for vehicle collision avoidance will have to guarantee safety in the presence of human drivers and pedestrians, whose intentions are unknown [1]. More generally, in a variety of multi-agent systems, for example assistive robotics, computer games, and robot-human interaction, the intentions of an observed agent are unknown and need to be identified for control [21].

There has been a wealth of research on safety control for hybrid systems in which the state is known [5, 25, 26, 37, 39, 48–50]. In [39, 48–50], the safety control problem is elegantly formulated in the context of optimal control and leads to the Hamilton-Jacobi-Bellman (HJB) equation. This equation implicitly determines the maximal controlled invariant set and the least restrictive feedback control map. Due to the complexity of exactly solving the HJB equation, researchers have been investigating approximate algorithms for computing inner-approximations of the maximal controlled invariant set [30, 31, 44, 50]. Termination of the algorithm that computes the maximal controlled invariant set is often an issue and work has been investigating special classes of systems that allow to prove termination [46–48]. The safety control problem for hybrid systems has also been investigated within a viability theory approach by a number of researchers [5, 26].

The safety control problem for hybrid systems when the mode is not available for feedback has been rarely addressed in the literature. The safety control problem in the case when the set of observations is a partition of the state space was discussed by [43]. The proposed algorithm can deal with a system with finite number of states. It excludes important classes of systems such as timed and hybrid automata. A number of recent works have addressed the safety control problem for special classes of hybrid systems with imperfect state information [13, 15, 17, 28, 54]. In [54], a controller that relies on a state estimator is proposed for finite state systems. The results are then extended to control a class of rectangular hybrid automata with imperfect state information, which can be abstracted by a finite state system. In [15, 17, 28], linear complexity state estimation and control algorithms are proposed for special classes of hybrid systems with order preserving dynamics. In particular, discrete time models are considered in [13, 15] while continuous time models are considered in [17, 28]. In these works, the mode is assumed to be known and only continuous state uncertainty is considered.

Here, we consider the safety control problem for HMHSs, in which the mode is unknown and its transitions are driven only by uncontrollable and unobservable events. For this class of systems, designing a controller to guarantee safety is a control problem with imperfect state information. In the theory of games, control problems with imperfect state information have been elegantly addressed by translating them to problems with perfect state information [36, 38]. This transformation is obtained by introducing the notion of derived information state (non-deterministic or probabilistic), which, in the case of the non-deterministic information state, keeps track of the set of all possible current states compatible with the system history up to the current time. In the case in which a recursive update law can be constructed for the derived information state, the control problem can be described completely in terms of this new state. Since the derived information state is known, the problem becomes one with perfect state information.

In this paper, we introduce the notion of non-deterministic discrete information state for a HMHS and formulate the safety

R. Verma is with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI, 48109 USA. e-mail: rajverma@umich.edu.

D. Del Vecchio is with the Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA, 02139 USA. e-mail: ddv@mit.edu

control problem in terms of this derived information state. We translate this problem to one with perfect state information by introducing a new hybrid system called an estimator, which updates a discrete state estimate in the form of a set of possible discrete states. In this paper, we only require that the discrete state estimate is correct, that is, that it contains the current mode of the original HMHS at any time, while we are not concerned with tightness or convergence guarantees [18]. This ensures that an estimator always exists and allows to *separate* the estimation problem from the control problem. Since the estimator state is measured, the original control problem becomes one with perfect state information.

We solve the new perfect state information control problem by providing an algorithm to determine the capture set (the complement of the maximal controlled invariant set) and the least restrictive control map. Then, we provide sufficient conditions for the termination of the algorithm that determines the capture set. We further illustrate how to construct an abstraction of the estimator for which the algorithm that determines the capture set always terminates and has as fixed point the capture set of the estimator. Finally, we tackle the question of how the perfect state information problem that we have solved is related to the original problem with imperfect state information. Under a structural assumption and a mode distinguishability assumption on the original HMHS, we show that the two problems are equivalent, that is, their solution gives the same capture sets and control maps.

The problem considered in this paper has much in common with two-person repeated games of incomplete information, in which one player is informed about the environment state while the other is not [6, 27]. In these types of games, the informed player must take into account how his/her actions may reveal information that will affect future payoffs. The control of a HMHS can be viewed as a game between the controller (uninformed agent) and the disturbance (informed agent), in which the actions of the latter can reveal information on the current mode of the hybrid automaton. The equivalence result of this paper implies that the best strategy for the disturbance is simply to keep the maximal uncertainty possible on the mode. In doing so, it will in fact not reveal useful information to the controller regarding its range of action.

This paper is organized as follows. In Section II, we recall basic definitions and concepts. In Section III, we introduce the HMHS model and its information structure. In Section IV, we introduce the control problem with imperfect state information (Problem 1) and its translation to a problem with perfect state information (Problem 2). We then provide the solution to Problem 2 in Section V. We consider the problem of termination in Section VI. In Section VII, we show the equivalence of Problem 1 and Problem 2. In Section VIII, we illustrate the application of the proposed control algorithms to a collision avoidance problem at a traffic intersection.

## II. Basic notions and definitions

In this section, we introduce some basic notions and definitions. We employ basic notions from partial order theory [12]. A *partial order* is a set $P$ with a partial order relation "$\leq$" and it is denoted by $(P, \leq)$. If any two elements in $P$ have a unique supremum and a unique infimum in $P$, then $P$ is a lattice. If $(P, \leq)$ is a lattice, we denote for any subset $S \subseteq P$ its supremum by $\bigvee S$. For a set $X$, we denote by $2^X$ the power set, that is, the set of all subsets of $X$. In this paper, we consider the lattice given by $2^X$ with order established by set inclusion. This lattice is denoted by $(2^X, \subseteq)$. For any subset $S \subseteq 2^X$, the supremum $\bigvee S$ is given by the union of all sets in $S$. Another partial order that is considered in this paper is given by $\mathbb{R}^n$ with order established component-wise, that is, for $x = (x_1, ..., x_n) \in \mathbb{R}^n$ and $w = (w_1, ..., w_n) \in \mathbb{R}^n$, we say that $x \leq w$ provided $x_i \leq w_i$ for all $i \in \{1, ..., n\}$. We denote this partial order by $(\mathbb{R}^n, \leq)$. Let $(P, \leq)$ be a lattice, an interval in $P$ is denoted by $[L, U] := \{p \in P \mid L \leq p \leq U\}$. For any vector $v \in \mathbb{R}^n$, we denote by $v_i$ its ith component. Let $\mathbb{R}_+$ denote the set of non-negative real numbers and let $\mathbf{u} : \mathbb{R}_+ \to \mathbb{R}$ denote a signal with values in $\mathbb{R}$. Denote the set of all such signals by $\mathcal{S}(\mathbb{R})$. We define a partial order on this space of signals as follows. For any two signals $\mathbf{u}, \mathbf{w} \in \mathcal{S}(\mathbb{R})$, we say that $\mathbf{u} \leq \mathbf{w}$ provided $u(t) \leq w(t)$ for all $t \in \mathbb{R}$. Let $(P, \leq)$ and $(Q, \leq)$ be two partial orders and consider the map $f : P \to Q$. This map is said to be an *order preserving map* if for all $p_1, p_2 \in P$ such that $p_1 \leq p_2$, we have that $f(p_1) \leq f(p_2)$. It is said to be a *strongly order preserving map* if for all $p_1, p_2 \in P$ such that $p_1 < p_2$, we have that $f(p_1) < f(p_2)$. For any map $f : P \to Q$ and any subset $S \subseteq P$, we define $f(S) := \bigcup_{p \in S} f(p)$.

Notions from viability theory as found in [4] are here recalled. Let $X$ be a normed space and let $S \subset X$ be nonempty. The *contingent cone* to $S$ at $x \in S$ is the set given by $T_S(x) := \{v \in S \mid \liminf_{h \to 0+} \frac{d_S(x+h\,v)}{h} = 0\}$, in which $d_S(y)$ denotes the distance of $y$ from set $S$, that is, $d_S(y) := \inf_{z \in K} \|y - z\|$. When $S$ is an open set, the contingent cone to $S$ at any point in $S$ is always equal to the whole space.

A set valued map $F : X \to 2^X$ is said to be *Marchaud* provided (i) the graph and the domain of $F$ are nonempty and closed; (ii) for all $x \in X$, $F(x)$ is compact, convex and nonempty; (iii) $F$ has linear growth, that is, there exist $\alpha > 0$ such that for all $x \in X$ we have $\sup\{\|v\| \mid v \in F(x)\} \leq \alpha(\|x\|+1)$.

A set valued map $F : X \to 2^X$ is said to be *Lipschitz* continuous on $X$ if there is $\lambda > 0$ such that for all $x_1, x_2 \in X$ we have that $F(x_1) \subseteq F(x_2) + \lambda \|x_1 - x_2\| B_1(0)$, in which $B_1(0)$ is a ball in $X$ of radius 1 centered at 0.

## III. Hidden Mode Hybrid Systems

A hybrid system model with hidden modes is a hybrid automaton [39] in which the current mode of the system is unknown and mode transitions are driven by disturbance events only. This model is formally introduced by the following definitions.

**Definition 1.** A *hybrid system with uncontrolled mode transitions* is a tuple $H = (Q, X, U, D, \Sigma, R, f)$, in which $Q$ is a finite set of modes; $X$ is a vector space; $U$ is a set of control inputs; $D$ is a bounded set of disturbance inputs; $\Sigma$ is a finite set of disturbance events, which includes a silent event denoted $\epsilon$; $R : Q \times \Sigma \to Q$ is the discrete state update map; $f : X \times Q \times U \times D \to X$ is the vector field, which is piecewise continuous on $X \times U \times D$.

The vector field $f$ is allowed to be piece-wise continuous in order to model switches in the dynamics determined by submanifolds in the space of states and inputs. We denote by $(q, x) \in Q \times X$ the hybrid state of the system. Similarly, we denote by $(u, d) \in U \times D$ the continuous inputs to the system and by $\sigma \in \Sigma$ the disturbance event. We define $R(q, \epsilon) := q$ for all $q \in Q$. Let $\{\tau'_i\}_{i\in I} \subset \mathbb{R}$ for $I = \{0, 1, 2, ...\}$ with $\tau'_i \leq \tau'_{i+1}$ be the sequence of times at which $\sigma(\tau'_i) \in \Sigma/\epsilon$ and $\sigma(t) = \epsilon$ for $t \notin \{\tau'_i\}_{i\in I}$. Let $\mathcal{T} := \bigcup_{i\in I}[\tau_i, \tau'_i)]$ in which $\tau_i \leq \tau'_i = \tau_{i+1}$ with $\tau_0 = 0$, and the ")]" parenthesis is closed ("]") if $\tau'_i$ is finite and open (")") if it is not finite. Then, we define the discrete and continuous trajectories of $H$, that is, $q(t)$ and $x(t)$ for $t \in \mathcal{T}$ as follows.

**Definition 2.** Given initial conditions $(q_o, x_o) \in Q \times X$,

*the discrete trajectory* $q(t)$ for $t \in \mathcal{T}$ is such that $q(\tau_{i+1}) = R(q(\tau'_i), \sigma(\tau'_i))$ and $q(t) = q(\tau_i)$ for $t \in [\tau_i, \tau'_i]$ if $\tau_i < \tau'_i$ with $q(\tau_0) = q_o$;

*the continuous trajectory* $x(t)$ for $t \in \mathcal{T}$ is such that $\dot{x}(t) = f(x(t), q(t), u(t), d(t))$, $d(t) \in D$ for $t \in [\tau_i, \tau'_i]$ with $\tau_i < \tau'_i$ and $x(\tau_{i+1}) = x(\tau'_i)$ with $x(\tau_0) = x_o$.

Since we can have that $\tau'_i = \tau_{i+1}$, multiple discrete transitions can occur at one time. The value of $x$ immediately before and immediately after a set of transitions occurring at the same time is unchanged. The vector field $f$ immediately after a set of transitions occurring at the same time $t$ is evaluated on the value that $q$ takes after the last transition occurred at time $t$. It is therefore useful to define also the discrete and continuous flows of $H$ as follows. Let $\boldsymbol{\sigma} : \mathcal{T} \to \Sigma$, $\mathbf{u} : \mathcal{T} \to U$, and $\mathbf{d} : \mathcal{T} \to D$ be the disturbance event, the continuous control, and the continuous disturbance signals.

**Definition 3.** For initial condition $(q_o, x_o) \in Q \times X$,

*the discrete flow* is defined as $\phi_q(t, q_o, \boldsymbol{\sigma}) := q(\sup_{\tau_i \leq t} \tau_i)$ for all $t \geq 0$;

*the continuous flow* is defined as $\phi_x(t, (q_o, x_o), \mathbf{u}, \mathbf{d}, \boldsymbol{\sigma}) := x(t)$ in which $\dot{x}(t) = f(x(t), \phi_q(t, q_o, \boldsymbol{\sigma}), u(t), d(t))$, $d(t) \in D$ for all $t \geq 0$.

Therefore, $\phi_q(t, q_o, \boldsymbol{\sigma})$ is a piece-wise constant signal that at time $t$ takes the value of $q$ at the last transition that occurred before or at time $t$. When $\sigma(t) = \epsilon$ for all $t$, we denote the corresponding continuous flow by $\phi_x(t, (q_o, x_o), \mathbf{u}, \mathbf{d}, \epsilon)$.

**Definition 4.** A *Hidden Mode Hybrid System* (HMHS) is a hybrid system with uncontrolled mode transitions in which $q(t)$ is not measured and $q_o$ is only known to belong to a set $\bar{q}_o \subseteq Q$.

Therefore, in a HMHS only $x(t)$ is measured and its evolution is driven by hidden mode transitions. In the reminder of this paper, $H$ denotes a HMHS.

**Definition 5.** Let $\bar{q} \subseteq Q$. The set of modes *reachable* from $\bar{q}$ under the trajectories of $H$ is denoted $\text{Reach}(\bar{q}) \subseteq Q$ and is defined as $\text{Reach}(\bar{q}) := \bigcup_{q_o\in\bar{q}} \bigcup_{t\geq 0} \bigcup_{\sigma} \phi_q(t, q_o, \boldsymbol{\sigma})$.

*Remark* 1. The hybrid automaton model considered in this paper is a special case of more general models [29, 39]. Specifically, we assume that there is no continuous state reset, that mode transitions cannot be controlled, and that no mode in $Q$ has a non-zero minimum dwell time (as it would be enforced by suitable interaction between guards and invariants). As a consequence, any mode in $Q$ can instantaneously transit to any element in its reachable set $\text{Reach}(q)$. Even though this structure limits the generality of the model, it still well captures application scenarios of interest, as described in Section IV-B.

### A. The non-deterministic discrete information state

For a signal $\mathbf{s} : \mathbb{R}_+ \to S$, we define its truncation up to time $t$ as $\mathbf{s}_t : [0, t] \to S$ and its truncation up to time $t^-$ as $\mathbf{s}_{t^-} : [0, t) \to S$. At time $t$, the measured signals of $H$ are given by $\mathbf{u}_{t^-}$ and $\mathbf{x}_t$, in which $\mathbf{x_0} := x_o$. Furthermore, the knowledge of the function $\mathbf{x}_t : [0, t] \to X$ implies that also the function $\dot{\mathbf{x}}_{t^-} : [0, t) \to X$ is known.

**Definition 6.** The *history* of system $H$ at time $t$ for $t \geq 0$ is defined as $\boldsymbol{\eta}(t) := (\bar{q}_o, \mathbf{u}_{t^-}, \mathbf{x}_t, \dot{\mathbf{x}}_{t^-})$, in which for $\bar{q}_o \subseteq Q$ is the initial mode information.

The available *information* on the system mode at time $t$ must be derived from the history signal $\boldsymbol{\eta}(t)$, in which $\eta(0) = (\bar{q}_o, \emptyset, x_o, \emptyset)$ contains information on the initial state of the system. We define the set of all possible current modes of the system compatible with the history. This set is called the non-deterministic discrete information state and is formally defined as follows in analogy to what is performed in the theory of games with imperfect information [38].

**Definition 7.** The *non-deterministic discrete information state* at time $t \geq 0$ for system $H$ is the set $\bar{q}(\boldsymbol{\eta}(t)) \subset Q$ defined as

$$\bar{q}(\boldsymbol{\eta}(t)) := \left\{ \begin{array}{r} q \in Q \mid \exists\, q_o \in \bar{q}_o,\ \boldsymbol{\sigma}\ s.t.\ q = \phi_q(t, q_o, \boldsymbol{\sigma}) \\ \text{and } \exists\, \mathbf{d}\ s.t. \dot{x}(\tau) = f(x(\tau), \phi_q(\tau, q_o, \boldsymbol{\sigma}), u(\tau), d(\tau)) \\ \text{for all } 0 \leq \tau < t \end{array} \right\}.$$

Hence, a mode $q$ is possible at time $t$ provided (a) there is a discrete state trajectory starting from a mode in $\bar{q}_o$ that reaches $q$ at time $t$ and (b) such a discrete state trajectory is consistent with the continuous state trajectory up to time $t$. It follows that $q(t) \in \bar{q}(\boldsymbol{\eta}(t))$ for all $t$ and that $\bar{q}(\boldsymbol{\eta}(0)) = \text{Reach}(\bar{q}_o)$.

## IV. Problem Formulation

In this section, we first employ the notion of non-deterministic discrete information state to formulate the safety control problem with imperfect state information. Then, we translate this problem to one with perfect state information by introducing a mode estimator.

### A. Safety control problem with imperfect mode information

Let $Bad \subset X$ represent a set of unsafe continuous states. We consider the problem of determining the set of all initial informations $(\bar{q}_o, x_o)$ for which a *dynamic feedback* map does not exist that maintains the trajectory $x(t)$ outside $Bad$ for all time. For this purpose, we first define the closed loop system $H$ under a feedback map $\pi : 2^Q \times X \to U$.

**Definition 8.** Consider a feedback map $\pi : 2^Q \times X \to U$. The *closed loop system* $H^\pi$ is defined as system $H$, in which

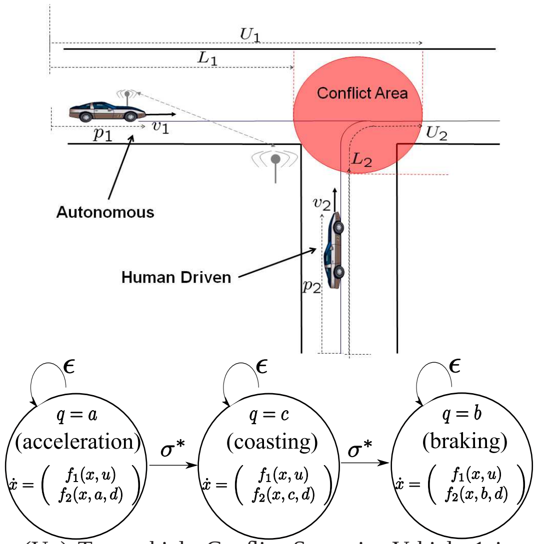


Fig. 1. (Up) Two-vehicle Conflict Scenario. Vehicle 1 is equipped with a cooperative active safety system and communicates with the infrastructure wirelessly. Vehicle 2 does not communicate with the infrastructure. A collision occurs when both vehicles occupy the conflict area. We refer to vehicle 1 as the "autonomous vehicle" and to vehicle 2 as the "human driven vehicle". (Down) Hybrid automaton model $H$, in which $f_1$ and $f_2$ are given by equations (1-2).

$u(t) = \pi(\bar{q}(\boldsymbol{\eta}(t)), x(t))$ for all $t \geq 0$. The continuous flow of $H^\pi$ is denoted $\phi_x^\pi(t, (q_o, x_o), \mathbf{d}, \boldsymbol{\sigma})$.

The set of all initial informations $(\bar{q}_o, x_o)$ for which there is no feedback map $\pi$ that maintains the trajectory $\phi_x^\pi(t, (q_o, x_o), \mathbf{d}, \boldsymbol{\sigma})$ outside *Bad* for all $q_o \in \bar{q}_o$, $\boldsymbol{\sigma}$, and $\mathbf{d}$ is called the *capture set* and is formally defined as follows.

**Definition 9.** For $Bad \subseteq X$, the *capture set* for system $H$ is defined as $C := \{(\bar{q}_o, x_o) \in 2^Q \times X \mid \forall\, \pi,\ \exists\, q_o \in \bar{q}_o,\ \boldsymbol{\sigma},\ \mathbf{d},\ t \geq 0,\ s.t.\ \phi_x^\pi(t, (q_o, x_o), \mathbf{d}, \boldsymbol{\sigma}) \in Bad\}$.

The following alternative expression of the capture set (obtained directly from the definition) is used in this paper.

**Proposition 1.** *For all $\bar{q} \in 2^Q$, let the mode-dependent capture set be defined as $C_{\bar{q}} := \{x_o \in X \mid \forall\, \pi,\ \exists\, q_o \in \bar{q},\ \boldsymbol{\sigma},\ \mathbf{d},\ t \geq 0,\ s.t.\ \phi_x^\pi(t, (q_o, x_o), \mathbf{d}, \boldsymbol{\sigma}) \in Bad\}$. Then, $C = \bigcup_{\bar{q} \in 2^Q} (\bar{q} \times C_{\bar{q}})$.*

**Proposition 2.** *For all $\bar{q} \in 2^Q$, we have that $C_{\bar{q}} = C_{Reach(\bar{q})}$.*

*Proof:* We first show that $C_{\bar{q}} \subseteq C_{\mathrm{Reach}(\bar{q})}$. Let $x_o \notin C_{\mathrm{Reach}(\bar{q})}$. Then, there is a feedback map $\pi^*$ such that for all $q_o \in \mathrm{Reach}(\bar{q})$ and $t \geq 0$ we have that $\phi_x^{\pi^*}(t, (q_o, x_o), \mathbf{d}, \boldsymbol{\sigma}) \notin Bad$ for all $\mathbf{d}$, $\boldsymbol{\sigma}$, and $\boldsymbol{\eta}$ with $\boldsymbol{\eta}(0)$ such that $\bar{q}(\boldsymbol{\eta}(0)) = \mathrm{Reach}(\bar{q})$. In particular, such $\pi^*$ is such that for all $q_o \in \bar{q}$ and $t \geq 0$, $\phi_x^{\pi^*}(t, (q_o, x_o), \mathbf{d}, \boldsymbol{\sigma}) \notin Bad$ for all $\mathbf{d}$, $\boldsymbol{\sigma}$, and $\boldsymbol{\eta}$ with $\boldsymbol{\eta}(0)$ such that $\bar{q}(\boldsymbol{\eta}(0)) = \mathrm{Reach}(\bar{q})$. This, in turn, implies that $x_o \notin C_{\bar{q}}$ from the definition of $C_{\bar{q}}$ and the fact that $\boldsymbol{\eta}(0) = (\bar{q}, \emptyset, x_o, \emptyset)$ implies $\bar{q}(\boldsymbol{\eta}(0)) = \mathrm{Reach}(\bar{q})$.

We then show that $C_{\mathrm{Reach}(\bar{q})} \subseteq C_{\bar{q}}$. Let $x_o \notin C_{\bar{q}}$. Then, there is $\pi^*$ in which $\bar{q}(\boldsymbol{\eta}(0)) = \mathrm{Reach}(\bar{q})$ such that for all $q_o \in \bar{q}$, $\boldsymbol{\sigma}$, $\mathbf{d}$, we have that $\phi_x^{\pi^*}(t, (q_o, x_o), \mathbf{d}, \boldsymbol{\sigma}) \notin Bad$ for all $t$. For all $q_j \in \mathrm{Reach}(\bar{q})$, there is $\boldsymbol{\sigma}$ and $q_o \in \bar{q}$ such that $\phi_q(0, q_o, \boldsymbol{\sigma}) = q_j$. Therefore, for any piece-wise continuous signal $\phi_q(t, q_o', \boldsymbol{\sigma}')$ with $q_o' \in \mathrm{Reach}(\bar{q})$, we can find $\boldsymbol{\sigma}$ and $q_o \in \bar{q}$ such that $\phi_q(t, q_o, \boldsymbol{\sigma}) = \phi_q(t, q_o', \boldsymbol{\sigma}')$ for all $t \geq 0$. This implies that the feedback map $\pi^*$ is such that $\phi_x^{\pi^*}(t, (q_o', x_o), \mathbf{d}, \boldsymbol{\sigma}') \notin Bad$ for all $t$, $\boldsymbol{\sigma}'$, and $q_o' \in \mathrm{Reach}(\bar{q})$. Hence, $x_o \notin C_{\mathrm{Reach}(\bar{q})}$. ■

**Problem 1.** (Safety Control with Imperfect State Information) Determine the capture set $C$ and the set of feedback maps $\pi$ such that if $(\bar{q}_o, x_o) \notin C$, then $(\bar{q}(\boldsymbol{\eta}(t)), \phi_x^\pi(t, (q_o, x_o), \mathbf{d}, \boldsymbol{\sigma})) \notin C$ for all $t \geq 0$, $\mathbf{d}$, $\boldsymbol{\sigma}$, and $q_o \in \bar{q}_o$.

### B. Motivating example

In this section, we present an example in the context of cooperative active safety at traffic intersections [1], wherein a controlled vehicle has to prevent a collision with a non-controlled/non-communicating, possibly human-driven, vehicle (Figure 1). A possible approach to tackle this problem is to treat the non-communicating vehicle as a "disturbance" and employ available safety control techniques for hybrid systems with measured state. This approach, however, leads to conservative controllers, which are not acceptable as they result in warnings/control actions that the driver perceives as unnecessary. Therefore, in this application it is crucial to exploit all the available sensory information to reduce as much as possible the uncertainty on the non-communicating vehicle. For the controller on board the autonomous vehicle, the human-driven vehicle is a hybrid automaton with unknown state. A related but different application is the one in which a single vehicle can receive inputs from both a human driver and an on-board controller as considered, for example, by [40] in the context of a red-light violation problem. As opposed to our application, the resulting hybrid automaton to control in [40] has known state.

Since both vehicles are constrained to move along their lanes (see Figure 1), only the longitudinal dynamics of the vehicles along their respective paths are relevant. The longitudinal dynamics of vehicle 1 along its path are modeled by the equation $\ddot{p}_1 = k_1 u - k_2 v_1^2 - k_3$, in which $p_1, v_1$ are the longitudinal displacement and speed along the path, respectively, $u$ represents throttle/braking, $k_3 > 0$ represents the static friction term, and $k_2 v_1^2$ with $k_2 > 0$ models air drag (see [52] for more details). The control input $u$ ranges in the interval $[u_L, u_H]$ for given maximum braking action $u_L < 0$ and maximum throttle action $u_H > 0$. For vehicle 2, we assume a model given by $\ddot{p}_2 = \beta_q + d$, in which $d \in [-\bar{d}, \bar{d}]$ for some $\bar{d} > 0$ and $q$ represents the *unknown* driving mode that can be acceleration mode, denoted $a$, coasting mode, denoted $c$, and braking mode, denoted $b$. For each mode, $\beta_q$ has a different value representing the nominal acceleration corresponding to that mode. For more details on modeling human (controlled) activities through non-deterministic hybrid systems, the reader is referred to [19, 20]. Vehicle 1 receives information about the position and speed of vehicle 2 from the infrastructure, which monitors speed and position of vehicles through road-side sensors. We assume that there are a lower bound $v_{min}$ and an upper bound $v_{max}$ on the achievable speed of the vehicles due, for example, to physical limitations (i.e., vehicles cannot go in reverse and have a finite maximum achievable speed).

The resulting HMHS $H = (Q, X, U, D, \Sigma, R, f)$ modeling the system is such that $Q = \{a, b, c\}$, $X = \mathbb{R}^4$, $U = [u_L, u_H]$, and

$D = [-\overline{d}, \overline{d}]$. Denote $x = (x_1, x_2, x_3, x_4)$ with $x_1 = p_1, x_2 = v_1, x_3 = p_2, x_4 = v_2$. Let $\alpha := k_1 u - k_2 x_2^2 - k_3$. The vector field $f$ is piece-wise continuous and given by $f(x, q, u, d) = (f_1(x, u), f_2(x, q, d))$, with

$$f_1(x,u) = \begin{cases} (x_2, \alpha), & \text{if } x_2 \in (v_{min}, v_{max}) \\ (x_2, 0), & \text{if } x_2 \leq v_{min} \text{ and } \alpha < 0 \\ & \text{or } x_2 \geq v_{max} \text{ and } \alpha > 0 \end{cases} \tag{1}$$

$$f_2(x,q,d) = \begin{cases} (x_4, \beta_q + d), & \text{if } x_4 \in (v_{min}, v_{max}) \\ (x_4, 0), & \text{if } x_4 \leq v_{min} \text{ and } \beta_q + d < 0 \\ & \text{or } x_4 \geq v_{max} \text{ and } \beta_q + d > 0. \end{cases} \tag{2}$$

We assume that the human driven vehicle can transit from acceleration, to coasting, to braking [35]. This scenario can be modeled by $\Sigma = \{\epsilon, \sigma^*\}$ and $R : Q \times \Sigma \to Q$ such that $R(a, \sigma^*) = c$ and $R(c, \sigma^*) = b$. Here, we assume that $\beta_b < 0$, $\beta_c = 0$, and $\beta_a > 0$, with $\overline{d} < |\beta_q| < 2\overline{d}$ for $q \in \{a, b\}$. This system is a HMHS, in which $\overline{q}_o = \{a, b, c\}$ and it is pictorially represented in the right-side plot of Figure 1. Finally, the unsafe set is given by $Bad = \{x \mid (x_1, x_3) \in [L_1, U_1] \times [L_2, U_2]\}$ corresponding to both vehicles constrained to their paths being in the conflict area of Figure 1.

### C. Translation to a perfect state information control problem

In order to solve Problem 1, it is necessary to compute the set $\overline{q}(\boldsymbol{\eta}(t))$. Computing this set from its definition is impractical as one would need to keep track of a growing history. Hence, it is customary to determine it recursively through a suitable update law [38]. A wealth of research on observer design and state estimation for hybrid systems has been concerned with determining such an update law and in particular with its properties for special classes of hybrid systems [7–9, 14, 16, 18, 23, 53]. Specifically, key properties, when considering discrete state estimation, are correctness, tightness, and convergence [14, 18]. Correctness requires that the estimated set of modes contains the true mode at any time; tightness requires that the estimated set of modes contains only modes compatible with the system history and dynamics; convergence requires that the estimated set converges to a singleton. In this paper, we only require that the discrete state estimator has the correctness property. We are not concerned with tightness nor with convergence guarantees, which usually require observability assumptions. Hence, a discrete state estimator always exists as, for example, $\hat{q}(t) \equiv Q$ for all $t$ is also an estimator. This allows us to *separate* the design of the estimator from that of the control map.

More formally, let $\hat{H} = (\hat{Q}, X, U, D, Y, \hat{R}, \hat{f})$ be a hybrid system with uncontrolled mode transitions with state $(\hat{q}, \hat{x}) \in \hat{Q} \times X$, in which $\hat{Q} \subseteq 2^Q$, and disturbance events $y \in Y$. Let $\{\hat{\tau}'_i\}_{i \in \hat{I}} \subset \mathbb{R}$ for $\hat{I} = \{0, 1, 2, 3, ...\}$ with $\hat{\tau}'_i = \hat{\tau}_{i+1} \leq \hat{\tau}'_{i+1}$ be the sequence of times at which $y(\hat{\tau}'_i) \in Y/\epsilon$ and $y(t) = \epsilon$ for $t \notin \{\hat{\tau}'_i\}_{i \in \hat{I}}$. Denote $\hat{\mathcal{T}} := \bigcup_{i \in \hat{I}} [\hat{\tau}_i, \hat{\tau}'_i)]$ in which $\hat{\tau}_i \leq \hat{\tau}'_i = \hat{\tau}'_{i+1}$, and $\hat{\tau}_0 = \tau_0 = 0$. For all $\hat{q} \in \hat{Q}$, we define $\hat{R}(\hat{q}, \epsilon) := \hat{q}$. Let the initial state be $(\overline{q}_o, x_o) \in \hat{Q} \times X$. The trajectories of $\hat{H}$ are defined as in Definition 2, in which the continuous state obeys the differential inclusion

$$\dot{\hat{x}}(t) \in \hat{f}(\hat{x}(t), \hat{q}(t), v(t), d(t)), \; d(t) \in D, \; \text{for } t \in [\hat{\tau}_i, \hat{\tau}'_i], \; \hat{\tau}_i < \hat{\tau}'_i,$$

in which $\hat{x}(\hat{\tau}_{i+1}) = x(\hat{\tau}'_i)$ and $\hat{x}(\tau_0) = x_o$. As performed for system $H$, we can define the flow of system $\hat{H}$. Specifically, the discrete flow of $\hat{H}$ is denoted $\phi_{\hat{q}}(t, \overline{q}_o, \mathbf{y}) := \hat{q}(\sup_{\hat{\tau}_i \leq t} \hat{\tau}_i)$ and *any* continuous flow of $\hat{H}$ is denoted by $\phi_{\hat{x}}(t, (\overline{q}_o, x_o), \mathbf{v}, \mathbf{d}, \mathbf{y}) := \hat{x}(t)$ for all $t \geq 0$. When $\mathbf{y} = \epsilon$, it is useful to extend the definition of this flow to when $\overline{q}$ is any element in $2^Q$, that is, $\phi_{\hat{x}}(t, (\overline{q}, x_o), \mathbf{v}, \mathbf{d}, \epsilon) := \hat{x}(t)$ with $\hat{x}(t)$ such that $\dot{\hat{x}}(t) \in \hat{f}(\hat{x}(t), \overline{q}, v(t), d(t))$ for all $t > 0$ and $x(0) = x_o$. Note that, however, this may not be realizable in $\hat{H}$ if $\overline{q} \notin \hat{Q}$. Also, for all $\overline{q}_o \in \hat{Q}$, we denote $\widehat{\text{Reach}}(\overline{q}_o) \subseteq \hat{Q}$ the set of reachable modes from $\overline{q}_o$ and it is defined as $\widehat{\text{Reach}}(\overline{q}_o) := \bigcup_{t \geq 0} \bigcup_{\mathbf{y}} \phi_{\hat{q}}(t, \overline{q}_o, \mathbf{y})$. Then, we have the following definition of an estimator for $H$.

**Definition 10.** The hybrid system with uncontrolled mode transitions $\hat{H}$ with initial state $(\overline{q}_o, x_o) \in \hat{Q} \times X$ is called an *estimator* for $H$ provided

(i) for all input/output signals $(\mathbf{u}, \mathbf{x})$ of $H$ and all initial mode informations $\overline{q}_o \in \hat{Q}$, there is an event signal $\mathbf{y}$ in $\hat{H}$ such that $\phi_{\hat{q}}(t, \overline{q}_o, \mathbf{y}) \ni q(t)$ for all $t \in \mathcal{T}$;
(ii) for all $y \in Y$ and $\hat{q} \in \hat{Q}$, we have that $\hat{R}(\hat{q}, y) \subseteq \text{Reach}(\hat{q})$;
(iii) for all $(\hat{x}, \hat{q}, v, d) \in X \times \hat{Q} \times U \times D$, we have that $\hat{f}(\hat{x}, \hat{q}, v, d) = \bigcup_{q \in \hat{q}} f(\hat{x}, q, v, d)$.

The dynamics of $\hat{x}$ model for a suitable event signal $\mathbf{y}$ the set of all possible dynamics of $x$ in system $H$ compatible with the current mode estimate $\hat{q}(t)$. Note that in $H$ we can have that $\tau'_0 = \tau_0$ with the mode $q(\tau'_0)$ taking any value in $\text{Reach}(\overline{q}_o)$. Since by (i) of the above definition $\overline{q}_o$ can be any element of $\hat{Q}$, we must have that for all $\hat{q} \in \hat{Q}$ there is $y \in Y$ such that $\hat{R}(\hat{q}, y) = \text{Reach}(\hat{q})$ to ensure that $\phi_{\hat{q}}(t, \overline{q}_o, \mathbf{y}) \ni q(t)$. According to the above definition, an estimator always exists as one can choose, for example, $\hat{Q} = \{\overline{q}_o, \text{Reach}(\overline{q}_o)\}$, $Y = \{\epsilon, y_0\}$, $\hat{R}$ such that $\hat{R}(\overline{q}_o, y_0) = \text{Reach}(\overline{q}_o)$, $\hat{\tau}'_0 = \hat{\tau}_0$, and $y(\hat{\tau}'_0) = y_0$. This implies that $\hat{q}(\hat{\tau}_0) = \overline{q}_o$, that $\hat{q}(\hat{\tau}'_0) = \text{Reach}(\overline{q}_o)$, and that $\hat{q}(\hat{\tau}'_0) \equiv \text{Reach}(\overline{q}_o)$ for all $t \geq \hat{\tau}'_0$. Hence, $\phi_{\hat{q}}(t, \overline{q}_o, \mathbf{y}) \equiv \text{Reach}(\overline{q}_o)$ always contains $q(t)$ for all $t \in \mathcal{T}$ as $q(t) \in \text{Reach}(\overline{q}_o)$ for all $t \in \mathcal{T}$. An example of how to construct a less trivial estimator is provided in the following paragraph.

*Example* 1. Consider the HMHS $H = (Q, \underline{X}, \underline{U}, D, \Sigma, R, \underline{f})$, in which $X = \mathbb{R}^2$, $Q = \{a, b\}$, $U = \emptyset$, $D = [-\overline{d}, \overline{d}] \subset \mathbb{R}$ for $\overline{d} > 0$, $\Sigma = \{\epsilon\}$, and $f(x, d) = (x_2, \beta_q + d)$, in which $\beta_q$ is a parameter whose value depends on the mode $q$. This system can model, for example, the non-communicating vehicle of the application example of Section IV-B, in which "$a$" is acceleration mode and "$b$" is braking mode. Let the initial information be $(\overline{q}_o, x_o)$, in which $\overline{q}_o = Q$. We let $\hat{Q} = \{\hat{q}_1, \hat{q}_2, \hat{q}_3\}$, in which $\hat{q}_1 = Q$, $\hat{q}_2 = \{a\}$, and $\hat{q}_3 = \{b\}$. The signal $\mathbf{y}$ determines how to transit among these modes on the basis of $x(t)$ so to guarantee that $\phi_{\hat{q}}(t, \overline{q}_o, \mathbf{y}) \ni q(t)$. Since $R$ does not allow transitions between $a$ and $b$, the only transitions allowed by $\hat{R}$ are from $\hat{q}_1$ to $\hat{q}_2$ and from $\hat{q}_1$ to $\hat{q}_3$ by property (ii) of Definition 10. Then, let $Y = \{y_a, y_b, \epsilon\}$, in which $y_a$ is such that $\hat{R}(\hat{q}_1, y_a) = \hat{q}_2$ and $y_b$ is such that $\hat{R}(\hat{q}_1, y_b) = \hat{q}_3$. Let $\hat{\beta}(t) = \frac{1}{T} \int_{t-T}^{t} \dot{x}_2(\tau) d\tau$, $t > T$ and define $y(t)$ as $y(t) = y_a$ if $|\hat{\beta}(t) - \beta_b| > \overline{d}$, $y(t) = y_b$ if $|\hat{\beta}(t) - \beta_a| > \overline{d}$, and $y(t) = \epsilon$ otherwise.

Note that while the discrete state of system $H$ is unknown, the discrete state of system $\hat{H}$ is known as its initial state is known and both $\hat{q}(t)$ and $\hat{x}(t)$ are measured. Hence, we define the closed loop system under a *static* feedback map as follows.

**Definition 11.** Consider a feedback map $\hat{\pi} : \hat{Q} \times X \to U$. The *closed loop system* $\hat{H}^{\hat{\pi}}$ is defined as system $\hat{H}$, in which $v(t) = \hat{\pi}(\phi_{\hat{Q}}(t, \overline{q}_o, \mathbf{y}), \hat{x}(t))$ for all $t \geq 0$. The flow of $\hat{H}^{\hat{\pi}}$ is denoted by $\hat{\phi}^{\hat{\pi}}(t, (\overline{q}_o, x_o), \mathbf{d}, \mathbf{y})$ and the continuous flow by $\phi^{\hat{\pi}}_{\hat{x}}(t, (\overline{q}_o, x_o), \mathbf{d}, \mathbf{y})$.

**Definition 12.** The capture set for system $\hat{H}$ is denoted $\hat{C}$ and is given by $\hat{C} := \{(\overline{q}_o, x_o) \in \hat{Q} \times X \,|\, \forall \hat{\pi}, \exists \mathbf{d}, \mathbf{y}, t \geq 0 \text{ s.t. some } \phi^{\hat{\pi}}_{\hat{x}}(t, (\overline{q}_o, x_o), \mathbf{d}, \mathbf{y}) \in Bad\}$.

**Proposition 3.** *Let $\overline{q} \in \hat{Q}$ and define the mode-dependent capture set $\hat{C}_{\overline{q}} := \{x_o \in X \,|\, \forall \hat{\pi}, \exists \mathbf{d}, \mathbf{y}, t \geq 0 \text{ s.t. some } \phi^{\hat{\pi}}_{\hat{x}}(t, (\overline{q}, x_o), \mathbf{d}, \mathbf{y}) \in Bad\}$. Then, we have that $\hat{C} = \bigcup_{\overline{q} \in \hat{Q}} \left(\overline{q} \times \hat{C}_{\overline{q}}\right)$.*

**Problem 2.** (Safety Control with Perfect State Information) Let $\hat{H}$ be an estimator for $H$. Determine the capture set $\hat{C}$ and the set of feedback maps $\hat{\pi}$ such that if $(\overline{q}_o, x_o) \notin \hat{C}$, then all flows $(\phi_{\hat{Q}}(t, \overline{q}_o, \mathbf{y}), \phi^{\hat{\pi}}_{\hat{x}}(t, (\overline{q}, x_o), \mathbf{d}, \mathbf{y})) \notin \hat{C}$ for all $t \geq 0$, $\mathbf{d}$, and $\mathbf{y}$.

**Definition 13.** Consider the feedback map $\hat{\pi} : \hat{Q} \times X \to U$ and an estimator $\hat{H}$. The *estimator-based closed loop system* $H^{\hat{\pi}}_e$ is defined as system $H$, in which $u(t) = \hat{\pi}(\phi_{\hat{Q}}(t, \overline{q}_o, \mathbf{y}), x(t))$ for all $t \geq 0$.

**Definition 14.** We say that system $\hat{H}^{\hat{\pi}}$ with initial state $(\overline{q}_o, x_o)$ is safe provided $(\overline{q}_o, x_o) \notin \hat{C}$ implies that $\hat{x}(t) \notin Bad$ for all $t$, $\mathbf{d}$, and $\mathbf{y}$. Similarly, we say that system $H^{\hat{\pi}}_e$ with initial information $(\overline{q}_o, x_o)$ is safe provided $(\overline{q}_o, x_o) \notin \hat{C}$ implies that $x(t) \notin Bad$ for all $t$, $\mathbf{d}$, and $\boldsymbol{\sigma}$.

**Definition 15.** (Weak equivalence) We say that Problem 1 and Problem 2 are *weakly equivalent* provided that (i) if $\hat{H}^{\hat{\pi}}$ with initial state $(\overline{q}_o, x_o)$ is safe then also $H^{\hat{\pi}}_e$ with initial information $(\overline{q}_o, x_o)$ is safe; (ii) for all $\overline{q} \in \hat{Q}$, we have that $C_{\overline{q}} \subseteq \hat{C}_{\overline{q}}$.

**Definition 16.** (Equivalence) We say that Problem 1 and Problem 2 are *equivalent* provided that (i) they are weakly equivalent; (ii) for all $\overline{q} \in \hat{Q}$, we have that $C_{\overline{q}} = \hat{C}_{\overline{q}}$.

Weak equivalence guarantees that any feedback map $\hat{\pi}$ that keeps $\hat{H}^{\hat{\pi}}$ safe keeps also system $H^{\hat{\pi}}_e$ safe. Equivalence guarantees that system $\hat{H}$ has the same mode-dependent capture sets as system $H$.

**Proposition 4.** *Problem 1 and Problem 2 are weakly equivalent.*

*Proof:* (i) If $\hat{H}^{\hat{\pi}}$ is safe with initial state $(\overline{q}_o, x_o)$, we have that $(\overline{q}_o, x_o) \notin \hat{C}$ implies that $\hat{x}(t) \notin Bad$ for all $t$, $\mathbf{d}$, and $\mathbf{y}$. In particular, this is true for $\mathbf{y}$ such that $\phi_{\hat{Q}}(t, \overline{q}_o, \mathbf{y}) \ni q(t)$ for all $t$ and hence for $\hat{x}^*(t)$ such that $\dot{\hat{x}}^*(t) = f(\hat{x}^*(t), q(t), \hat{\pi}(\phi_{\hat{Q}}(t, \overline{q}_o, \mathbf{y}), \hat{x}^*(t)), d(t))$, $d(t) \in D$, and hence for $x(t)$ trajectory of $H^{\hat{\pi}}_e$.

(ii) We show that $C_{\overline{q}} \subseteq \hat{C}_{\overline{q}}$ for all $\overline{q} \in \hat{Q}$. Specifically, we show that if $x_o \notin \hat{C}_{\overline{q}}$ then $x_o \notin C_{\overline{q}}$. If $x_o \notin \hat{C}_{\overline{q}}$, there is a feedback map $\hat{\pi}$ such that for all $\mathbf{d}$, $\mathbf{y}$, $t \geq 0$ all flows $\phi^{\hat{\pi}}_{\hat{x}}(t, (\overline{q}, x_o), \mathbf{d}, \mathbf{y}) \notin Bad$. In particular, this is true for $\mathbf{y}'$ such that $\hat{\tau}_0 = \hat{\tau}'_0$, $\hat{R}(\overline{q}, y'(\hat{\tau}'_0)) = \text{Reach}(\overline{q})$, and $y'(t) = \epsilon$ for all $t > \hat{\tau}'_0$ (note that a $y$ for which $\hat{R}(\overline{q}, y) = \text{Reach}(\overline{q})$ must always exist in $Y$ by the definition of an estimator). This implies that $\phi_{\hat{Q}}(t, \overline{q}, \mathbf{y}') = \phi_{\hat{Q}}(0, \overline{q}, \mathbf{y}') = \text{Reach}(\overline{q})$ for all $t$. In such a case, $\pi'(\hat{x}) := \hat{\pi}(\text{Reach}(\overline{q}), \hat{x})$ is a map from the continuous state only as the first argument is always constant. Hence, the flow $\hat{x}(t) = \phi^{\pi'}_{\hat{x}}(t, (\overline{q}, x_o), \mathbf{d}, \mathbf{y}')$ satisfies $\dot{\hat{x}}(t) \in f(\hat{x}(t), \text{Reach}(\overline{q}), \pi'(\hat{x}(t)), d(t))$ for all $t$. In turn, any $\hat{x}(t)$ that satisfies this also satisfies $\dot{\hat{x}}(t) = f(x(t), \phi_q(t, q_o, \boldsymbol{\sigma}), \pi'(x(t)), d(t))$ for all $q_o \in \overline{q}$ and all $\boldsymbol{\sigma}$. As a consequence, $\pi'$ is such that $\phi^{\pi'}_x(t, (q_o, x_o), \mathbf{d}, \boldsymbol{\sigma}) \notin Bad$ for all $t \geq 0$, all $\mathbf{d}$, all $\boldsymbol{\sigma}$, and all $q_o \in \overline{q}$. This, in turn, implies that $x_o \notin C_{\overline{q}}$. ■

We first solve Problem 2 and then address the question of when this problem is equivalent to Problem 1.

## V. Solution to Problem 2

Since $\hat{H}$ is a hybrid system with uncontrolled mode transitions, it has more structure than the general class of hybrid automata. We exploit this structure to provide a specialized iterative algorithm for the computation of the capture set and of the feedback maps $\hat{\pi}$. The proofs are in the Appendix.

### A. Computation of the capture set $\hat{C}$

In order to compute the set $\hat{C}$, we introduce the notion of uncontrollable predecessor operator.

**Definition 17.** For a set $S \subset X$ and $\overline{q} \in \hat{Q}$ the *uncontrollable predecessor operator* for $\hat{H}$ is defined as $\text{Pre}(\overline{q}, S) := \{x_o \in X \,|\, \forall \hat{\pi}\, \exists\, \mathbf{d}, t \geq 0, \text{s.t. some } \phi^{\hat{\pi}}_{\hat{x}}(t, (x_o, \overline{q}), \mathbf{d}, \epsilon) \in S\}$.

This set represents the set of all states that are mapped to $S$ when the mode estimate is constant and equal to $\overline{q}$. The following properties of the Pre operator follow from the fact that it is an order preserving map in both of its arguments.

**Proposition 5.** *The operator Pre : $\hat{Q} \times 2^X \to 2^X$ has the following properties for all $\hat{q} \in \hat{Q}$ and $S \in 2^X$: (i) $S \subseteq Pre(\hat{q}, S)$; (ii) $Pre(\hat{q}, Pre(\hat{q}, S)) = Pre(\hat{q}, S)$; (iii) $Pre(\hat{q}, S_1) \subseteq Pre(\hat{q}, S_2)$, for all $S_1 \subseteq S_2$; (iv) $Pre(\hat{q}_1, S) \subseteq Pre(\hat{q}_2, S)$, for all $\hat{q}_1 \subseteq \hat{q}_2$; (v) $Pre(\hat{q}_1, Pre(\hat{q}_2, S)) = Pre(\hat{q}_1, S)$, for all $\hat{q}_2 \subseteq \hat{q}_1$; (vi) $Pre(\hat{q}_0, S_0 \cup Pre(\hat{q}_1, S_1) \cup \ldots \cup Pre(\hat{q}_n, S_n)) = Pre(\hat{q}_0, S_0 \cup S_1 \cup \ldots \cup S_n)$ for $\hat{q}_i \subseteq \hat{q}_0$ for all $i$.*

We use for all $\hat{q} \in \hat{Q}$ the notation $\hat{R}(\hat{q}, Y) := \{\hat{q}' \in \hat{R}(\hat{q}, y) \mid y \in Y\}$, in which we set $\hat{R}(\hat{q}, y) := \emptyset$ if $\hat{R}(\hat{q}, y)$ is not defined for some $y \in Y$.

**Proposition 6.** *The sets $\hat{C}_{\hat{q}_i}$ for all $\hat{q}_i \in \hat{Q}$ satisfy $\hat{C}_{\hat{q}_i} = Pre\left(\hat{q}_i, \bigcup_{\{\hat{q}_j \in \hat{R}(\hat{q}_i, Y)\}} \hat{C}_{\hat{q}_j} \cup Bad\right)$.*

**Definition 18.** A set $\hat{W} \subseteq \hat{Q} \times X$ is said a *controlled invariant set* for $\hat{H}$ if there is a feedback map $\hat{\pi}$ such that for all $(\overline{q}_o, x_o) \in \hat{W}$, we have that all flows $\hat{\phi}^{\hat{\pi}}(t, (\overline{q}_o, x_o), \mathbf{d}, \mathbf{y}) \in \hat{W}$ for all $t$, $\mathbf{d}$, and $\mathbf{y}$. A set $\hat{W} \subseteq \hat{Q} \times X$ is *the maximal controlled invariant set* for $\hat{H}$ provided it is a controlled invariant set for $\hat{H}$ and any other controlled invariant set for $\hat{H}$ is a subset of $\hat{W}$.

**Proposition 7.** *The set $\hat{W} := (\hat{Q} \times X)/\hat{C}$ is the maximal controlled invariant set for $\hat{H}$ contained in $(\hat{Q} \times X)/(\hat{Q} \times Bad)$.*

Let $\hat{Q} = \{\hat{q}_1, ..., \hat{q}_M\}$ with $\hat{q}_i \in 2^Q$ for $i \in \{1, \ldots, M\}$, $S_i \in 2^X$ for $i \in \{1, \ldots, M\}$, and define $S := (S_1, \ldots, S_M) \subseteq (2^X)^M$. We define the map $G : (2^X)^M \to (2^X)^M$ as

$$G(S) := \begin{bmatrix} \mathrm{Pre}\left(\hat{q}_1, \bigcup_{\{j|\hat{q}_j \in \hat{R}(\hat{q}_1, Y)\}} S_j \cup Bad\right) \\ \vdots \\ \mathrm{Pre}\left(\hat{q}_M, \bigcup_{\{j|\hat{q}_j \in \hat{R}(\hat{q}_M, Y)\}} S_j \cup Bad\right) \end{bmatrix}.$$

**Proposition 8.** *Let $S := (S_1, ..., S_M)$ be a tuple of sets $S_i \subseteq X$ such that $S = G(S)$. Then, $(\hat{Q} \times X)/\bigcup_{i\in\{1,...,M\}}(\hat{q}_i \times S_i)$ is a controlled invariant set for $\hat{H}$.*

Let $Z := (2^X)^M$ represent the set of all M-tuples of subsets of $X$ and define the partial order $(Z, \subseteq)$, where $\subseteq$ is defined component-wise. One can verify that $G : Z \to Z$ is an order preserving map (it follows from property (iii) of the Pre operator from Proposition 5).

**Algorithm 1.** $S^0 := (S^0_1,\ S^0_2, \ldots, S^0_M) := (\emptyset, \ldots,\ \emptyset)$,
$S^1 = G(S^0)$
*while* $S^{k-1} \neq S^k$
 $S^{k+1} = G(S^k)$
*end.*

If Algorithm 1 terminates, that is, if there is a $K^*$ such that $S^{K^*} = (S^{K^*}_1, ..., S^{K^*}_M) = (S^{K^*+1}_1, ..., S^{K^*+1}_M) = S^{K^*+1}$, we denote the fixed point by $S^*$.

**Theorem 1.** *If Algorithm 1 terminates, the fixed point $S^*$ is such that $S^* = (\hat{C}_{\hat{q}_1}, ..., \hat{C}_{\hat{q}_M})$.*

*Proof:* If Algorithm 1 terminates, then there is $N^* > 0$ such that $G(\bot)^{N^*} = G(\bot)^{N^*+1} = S^*$, in which $\bot = \emptyset$. Thus, $S^*$ is a fixed point of $G$. To show that it is the least fixed point, consider any other fixed point of $G$, called $\beta$. Since $\bot \leq \beta$ and $G$ is an order preserving map, we have that $G(\bot) \leq G(\beta) = \beta$, $G^2(\bot) \leq G(\beta) = \beta$,...., $G^{N^*}(\bot) \leq \beta$. Since $G^{N^*}(\bot) = S^*$, we have that $S^* \leq \beta$. Thus $S^*$ is the least fixed point of $G$.

Proposition 6 indicates that the set $\hat{C} = \bigcup_{\hat{q}_i\in\hat{Q}}(\hat{q}_i \times \hat{C}_{\hat{q}_i})$ is such that the tuple of sets $(\hat{C}_{\hat{q}_1}, ..., \hat{C}_{\hat{q}_M})$ is a fixed point of $G$. Assume that such a tuple of sets is not the least fixed point of $G$. This implies that there are sets $S_i \subseteq \hat{C}_{\hat{q}_i}$ such that the tuple $(S_1, ..., S_M)$ is also a fixed point of $G$. Consider the sets $\hat{W} = (\hat{Q} \times X)/\bigcup_{\hat{q}_i\in\hat{Q}}(\hat{q}_i \times \hat{C}_{\hat{q}_i})$ and the new set $\hat{W}'$ defined as $\hat{W}' := (\hat{Q}\times X)/\bigcup_{i\in\{1,...,M\}}(\hat{q}_i \times S_i)$. By Proposition 8, these two sets are both controlled invariant and are both contained in $(\hat{Q}\times X)/(\hat{Q}\times Bad)$. Since $\hat{W} \subset \hat{W}'$, we have that $\hat{W}$ is not the maximal controlled invariant set contained in the complement of $\hat{Q} \times Bad$. This contradicts Proposition 7. Therefore, the tuple $(\hat{C}_{\hat{q}_1}, ..., \hat{C}_{\hat{q}_M})$ must be the least fixed point of $G$. Since the least fixed point of $G$ equals $S^*$ by the first part of the proof, it follows that $(\hat{C}_{\hat{q}_1}, ..., \hat{C}_{\hat{q}_M}) = S^*$. ∎

This result is based on the assumption that Algorithm 1 terminates and hence it is sufficient that the map $G$ is an order preserving map. A stronger property for $G$, such as omega-continuity [34], is required for the result of Theorem 1 to hold if termination of Algorithm 1 is not assumed. In Section VI, we address termination.

*B. The control map*

To determine the set of feedback maps that keep the complement of $\hat{C}$ invariant, we employ notions from viability theory.

**Definition 19.** A set valued map $F : X \to 2^X$ is said *piecewise Lipschitz continuous* on $X$ if it is Lipschitz continuous on a finite number of sets $X_i \subset X$ for $i = 1, ..., N$ that cover $X$, that is, $\bigcup_{i=1}^N X_i = X$, and $X_i \cap X_j = \emptyset$ for $i \neq j$.

The next result extends conditions for set invariance as found in [4] to the case of piece-wise Lipschitz continuous set valued maps. This extension is required in our case because the vector field $f$ is allowed to be piece-wise continuous.

**Proposition 9.** *Let $F : X \to 2^X$ be a set-valued Marchaud map. Assume that $F$ is piecewise Lipschitz continuous on $X$. A closed set $S \subseteq X$ is invariant under $F$ if and only if $F(x) \subseteq T_S(x)$ for all $x \in S$.*

For simplifying notation, for each mode $\hat{q} \in \hat{Q}$ define the set valued map $\bar{f} : X\times\hat{Q}\times U \to 2^X$ as $\bar{f}(\hat{x}, \hat{q}, u) = \{\hat{f}(\hat{x}, \hat{q}, u, d), d \in D\}$ for all $(\hat{x}, \hat{q}, u) \in X\times\hat{Q}\times U$. Define $L_{\hat{q}} := X\backslash\hat{C}_{\hat{q}}$ for all $\hat{q} \in \hat{Q}$ and consider the set valued map defined as

$$\Pi(\hat{q}, \hat{x}) := \{u \in U \mid \bar{f}(\hat{x}, \hat{q}, u) \subset T_{L_{\hat{q}}}(\hat{x})\}. \tag{3}$$

**Theorem 2.** *Assume that $\hat{\pi} : \hat{Q}\times X \to U$ is such that for all $\hat{q} \in \hat{Q}$ the set-valued map $F(\hat{x}, \hat{q}) := \bar{f}(\hat{x}, \hat{q}, \hat{\pi}(\hat{x}, \hat{q}))$ is Marchaud and piecewise Lipschitz continuous on $X$. Then, the set $(\hat{Q} \times X)\backslash\hat{C}$ is invariant for $\hat{H}^{\hat{\pi}}$ if and only if $\hat{\pi}(\hat{q}, \hat{x}) \in \Pi(\hat{q}, \hat{x})$.*

*Proof:* ($\Leftarrow$) Assume that $\hat{\pi}(\hat{q}, \hat{x}) \in \Pi(\hat{q}, \hat{x})$ and that $(\hat{q}(\hat{\tau}_0), \hat{x}(\hat{\tau}_0)) \notin \hat{C}$, we show that all $(\hat{q}(t), \hat{x}(t)) \notin \hat{C}$ for all $t \geq \hat{\tau}_0$. This is shown by induction argument on the transition times $\hat{\tau}'_i$. (Base case) By assumption we have that $(\hat{q}(\hat{\tau}_0), \hat{x}(\hat{\tau}_0)) \notin \hat{C}$. (Induction step) Assume that $(\hat{q}(\hat{\tau}_i), \hat{x}(\hat{\tau}_i)) \notin \hat{C}$. We show that this implies $(\hat{q}(t), \hat{x}(t)) \notin \hat{C}$ for all $t \in [\hat{\tau}_i, \hat{\tau}_{i+1}]$, in which $\hat{\tau}_{i+1} = \hat{\tau}'_i$. This in turn is equivalent to showing that $\hat{x}(t) \notin \hat{C}_{\hat{q}(\hat{\tau}_i)}$ for all $t \in [\hat{\tau}_i, \hat{\tau}'_i]$ and $\hat{x}(\hat{\tau}_{i+1}) \notin \hat{C}_{\hat{q}(\hat{\tau}_{i+1})}$. Since $\hat{C}_{\hat{q}(\hat{\tau}_{i+1})} \subseteq \hat{C}_{\hat{q}(\hat{\tau}_i)}$ by the properties of the Pre operator and by Proposition 6, then if $\hat{x}(\hat{\tau}'_i) \notin \hat{C}_{\hat{q}_{\hat{\tau}_{i+1}}}$ also $\hat{x}(\hat{\tau}'_i) \notin \hat{C}_{\hat{q}(\hat{\tau}_{i+1})}$. Therefore, it is enough to show that $\hat{x}(t) \notin \hat{C}_{\hat{q}(\hat{\tau}_i)}$ for all $t \in [\hat{\tau}_i, \hat{\tau}'_i]$. If $\hat{\tau}'_i = \hat{\tau}_i$, then since $\hat{x}(\hat{\tau}'_i) = \hat{x}(\hat{\tau}_i)$ we have that $\hat{x}(\hat{\tau}_i) \notin \hat{C}_{\hat{q}(\hat{\tau}_i)}$. If $\hat{\tau}_i < \hat{\tau}'_i$, for $t \in [\hat{\tau}_i, \hat{\tau}'_i)$, the trajectory $\hat{x}(t)$ satisfies $\dot{\hat{x}}(t) \in \bar{f}(\hat{x}(t), \hat{q}(\hat{\tau}_i), \hat{\pi}(\hat{q}(\hat{\tau}_i)) = F(x, \hat{q}(\hat{\tau}_i))$. Since $\hat{\pi}(\hat{q}, \hat{x}) \in \Pi(\hat{q}, \hat{x})$, it follows that $F(\hat{x}, \hat{q}(\hat{\tau}_i)) \subseteq T_{L_{\hat{q}(\hat{\tau}_i)}}(\hat{x})$. Proposition 9 thus implies that $L_{\hat{q}(\hat{\tau}_i)}$ is invariant by $F$. Therefore, we have that $\hat{x}(t) \in L_{\hat{q}(\hat{\tau}_i)}$ for all $t \in [\hat{\tau}_i, \hat{\tau}'_i]$. Thus, $\hat{x}(t) \notin \hat{C}_{\hat{q}(\hat{\tau}_i)}$ for all $t \in [\hat{\tau}_i, \hat{\tau}'_i]$.

($\Rightarrow$) The fact that if $\hat{\pi}(\hat{q}, \hat{x}) \notin \Pi(\hat{q}, \hat{x})$ the set $(\hat{Q} \times X)/\hat{C}$ is not invariant for $\hat{H}^{\pi}$ follows from Proposition 9. ∎

Given the current mode estimate $\hat{q}$, a control map as given in Theorem 2 is one that makes all the possible vector fields point outside the current mode-dependent capture set $\hat{C}_{\hat{q}}$. Once the mode estimate switches to $\hat{q}'$, the current mode-dependent capture set also switches to the new mode-dependent capture set $\hat{C}_{\hat{q}'}$, which is (by Algorithm 1) contained in the previous one $\hat{C}_{\hat{q}}$. At this point, the feedback map switches to one that makes all the possible vector fields originating from $\hat{q}'$ point outside the new current mode-dependent capture set $\hat{C}_{\hat{q}'}$. Note that control map (3) guarantees safety for any choice of an estimator. However, a coarser estimator leads to larger mode dependent capture sets to be avoided at any time and, as a consequence, the control actions are more conservative.

## VI. Termination of Algorithm 1

There are two main difficulties in the implementation of Algorithm 1. The first one is the exact computation of the Pre operator, which is known to be a hard problem for general classes of nonlinear and hybrid dynamics and general results are still lacking. Hence, research has been focusing on special classes of systems for which such an operator can be exactly computed [46–48]. The second difficulty lies in guaranteeing the termination of Algorithm 1. In this section, we address the termination of Algorithm 1, that is, the existence of a *finite* $N$ such that $S^N = S^{N+1}$. We then discuss the problem of the exact computation of the Pre operator.

For the termination problem, we first provide sufficient conditions on $\hat{H}$ for which Algorithm 1 terminates. Then, we show that one can construct an abstraction of $\hat{H}$ for which Algorithm 1 always terminates and such that the fixed point gives the mode-dependent capture sets of $\hat{H}$. In order to proceed, we introduce the notion of kernel sets for $\hat{H}$.

**Definition 20.** (Kernel set) The *kernel set* corresponding to a mode $\hat{q}^* \in \hat{Q}$ is defined as $ker(\hat{q}^*) := \{\hat{q} \in \hat{Q} \mid \hat{q} \in \widehat{\text{Reach}}(\hat{q}^*)$ and $\hat{q}^* \in \widehat{\text{Reach}}(\hat{q})\}$.

The kernel set for a mode $\hat{q}^*$ is thus the set of all modes that can be reached from $\hat{q}^*$ and from which $\hat{q}^*$ can be reached. One can verify that for all pairs of modes $\hat{q}_i, \hat{q}_j \in \hat{Q}$, we have that $\hat{q}_i \in \widehat{\text{Reach}}(\hat{q}_j)$ and $\hat{q}_j \in \widehat{\text{Reach}}(\hat{q}_i)$ if and only if $ker(\hat{q}_i) = ker(\hat{q}_j)$. The next result shows that any two modes of $\hat{H}$ in the same kernel set have the same mode-dependent capture set and hence the same set of safe feedback maps.

**Proposition 10.** *For every kernel set $ker \subseteq \hat{Q}$ and for any two modes $\hat{q}, \hat{q}' \in ker$, we have that $\hat{C}_{\hat{q}} = \hat{C}_{\hat{q}'}$ and hence that $\Pi(\hat{q}, x) = \Pi(\hat{q}', x)$.*

*Proof:* Since $\hat{q}, \hat{q}' \in ker$, we have that $\hat{q}' \in \widehat{\text{Reach}}(\hat{q})$ and that $\hat{q} \in \widehat{\text{Reach}}(\hat{q}')$. By Proposition 6, the first inclusion implies that $\hat{C}_{\hat{q}'} \subseteq \hat{C}_{\hat{q}}$, while the second inclusion implies that $\hat{C}_{\hat{q}} \subseteq \hat{C}_{\hat{q}'}$. Hence, we must have that $\hat{C}_{\hat{q}} = \hat{C}_{\hat{q}'}$. By equation (3), this in turn implies also that $\Pi(\hat{q}, x) = \Pi(\hat{q}', x)$. ■

Let $\mathcal{K} := \{ker(\hat{q}_1), \ldots, ker(\hat{q}_M)\}$. Let there be $p$ distinct elements in $\mathcal{K}$ denoted $ker_1, \ldots, ker_p$. Note that $ker_i \cap ker_j = \emptyset$, for $i \neq j$. If each of the kernel sets is just one element in $\hat{Q}$, it means that there are no discrete transitions possible in $\hat{R}$ that bring a discrete state $\hat{q}$ back to itself. That is, there is no loop in any of the trajectories of $\hat{q}$. In this case, one can verify that Algorithm 1 terminates in a finite number of steps. If instead there are kernel sets composed of more than one element, it means that there are discrete transitions that bring a discrete state back to itself, that is, there are loops in the trajectories of $\hat{q}$. In this situation, Algorithm 1 may not terminate. The next result shows that even when there are loops in the trajectories of $\hat{q}$, Algorithm 1 still terminates if each kernel set contains a maximal element.

**Theorem 3.** *Algorithm 1 terminates if all the kernel sets $ker_1, \ldots, ker_p$ have a maximal element with respect to the partial order $(\hat{Q}, \subseteq)$.*

This theorem provides an easily checkable sufficient condition for the termination of Algorithm 1 based on the structure of the map $\hat{R}$. Note that a corollary of this theorem is that if system $\hat{H}$ is such that all of its kernel sets are singletons in $\hat{Q}$, then Algorithm 1 terminates for $\hat{H}$. The proof of this theorem is in the Appendix. Here, we illustrate the logic of the proof and the concept of kernel set on a simple example.

*Example* 2. Consider a simple instance of $(\hat{R}, \hat{Q}, Y)$ in which $\hat{Q} = \{\hat{q}_1, \hat{q}_2\}$, $Y = \{\epsilon, y^*\}$, $\hat{R}(\hat{q}_1, y^*) = \hat{q}_2$, and $\hat{R}(\hat{q}_2, y^*) = \hat{q}_1$. That is, we have one kernel set equal to $\{\hat{q}_1, \hat{q}_2\}$. Because of the loop between $\hat{q}_1$ and $\hat{q}_2$, Algorithm 1 may not terminate. Here, we show that if we assume that, for example, $\hat{q}_2 \subseteq \hat{q}_1$, then Algorithm 1 terminates in three steps. In this example, we have that $S = (S_1, S_2)$ and $G(S) = (\text{Pre}(\hat{q}_1, S_2 \cup Bad), \text{Pre}(\hat{q}_2, S_1 \cup Bad))$. Hence, $S^1 = G(\emptyset) = (\text{Pre}(\hat{q}_1, Bad), \text{Pre}(\hat{q}_2, Bad))$, and $S^2 = G(S^1) = (\text{Pre}(\hat{q}_1, \text{Pre}(\hat{q}_2, Bad)), \text{Pre}(\hat{q}_2, \text{Pre}(\hat{q}_1, Bad)))$. Consider $S^2$. On the one hand, we have that $\text{Pre}(\hat{q}_1, \text{Pre}(\hat{q}_2, Bad)) \subseteq \text{Pre}(\hat{q}_1, Bad)$ by properties (iv) and (ii) of Proposition 5. On the other hand, we have that $\text{Pre}(\hat{q}_1, \text{Pre}(\hat{q}_2, Bad)) \supseteq \text{Pre}(\hat{q}_1, Bad)$ by property (iii) of Proposition 5. Hence, we must have that $S_1^2 = \text{Pre}(\hat{q}_1, Bad)$. Similar reasonings lead to $S_2^2 = \text{Pre}(\hat{q}_1, Bad)$. This leads to $S^3 = G(S^2) = (\text{Pre}(\hat{q}_1, \text{Pre}(\hat{q}_1, Bad)), \text{Pre}(\hat{q}_2, \text{Pre}(\hat{q}_1, Bad)))$, which, employing again the properties of the Pre operator, leads to $S^3 = (\text{Pre}(\hat{q}_1, Bad), \text{Pre}(\hat{q}_1, Bad))$. This set is, in turn, equal to $S^2$ and therefore Algorithm 1 terminates in three steps.

### A. Proving termination through abstraction

When not all kernel sets have a maximal element, Theorem 3 does not hold. However, for any estimator $\hat{H}$, one can construct an abstraction of $\hat{H}$, denoted $\hat{H}^a$, for which Algorithm 1 terminates and such that the fixed point gives the mode-dependent capture sets of $\hat{H}$. This abstraction is constructed by merging all the modes of $\hat{H}$ that belong to the same kernel set in a unique new mode as follows.

**Definition 21.** Given hybrid system $\hat{H} = (\hat{Q}, X, U, D, Y, \hat{R}, \hat{f})$, the abstraction $\hat{H}^a = (\hat{Q}^a, X, U, D, Y^a, \hat{R}^a, \hat{f}^a)$ is a hybrid system with uncontrolled mode transitions such that

(i) $\hat{Q}^a = \{\hat{q}_1^a, ..., \hat{q}_p^a\}$, $Y^a$ such that $\epsilon \in Y^a$ and $\hat{R}(\hat{q}^a, \epsilon) = \hat{q}^a$ for all $\hat{q}^a \in \hat{Q}^a$;

(ii) for all $i, j \in \{1, ..., p\}$ there is $y^a \in Y^a$ such that $\hat{q}_i^a = \hat{R}^a(\hat{q}_j^a, y^a)$ if and only if there are $\hat{q}' \in ker_i$, $\hat{q} \in ker_j$, and $y \in Y$ such that $\hat{q}' = \hat{R}(\hat{q}, y)$;

(iii) for all $i \in \{1, ..., p\}$, $x \in X$, $d \in D$, and $v \in U$, we have that $\hat{f}^a(x, \hat{q}_i^a, v, d) := \bigcup_{\hat{q} \in ker_i} \hat{f}(x, \hat{q}, v, d)$.

For a feedback map $\hat{\pi}^a : \hat{Q}^a \times X \to U$, initial states $x_o \in X$ and $\hat{q}_o^a \in \hat{Q}^a$, and signals $\mathbf{y^a}$, $\mathbf{d}$, we denote the flows of the closed loop system $\hat{H}^{a,\hat{\pi}^a}$ by $\phi_{\hat{Q}^a}(t, \hat{q}_o^a, \mathbf{y^a})$ and $\phi_{\hat{x}^a}^{\hat{\pi}^a}(t, (\hat{q}_o^a, x_o), \mathbf{d}, \mathbf{y^a})$, in which $\hat{x}^a(t) := \phi_{\hat{x}^a}^{\hat{\pi}^a}(t, (\hat{q}_o^a, x_o), \mathbf{d}, \mathbf{y^a})$ satisfies $\dot{\hat{x}}^a(t) \in \hat{f}^a(\hat{x}^a(t), \phi_{\hat{Q}^a}(t, \hat{q}_o^a, \mathbf{y^a}), \hat{\pi}^a(\phi_{\hat{Q}^a}(t, \hat{q}_o^a, \mathbf{y^a}), \hat{x}^a), d(t))$. We also denote by $\hat{C}^a_{\hat{q}_i^a}$ for $i \in \{1, ..., p\}$ the mode-dependent capture sets of $\hat{H}^a$. For any $\hat{q}^a \in \hat{Q}^a$, we define $ker(\hat{q}^a) := ker_i$ provided $\hat{q}^a = \hat{q}^a_i$. Also, for all $\hat{q}^a \in \hat{Q}^a$, we denote the set of reachable modes from $\hat{q}^a$ as $\widehat{\text{Reach}}^a(\hat{q}^a) := \bigcup_{t\geq 0} \bigcup_{\mathbf{y^a}} \phi_{\hat{Q}^a}(t, \hat{q}^a, \mathbf{y^a})$. In the sequel, we denote $\hat{R}^a(\hat{q}^a, Y^a) := \bigcup_{y^a \in Y^a} \hat{R}^a(\hat{q}^a, y^a)$, in which we set $\hat{R}^a(\hat{q}^a, y^a) := \hat{q}^a$ if $\hat{R}^a(\hat{q}^a, y^a)$ is not defined for some $y^a \in Y^a$. The following proposition is a direct consequence of Theorem 3 and of the fact that all kernel sets of $\hat{H}^a$ are singletons.

**Proposition 11.** *Algorithm 1 terminates for system $\hat{H}^a$.*

The next result shows that any piece-wise continuous signal, which is continuous from the right and contained in $ker(\phi_{\hat{Q}^a}(t, \hat{q}^a_o, \mathbf{y^a}))$ is a possible discrete flow of $\hat{H}$ for suitable $\mathbf{y}$ starting from some $\hat{q}_o \in ker(\hat{q}^a_o)$.

**Proposition 12.** *For any piece-wise continuous signal $\boldsymbol{\alpha}$ that is continuous from the right and such that $\alpha(t) \in ker(\phi_{\hat{Q}^a}(t, \hat{q}^a_o, \mathbf{y^a}))$, there are $\hat{q}_o \in ker(\hat{q}^a_o)$ and $\mathbf{y}$ such that $\alpha(t) = \phi_{\hat{Q}}(t, \hat{q}_o, \mathbf{y})$ for all $t$.*

*Proof:* Since $\alpha(t) \in ker(\phi_{\hat{Q}^a}(t, \hat{q}^a_o, \mathbf{y^a}))$ for all $t$, there are times $t_0, ..., t_N \leq t$ and a sequence $j_0, ..., j_N \in \{1, ..., p\}$ such that $\alpha(t) \in ker_{j_i}$ for all $t \in [t_i, t_{i+1})$. Since any mode in $ker_{j_i}$ can transit to any other mode in $ker_{j_i}$ instantaneously under the discrete transitions of $\hat{H}$, we have that there are $\hat{q}_{o,i} \in ker_{j_i}$ and $\mathbf{y}_i$ such that $\alpha(t) = \phi_{\hat{Q}}(t - t_i, \hat{q}_{o,i}, \mathbf{y}_i)$ for all $t \in [t_i, t_{i+1})$. Also, for any two modes $\alpha_i \in ker_{j_i}$ and $\alpha_{i+1} \in ker_{j_{i+1}}$ we have that $\alpha_{i+1} \in \widehat{\text{Reach}}(\alpha_i)$. Hence, let $\alpha_i^- := \lim_{t \to t_{i+1}^-} \phi_{\hat{Q}}(t - t_i, \hat{q}_{o,i}, \mathbf{y}_i)$ and $\alpha_i^+ := \lim_{t \to t_{i+1}^+} \phi_{\hat{Q}}(t - t_{i+1}, \hat{q}_{o,i+1}, \mathbf{y}_{i+1})$. Then, since multiple transitions are possible in $\hat{H}$ at the same time, there is a signal $\mathbf{y}_{i,i+1}$ such that $\alpha_i^+ = \phi_{\hat{Q}}(0, \alpha_i^-, \mathbf{y}_{i,i+1})$. Hence, there is a signal $\mathbf{y}$ such that $\alpha(t) = \phi_{\hat{Q}}(t, \hat{q}_{o,0}, \mathbf{y})$ for all $t$. ■

**Theorem 4.** *For all kernel sets $ker_i$ with $i \in \{1, ..., p\}$ and for all $\hat{q} \in ker_i$, we have that $\hat{C}_{\hat{q}} = \hat{C}^a_{\hat{q}^a_i}$.*

*Proof:* Let $\hat{q} \in ker_i$. We first show that $\hat{C}_{\hat{q}} \subseteq \hat{C}^a_{\hat{q}^a_i}$. Let $x_o \in \hat{C}_{\hat{q}}$, then for all $\hat{\pi} : \hat{Q} \times X \to U$, there are $\mathbf{y}$, $\mathbf{d}$, and $t > 0$ such that $\phi^{\hat{\pi}}_{\hat{X}}(t, (\hat{q}, x), \mathbf{d}, \mathbf{y}) \in Bad$. This is in particular true for all those feedback maps $\hat{\pi}$ such that $\hat{\pi}(\hat{q}, x) = \hat{\pi}(\hat{q}', x)$ whenever $\hat{q}, \hat{q}' \in ker_j$ for some $j \in \{1, ..., p\}$. Hence, we also have that for all $\hat{\pi}^a : \hat{Q}^a \times X \to U$, there are $\mathbf{y}$, $\mathbf{d}$, and $t > 0$ such that $\hat{x}(t) := \phi^{\hat{\pi}^a}_{\hat{X}}(t, (\hat{q}, x), \mathbf{d}, \mathbf{y}) \in Bad$, in which $\dot{\hat{x}} \in \hat{f}(\hat{x}(t), \phi_{\hat{Q}}(t, \hat{q}, \mathbf{y}), \hat{\pi}^a(\alpha(t), x(t)), d(t))$ with $\alpha(t) := \hat{q}^a_j$ if $\phi_{\hat{Q}}(t, \hat{q}, \mathbf{y}) \in ker_j$. Such a signal $\hat{x}(t)$ also satisfies $\dot{\hat{x}} \in \hat{f}^a(\hat{x}(t), \alpha(t), \hat{\pi}^a(\alpha(t), x(t)), d(t))$ by the definition of $\hat{f}^a$. By the definition of $\hat{R}^a$, there is $\mathbf{y^a}$ such that $\alpha(t) = \phi_{\hat{Q}^a}(t, \hat{q}^a_i, \mathbf{y^a})$ for all $t$. Hence, $\hat{x}(t)$ is also a continuous flow of $\hat{H}^a$ starting at $(\hat{q}^a_i, x_o)$ and therefore $x_o \in \hat{C}^a_{\hat{q}^a_i}$.

We now show that $\hat{C}^a_{\hat{q}^a_i} \subseteq \hat{C}_{\hat{q}}$. If $x_o \in \hat{C}^a_{\hat{q}^a_i}$, then for all feedback maps $\hat{\pi}^a : \hat{Q}^a \times X \to U$, there are $\mathbf{y^a}$, $\mathbf{d}$, and $t > 0$ such that $\hat{x}^a(t) := \phi^{\hat{\pi}^a}_{\hat{X}^a}(t, (\hat{q}^a_i, x_o), \mathbf{y^a}, \mathbf{d}) \in Bad$. Here, we have that $\hat{x}^a(t)$ satisfies $\dot{\hat{x}}^a(t) \in \hat{f}^a(\hat{x}^a(t), \phi_{\hat{Q}^a}(t, \hat{q}^a_i, \mathbf{y^a}), \hat{\pi}^a(\phi_{\hat{Q}^a}(t, \hat{q}^a_i, \mathbf{y^a}), \hat{x}^a), d(t))$, which is equivalent (by the definition of $\hat{f}^a$) to $\dot{\hat{x}}^a(t) \in \hat{f}(\hat{x}^a(t), ker(\phi_{\hat{Q}^a}(t, \hat{q}^a_i, \mathbf{y^a})), \hat{\pi}^a(\phi_{\hat{Q}^a}(t, \hat{q}^a_i, \mathbf{y^a}), \hat{x}^a), d(t))$, which is equivalent to $\dot{\hat{x}}^a(t) = \hat{f}(\hat{x}^a(t), \alpha(t), \hat{\pi}^a(\phi_{\hat{Q}^a}(t, \hat{q}^a_i, \mathbf{y^a}), \hat{x}^a), d(t))$ for piece-wise continuous signal $\boldsymbol{\alpha}$ (continuous from the right) such that $\alpha(t) \in ker(\phi_{\hat{Q}^a}(t, \hat{q}^a_i, \mathbf{y^a}))$. By Proposition 12, any such $\alpha(t)$ is such that there are $\mathbf{y}$ and $\hat{q}_o \in ker(\hat{q}^a_i)$ such that $\alpha(t) = \phi_{\hat{Q}}(t, \hat{q}_o, \mathbf{y})$ for all $t$, that is, it is a discrete flow of system $\hat{H}$. Hence, for all $\pi' : \hat{Q} \times X \to U$ with $\hat{\pi}'(\hat{q}, x) = \hat{\pi}'(\hat{q}', x)$ for all $\hat{q}, \hat{q}' \in ker_j$ for all $j$, there are $\mathbf{y}$, $\mathbf{d}$, $\hat{q}_o \in ker_i$, such that $\phi^{\hat{\pi}'}_{\hat{X}}(t, (\hat{q}_o, x_o), \mathbf{y}, \mathbf{d}) \in Bad$. By Proposition 10, this implies that for all $\pi : \hat{Q} \times X \to U$ there are $\mathbf{y}$, $\mathbf{d}$, $\hat{q}_o \in ker_i$, such that $\phi^{\hat{\pi}}_{\hat{X}}(t, (\hat{q}_o, x_o), \mathbf{y}, \mathbf{d}) \in Bad$. Hence, $x_o \in \hat{C}_{\hat{q}_o}$. ■

The above theorem provides a useful result for the computation of the mode-dependent capture sets of $\hat{H}$. In particular, one constructs the abstraction $\hat{H}^a$ and applies Algorithm 1 to it. Algorithm 1 is in turn always guaranteed to terminate for system $\hat{H}^a$. The result (by Theorem 4) provides the sets $\hat{C}_{\hat{q}}$. Hence, $\hat{H}^a$ can be considered only as a structural abstraction as it does not provide an over-approximation of the capture set of $\hat{H}$, but provides it exactly.

The next two technical propositions provide a characterization of the Pre operator computed for system $\hat{H}^a$ and the relationship between $\hat{R}^a$ and $R$. Specifically, denote the predecessor operator for system $\hat{H}^a$ by $\text{Pre}^a(\hat{q}^a, S)$ for some $S \subseteq X$ as $\text{Pre}^a(\hat{q}^a, S) := \{x_o \in X \mid \forall\ \hat{\pi}^a\ \exists\ t, \mathbf{d},\ \text{s.t.}\ \phi^{\hat{\pi}^a}_{\hat{X}^a}(t, (\hat{q}^a, x_o), \mathbf{d}, \epsilon) \in S\}$.

**Proposition 13.** *For all $\hat{q}^a \in \hat{Q}^a$ and $S \subseteq X$, we have that $Pre^a(\hat{q}^a, S) = Pre(\bigvee ker(\hat{q}^a), S)$.*

*Proof:* From the definition of $\text{Pre}^a(\hat{q}^a, S)$, we have that $x_o \in \text{Pre}^a(\hat{q}^a, S)$ if and only if for all $\hat{\pi}^a$, there are $t, \mathbf{d}$ such that $\hat{x}^a(t) = \phi^{\hat{\pi}^a}_{\hat{X}^a}(t, (\hat{q}^a, x_o), \mathbf{d}, \epsilon) \in S$, in which $\dot{\hat{x}}^a(t) \in \hat{f}^a(\hat{x}^a(t), \hat{q}^a, \hat{\pi}^a(\hat{x}^a(t)), d(t))$, which, by the definition of $\hat{f}^a$ and of $\hat{f}$ is equivalent to $\dot{\hat{x}}^a(t) \in f(\hat{x}^a(t), \bigcup_{\hat{q} \in ker(\hat{q}^a)} \bigcup_{q \in \hat{q}} q, \hat{\pi}^a(\hat{x}^a(t)), d(t)) = f(\hat{x}^a(t), \bigvee ker(\hat{q}^a), \hat{\pi}^a(\hat{x}^a(t)), d(t))$. Hence, by the definition of Pre, we have that $x_o \in \text{Pre}^a(\hat{q}^a, S)$ if and only if $x_o \in \text{Pre}(\bigvee ker(\hat{q}^a), S)$. ■

**Proposition 14.** *Let $\hat{q}^a_{j_1}, \hat{q}^a_{j_0} \in \hat{Q}^a$. If $\hat{q}^a_{j_1} \in \hat{R}^a(\hat{q}^a_{j_0}, Y^a)$ then $\bigvee ker(\hat{q}^a_{j_1}) \subseteq Reach(\bigvee ker(\hat{q}^a_{j_0}))$.*

*Proof:* If $\hat{q}^a_{j_1} \in \hat{R}^a(\hat{q}^a_{j_0}, Y^a)$, then by the definition of $\hat{R}^a$ there are $\hat{q} \in ker(\hat{q}^a_{j_0})$ and $\hat{q}' \in ker(\hat{q}^a_{j_1})$ such that $\hat{q}' = \hat{R}(\hat{q}, y)$ for some $y \in Y$. By the definition of a kernel set, this also implies that for all $\hat{q} \in ker(\hat{q}^a_{j_0})$ and $\hat{q}' \in ker(\hat{q}^a_{j_1})$, there is a sequence of events $y_1, ..., y_k$ and of modes $\hat{q}_{j_0}, ..., \hat{q}_{j_k} \in \hat{Q}$ such that $\hat{q}_{j_0} = \hat{q}$, $\hat{q}_{j_k} = \hat{q}'$ and $\hat{q}_{j_{i+1}} = \hat{R}(\hat{q}_{j_i}, y_{i+1})$ for $i \in \{0, ..., k-1\}$. Since $\hat{R}(\hat{q}, y) \subseteq \text{Reach}(\hat{q})$ for all $y \in Y$ and $\hat{q} \in \hat{Q}$, this in turn implies that $\hat{q}_{j_{i+1}} \subseteq \text{Reach}(\hat{q}_{j_i})$ for $i \in \{0, ..., k-1\}$. This leads to $\hat{q}' \subseteq \text{Reach}(\hat{q})$ for all $\hat{q} \in ker(\hat{q}^a_{j_0})$ and $\hat{q}' \in ker(\hat{q}^a_{j_1})$. This also implies that $\hat{q}' \subseteq \text{Reach}(\bigvee ker(\hat{q}^a_{j_0}))$ and hence (since this holds for all $\hat{q}' \in ker(\hat{q}^a_{j_1})$) to $\bigvee ker(\hat{q}^a_{j_1}) \subseteq \text{Reach}(\bigvee ker(\hat{q}^a_{j_0}))$. ■

**Lemma 1.** *For all $\overline{q} \in \hat{Q}$, we have that $\hat{C}_{\overline{q}} = Pre(Reach(\overline{q}), Bad)$.*

*Proof:* First, we show that $\hat{C}_{\overline{q}} \subseteq \text{Pre}(\text{Reach}(\overline{q}), Bad)$. Since Algorithm 1 terminates in a finite number $n$ of steps for $\hat{H}^a$, we have that $\hat{C}^a_{\hat{q}^a} = \text{Pre}^a\,(\hat{q}^a, \bigcup_{\hat{q}^a_{j_1} \in \hat{R}^a(\hat{q}^a, Y^a)} \text{Pre}^a\left(\hat{q}^a_{j_1}, \bigcup_{\hat{q}^a_{j_2} \in \hat{R}^a(\hat{q}^a_{j_1}, Y^a)} \text{Pre}^a\left(\hat{q}^a_{j_2}, ... \bigcup_{\hat{q}^a_{j_{n-1}} \in \hat{R}^a(\hat{q}^a_{j_{n-2}}, Y^a)} \text{Pre}^a(\hat{q}^a_{j_{n-1}}, Bad)...\right)\right)\right)$. By Proposition 13, we also have that

$$\hat{C}^a_{\hat{q}^a} = \text{Pre}\Big(\bigvee ker(\hat{q}^a), \bigcup_{\hat{q}^a_{j_1} \in \hat{R}^a(\hat{q}^a, Y^a)} \text{Pre}\Big(\bigvee ker(\hat{q}^a_{j_1}), \bigcup_{\hat{q}^a_{j_2} \in \hat{R}^a(\hat{q}^a_{j_1}, Y^a)} \text{Pre}\Big(\bigvee ker(\hat{q}^a_{j_2}), \ldots \bigcup_{\hat{q}^a_{j_{n-1}} \in \hat{R}^a(\hat{q}^a_{j_{n-2}}, Y^a)} \text{Pre}(\bigvee ker(\hat{q}^a_{j_{n-1}}), Bad)\ldots\Big)\Big)\Big).$$

By Proposition 14, we have that $\bigvee ker(\hat{q}^a_{j_1}) \subseteq \text{Reach}(\bigvee ker(\hat{q}^a))$ and that $\bigvee ker(\hat{q}^a_{j_{i+1}}) \subseteq \text{Reach}(\bigvee ker(\hat{q}^a_{j_i}))$ for $i < n$. Since the Pre operator and Reach preserve the inclusion relation in the first argument, these imply that $\hat{C}^a_{\hat{q}^a} \subseteq \text{Pre}(\text{Reach}(\bigvee ker(\hat{q}^a)), Bad)$. Since for all $\overline{q}_1, \overline{q}_2 \in ker(\hat{q}^a)$ we have that $\text{Reach}(\overline{q}_1) = \text{Reach}(\overline{q}_2)$, we also have that $\text{Reach}(\overline{q}) = \text{Reach}(\bigvee ker(\hat{q}^a))$ for all $\overline{q} \in ker(\hat{q}^a)$. Hence, $\hat{C}^a_{\hat{q}^a} \subseteq \text{Pre}(\text{Reach}(\overline{q}), Bad)$ for all $\overline{q} \in ker(\hat{q}^a)$. This along with Theorem 4 finally imply that for all $\overline{q} \in ker(\hat{q}^a)$ we have $\hat{C}_{\overline{q}} \subseteq \text{Pre}(\text{Reach}(\overline{q}), Bad)$.

To show that $\hat{C}_{\overline{q}} \supseteq \text{Pre}(\text{Reach}(\overline{q}), Bad)$, we employ the properties of the Pre operator and Proposition 6. By such a proposition, by the fact that (since $\hat{H}$ is an estimator for $H$) for all $\overline{q} \in \hat{Q}$ there is $y \in Y$ such that $\hat{R}(\overline{q}, y) = \text{Reach}(\overline{q})$, and by property (iii) of Proposition 5, it follows that $\hat{C}_{\overline{q}} \supseteq \text{Pre}(\overline{q}, \hat{C}_{\text{Reach}(\overline{q})})$. In turn we have that $\hat{C}_{\text{Reach}(\overline{q})} \supseteq \text{Pre}(\text{Reach}(\overline{q}), Bad)$ by Proposition 6 and property (iii) of Proposition 5. Hence, we have that $\hat{C}_{\overline{q}} \supseteq \text{Pre}(\overline{q}, \text{Pre}(\text{Reach}(\overline{q}), Bad))$, which by property (i) of Proposition 6 leads to $\hat{C}_{\overline{q}} \supseteq \text{Pre}(\text{Reach}(\overline{q}), Bad)$. ■

This result shows that the mode-dependent capture set $\hat{C}_{\overline{q}}$ can be computed by computing the Pre operator only once as opposed to being determined through a (finite, by Theorem 4 and Proposition 11) iteration of Pre operator computations. Exact computation of Pre for general dynamics is not always possible. However, there are a number of works that have focused on the exact computation of uncontrollable predecessor operators for restricted classes of systems. For example, the work of [46] shows that Pre can be exactly computed for special classes of linear systems; [47] further extends this result to linear hybrid systems; [48] shows that Pre is exactly computable also for triangular hybrid systems. Finally, [17, 28] show that Pre is computable with a linear complexity algorithm for classes of order preserving systems. Based on these results and on Lemma 1, we conclude that Problem 2 is *decidable* when for each mode $\overline{q} \in \hat{Q}$ the continuous dynamics $\dot{x} \in f(x, \overline{q}, u, d)$, $d \in D$ belong to one of the above cited classes of systems. Since the application example falls in the class of systems described in [17, 28], we summarize the main result here. For this sake, we restrict the structure of $H$ and $Bad$ to that of a two-agent game.

**Definition 22.** The pair $(H, Bad)$ has the form of a two-agent game provided $H = H^1 \parallel H^2$ with $H^i = (Q^i, X^i, U^i, D^i, \Sigma^i, R^i, f^i)$ for $i \in \{1, 2\}$ with $Q^1 = \emptyset$, $D^1 = \emptyset$, $\Sigma^1 = \emptyset$, $U^2 = \emptyset$, and $Bad = B^1 \times B^2$ with $B^i \subseteq X^i$.

**Proposition 15.** *Let $(H, Bad)$ be in the form of a two-agent game. Assume that*

(i) *$U^1 = [u_L, u_H] \subseteq \mathbb{R}$; the flow of $H^1$ denoted $\phi^1(t, \cdot, \cdot) : X \times \mathcal{S}(U) \to X$ is an order preserving function in both arguments; there is $\zeta > 0$ such that $f^1_1(x^1, u) \geq \zeta$; $B^1 = B^1_1 \times \mathbb{R}^{n_1 - 1}$;*

(ii) *For $\hat{q} \in \hat{Q}$ there are $\theta_L, \theta_U \in \mathbb{R}$ and a function $\overline{f} : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n$ such that $\{f^2(x^2, \hat{q}, d) \mid d \in D^2\} = \{\overline{f}(x^2, \theta) \mid \theta \in [\theta_L, \theta_U]\}$; the flow of $\dot{x}^2 = \overline{f}(x^2, \theta)$, that is, $\phi^2(t, \cdot, \cdot) : X \times \mathcal{S}([\theta_L, \theta_U]) \to X$, is an order preserving map in both arguments; there is $\zeta > 0$ such that $\overline{f}_1(x^2, u) \geq \zeta$; $B^2 = B^2_1 \times \mathbb{R}^{n_2 - 1}$.*

*Then, $Pre(\hat{q}, Bad) = Pre(\hat{q}, Bad)_L \cap Pre(\hat{q}, Bad)_H$, in which $Pre(\hat{q}, Bad)_L = \{x_o \in X \mid \exists\, t,\ \mathbf{d}$ s.t. some $\phi_{\hat{x}}(t, (\hat{q}, x_o), \mathbf{d}, u_L, \epsilon) \in Bad\}$ and $Pre(\hat{q}, Bad)_H = \{x_o \in X \mid \exists\ t,\ \mathbf{d}$ s.t. some $\phi_{\hat{x}}(t, (x_o, \hat{q}), \mathbf{d}, u_H, \epsilon) \in Bad\}$. A feedback map $\hat{\pi}(\hat{q}, x) \in \Pi(\hat{q}, x)$ is given by*

$$\hat{\pi}(\hat{q}, x) := \begin{cases} u_L & if\ \ x \in Pre(\hat{q}, Bad)_H \wedge x \in \partial Pre(\hat{q}, Bad)_L \\ u_H & if\ \ x \in Pre(\hat{q}, Bad)_L \wedge x \in \partial Pre(\hat{q}, Bad)_H \\ u_L & if\ \ x \in \partial Pre(\hat{q}, Bad)_L \wedge \partial Pre(\hat{q}, Bad)_L \\ * & otherwise. \end{cases} \quad (4)$$

By virtue of this result, one can avoid computing the set $\text{Pre}(\hat{q}, Bad)$, which requires optimization over the space of control inputs. One can instead compute the sets $\text{Pre}(\hat{q}, Bad)_L$ and $\text{Pre}(\hat{q}, Bad)_H$, which, since the control input is fixed and the flow preserves the ordering, can be computed by linear complexity algorithms. The structure of the set *Bad* well models collision configurations between agents sharing a common space as illustrated in the application examples of Section VIII. We omit the details of the algorithms, which can be found elsewhere [17, 28] and instead present in Section VIII their application to a concrete example.

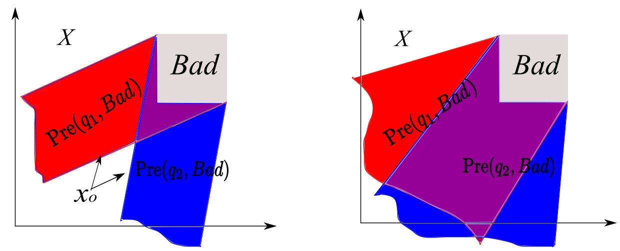


Fig. 2. (Left) Example 3, in which the continuous dynamics are given by equations (5). (Right) Example 3, in which the continuous dynamics are given by equations (6). The set $\text{Pre}(q_1, Bad)$ is in red while the set $\text{Pre}(q_2, Bad)$ is in blue. Both sets extend to $-\infty$.

## VII. Equivalence between Problem 1 and Problem 2

Showing that Problem 1 is equivalent to Problem 2 is based on showing that for all $\overline{q} \in \hat{Q}$ we have that $\hat{C}_{\overline{q}} = C_{\overline{q}}$. In general, the set of possible continuous trajectories of system $\hat{H}$ for every mode $\overline{q} \subseteq Q$ contains but is not equal to the set of continuous trajectories possible in $H$. This is due to the fact that in $H$ not all transitions may be possible among the modes in $\overline{q}$ due to the structure of $R$. This information was lost in the construction of $\hat{H}$ in order to obtain a hybrid system with uncontrolled mode transitions and *known* discrete/continuous state. In order to illustrate this point, consider the following example.

*Example* 3. Consider system $H$ with two modes $q_1$ and $q_2$ between which there is no transition and let the continuous dynamics for each mode be given, for $x \in \mathbb{R}^2$, by

$$\dot{x} = \begin{pmatrix} 2 \\ 1 \end{pmatrix} u, \text{ for } q = q_1 \text{ and } \dot{x} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} u, \text{ for } q = q_2, \quad (5)$$

in which $u \in [0,1]$ and $\overline{q}_o = \{q_1, q_2\}$. Let $Bad = [1,2] \times [1,2]$. In order to determine $C_{\overline{q}_o}$, refer to the left plot of Figure 2, in which we depict the sets $\text{Pre}(q_1, Bad)$ and $\text{Pre}(q_2, Bad)$. Any point $x_o \notin \text{Pre}(q_1, Bad) \cup \text{Pre}(q_2, Bad)$ admits a control that keeps $x_o$ outside $Bad$ for every initial mode. This is due to the fact that the mode of $H$ does not switch and hence a continuous trajectory starting at $x_o$ will follow either of the two directions depicted, none of which takes the flow inside $Bad$. Hence, we have that $C_{\overline{q}_o} = \text{Pre}(q_1, Bad) \cup \text{Pre}(q_2, Bad)$. By contrast, we have that $\hat{C}_{\overline{q}_o} = \text{Pre}(\overline{q}_o, Bad)$, which includes point $x_o$ in Figure 2 as this can be taken to $Bad$ by, for example, first flowing under $q_1$ and then under $q_2$. Hence, in this case we have that $\hat{C}_{\overline{q}_o}$ is strictly larger than $C_{\overline{q}_o}$.

If we instead had that $\text{Pre}(\overline{q}_o, Bad) = \text{Pre}(q_1, Bad) \cup \text{Pre}(q_2, Bad)$, we would also have that $\hat{C}_{\overline{q}_o} = C_{\overline{q}_o}$. In order to illustrate how we can obtain this equality, we modify system (5) to

$$\begin{aligned} \dot{x} &= \begin{pmatrix} 2 \\ 1 \end{pmatrix} u + \begin{pmatrix} 1 \\ 1 \end{pmatrix} d, \ d \in [0,1], \text{ when } q = q_1 \\ \dot{x} &= \begin{pmatrix} 1 \\ 2 \end{pmatrix} u + \begin{pmatrix} 1 \\ 1 \end{pmatrix} d, \ d \in [0,1], \text{ when } q = q_2. \end{aligned} \tag{6}$$

In this case, the sets $\text{Pre}(q_1, Bad)$ and $\text{Pre}(q_2, Bad)$ are larger than before and are depicted in the right side plot of Figure 2. One can check that in this case we still have that $C_{\overline{q}_o} = \text{Pre}(q_1, Bad) \cup \text{Pre}(q_2, Bad)$ and that $\hat{C}_{\overline{q}_o} = \text{Pre}(\overline{q}_o, Bad)$. But, as opposed to before, we also have that $\text{Pre}(\overline{q}_o, Bad) = \text{Pre}(q_1, Bad) \cup \text{Pre}(q_2, Bad)$ so that the two capture sets are the same, that is, $\hat{C}_{\overline{q}_o} = C_{\overline{q}_o}$.

This example illustrates an instance of a system in which $C_{\overline{q}} \neq \hat{C}_{\overline{q}}$ due to $\text{Pre}(\overline{q}, Bad)$ not being equal to $\bigcup_{q_i \in \overline{q}} \text{Pre}(q_i, Bad)$. It also illustrates how requiring that $\text{Pre}(\overline{q}, Bad) \subseteq \bigcup_{q_i \in \overline{q}} \text{Pre}(q_i, Bad)$ (note that $\bigcup_{q_i \in \overline{q}} \text{Pre}(q_i, Bad) \supseteq \text{Pre}(\overline{q}, Bad)$ derives from the definition of Pre) is sufficient to have $C_{\overline{q}} = \hat{C}_{\overline{q}}$. We thus pose the following assumption.

**Assumption 1.** For all $\overline{q} \in \hat{Q}$ we have that $\text{Pre}(\overline{q}, Bad) \subseteq \bigcup_{q_i \in \overline{q}} \text{Pre}(q_i, Bad)$.

This assumption requires that if an initial state $x_o$ is taken to $Bad$ by an arbitrary sequence of modes in $\overline{q}$, then there is a disturbance signal for which it is also taken to $Bad$ by at least one mode $q_i \in \overline{q}$. We provide at the end of this section classes of systems for which this assumption is satisfied.

Since by Lemma 1, $\text{Pre}(q_i, Bad) \subseteq \hat{C}_{\overline{q}}$ for all $q_i \in \overline{q}$, in order to obtain equivalence, we should at least have that $\text{Pre}(q_i, Bad)$ is also a subset of $C_{\overline{q}}$, which is not the case in general. In fact, an element $x_o$ is in $\text{Pre}(q_i, Bad)$ if and only if there is no feedback map $\pi'(x)$ that prevents the flow starting from this element to end-up in $Bad$. Nevertheless, for such an element $x_o$ there could still be a feedback map $\pi(\overline{q}(\boldsymbol{\eta}(t)), x)$ that prevents the flow originating from it to enter $Bad$. Hence, $x_o$ may not be in $C_{\overline{q}}$. However, if $x(t) = \phi_x(t, (x_o, q_i), \mathbf{u}, \mathbf{d}, \epsilon)$ implies that $\overline{q}(\boldsymbol{\eta}(t))$ is equal to a constant for all $t > 0$, then the map $\pi(\overline{q}(\boldsymbol{\eta}(t)), x)$ that prevents the flow from entering $Bad$ becomes a simple feedback map $\pi'(x)$. In this case, if $x_o$ is in $\text{Pre}(q_i, Bad)$, it must also be in $C_{\overline{q}}$. The next assumption and proposition provide conditions for when this is the case.

**Definition 23.** A mode $q_i \in Q$ is called *weakly distinguishable* provided

(i) there is a set of modes $I_{q_i} \subseteq Q$ such that $f(x, q_i, u, D) \subseteq f(x, q, u, D)$ for all $q \in I_{q_i}$ and for all $(x, u) \in X \times U$;
(ii) for all $(x, u) \in X \times U$ there is $d \in D$ such that $f(x, q_i, u, d) \notin f(x, q, u, D)$ for all $q \notin I_{q_i}$.

The set $I_{q_i}$ is called the *indistinguishable set* for $q_i$.

Note that in the case in which the indistinguishable set for $q_i$ is $q_i$ itself, the mode $q_i$ is distinguishable from any other mode, that is, for all $(x, u)$ there is $d$ such that $f(x, q_i, u, d) \notin f(x, q_j, u, D)$ for all $q_j \neq q_i$. Weak distinguishability allows for $q_i$ to generate the same vector fields as those generated by the modes in the set $I_{q_i}$.

**Assumption 2.** System $H$ is such that all modes in $Q$ are weakly distinguishable.

**Proposition 16.** *Let $q_i \in \overline{q}_o$, and $x(t) = \phi_x(t, (q_i, x_o), \mathbf{u}, \mathbf{d}, \epsilon)$. Then, Assumption 2 implies that there is $d(0)$ such that $\overline{q}(\boldsymbol{\eta}(t)) = Reach(Reach(\overline{q}_o) \cap I_{q_i})$ for all $t > 0$.*

*Proof:* Assumption 2 implies that for all $(x(0), u(0))$, there is a $d(0)$ such that $f(x(0), q_i, u(0), d(0)) = f(x(0), q_j, u(0), \overline{d}(0))$ for some $\overline{d}(0) \in D$ implies that $q_j \in I_{q_i}$. Hence, $\overline{q}(\boldsymbol{\eta}(t))$ can be re-written as

$$\overline{q}(\boldsymbol{\eta}(t)) = \left\{ \begin{array}{r} q \in Q \mid \exists\, q_o \in \overline{q}_o,\ \boldsymbol{\sigma} \ s.t. \ q = \phi_q(t, q_o, \boldsymbol{\sigma}), \\ \phi_q(0, q_o, \boldsymbol{\sigma}) \in I_{q_i}, \text{ and } \exists\, \overline{\mathbf{d}} \ s.t. \\ \dot{x}(\tau) = f(x(\tau), \phi_q(\tau, q_o, \boldsymbol{\sigma}), u(\tau), d(\tau)) \text{ for all } \tau < t \end{array} \right\}.$$

This, in turn, implies that $\overline{q}(\boldsymbol{\eta}(t)) \subseteq \text{Reach}(\text{Reach}(\overline{q}_o) \cap I_{q_i})$ for all $t > 0$.

Let $q^* \in \text{Reach}(\text{Reach}(\overline{q}_o) \cap I_{q_i})$. Then, for all $t > 0$ there are $\boldsymbol{\sigma}$ and $q_o \in \overline{q}_o$ such that $q^* = \phi_q(t, q_o, \boldsymbol{\sigma})$ and $\phi_q(\tau, q_o, \boldsymbol{\sigma}) \in \text{Reach}(\overline{q}_o) \cap I_{q_i}$ for all $\tau < t$. This, in turn, implies that $\phi_q(0, q_o, \boldsymbol{\sigma}) \in I_{q_i}$. Since for all $\mathbf{d}$ we have that $\dot{x}(\tau) = f(x(\tau), q_i, u(\tau), d(\tau)) \in f(x(\tau), q, u(\tau), D)$ for all $q \in I_{q_i}$, there must be a disturbance signal $\mathbf{d}^*$ such that $\dot{x}(\tau) = f(x(\tau), \phi_q(\tau, q_o, \boldsymbol{\sigma}), u(\tau), d^*(\tau))$ for all $\tau < t$. Hence, we also have that $q^* \in \overline{q}(\boldsymbol{\eta}(t))$ for all $t > 0$. ■

**Lemma 2.** *Let Assumption 2 hold. Then, we have that $Pre(q_i, Bad) \subseteq C_{\overline{q}}$ for all $q_i \in \overline{q}$.*

*Proof:* Let $x_o \notin C_{\overline{q}}$, then there is a feedback map $\pi$ such that for all $q \in \overline{q}$, $\boldsymbol{\sigma}$, $\mathbf{d}$, it guarantees that $\phi_x^{\pi}(t, (q, x_o), \mathbf{d}, \boldsymbol{\sigma}) \notin Bad$ for all $t \geq 0$. This holds in particular for $q = q_i$, $\boldsymbol{\sigma} = \epsilon$ and $\mathbf{d}$ such that $d(0)$ leads to $\overline{q}(\boldsymbol{\eta}(t)) = \text{Reach}(\text{Reach}(\overline{q}) \cap I_{q_i})$ for all $t > 0$, which exists by Proposition 16. In this case, $\pi(\overline{q}(\boldsymbol{\eta}(t)), x) = \pi(\text{Reach}(\text{Reach}(\overline{q}) \cap I_{q_i}), x) =: \pi'(x)$ is a simple feedback from $x$ for all $t > 0$. Since $x(0^+) = x(0) = x_o$, we thus have that $\pi'$ is also such that $\phi_x^{\pi'}(t, (q_i, x_o), \mathbf{d}, \epsilon) \notin Bad$ for all $\mathbf{d}$. Hence, $x_o \notin \text{Pre}(q_i, Bad)$. ■

**Theorem 5.** *Under Assumptions 1 and 2, Problem 1 and Problem 2 are equivalent.*

*Proof:* Proposition 4 proves that $C_{\overline{q}} \subseteq \hat{C}_{\overline{q}}$. We next prove the reverse inclusion. Specifically, by Lemma 1 and Assumption 1 we have that $\hat{C}_{\overline{q}} \subseteq \bigcup_{q \in \text{Reach}(\overline{q})} \text{Pre}(q, Bad)$, in which by Lemma 2 we have that $\text{Pre}(q, Bad) \subseteq C_{\text{Reach}(\overline{q})}$, in which $C_{\text{Reach}(\overline{q})} = C_{\overline{q}}$ by Proposition 2. This proves equivalence. ■

### A. Systems that satisfy Assumption 1 and Assumption 2

Assumption 1 can be difficult to check for general hybrid systems. We thus provide two classes of systems for which such an assumption is satisfied and illustrate in the next section how one of these classes well models the application example. We first introduce two intermediate results.

**Proposition 17.** *Let $x \in \mathbb{R}^n$, $\theta \in \Theta \subseteq \mathbb{R}^p$ with $(\Theta, \leq)$ a lattice, and consider the system $\dot{x} = f(x, \theta)$, in which $\theta \in \cup_{k\in\{1,...,N\}}[\theta_L^k, \theta_U^k]$. Assume that*

- (i) *the flow of the system $\phi(t, x_o, \circ) : \mathcal{S}(\Theta) \to \mathbb{R}^n$ is a continuous and order preserving map for all $x_o \in \mathbb{R}^n$ and $t \in \mathbb{R}_+$;*
- (ii) *we have that $[\theta_L^k, \theta_U^k] \cap [\theta_L^{k+1}, \theta_U^{k+1}] \neq \emptyset$, $\theta_L^1 \leq \theta_L^k$, and $\theta_U^N \geq \theta_U^k$ for all $k \in \{1, ..., N-1\}$.*

*Then, for all $x_o$, $T > 0$, $i \in \{1, ..., n\}$, and $\overline{x_i}$ such that there is $\boldsymbol{\theta}$ with $\theta(t) \in \cup_{k\in\{1,...,N\}}[\theta_L^k, \theta_U^k]$ for $t < T$ and with $\phi_i(T, x_o, \boldsymbol{\theta}) = \overline{x_i}$, there are $k \in \{1, ..., N\}$ and $\boldsymbol{\theta}'$ with $\theta'(t) \in [\theta_L^k, \theta_U^k]$ for $t < T$ such that $\phi_i(T, x_o, \boldsymbol{\theta}') = \overline{x_i}$.*

*Proof:* Let $\overline{x_i} = \phi_i(T, x_o, \boldsymbol{\theta})$ for $\theta(t) \in \cup_{k\in\{1,...,N\}}[\theta_L^k, \theta_U^k]$ for $t < T$. By property (i) and property (ii), we have that $[\phi_i(T, x_o, \theta_L^j), \phi_i(T, x_o, \theta_U^j)] \cap [\phi_i(T, x_o, \theta_L^{j+1}), \phi_i(T, x_o, \theta_U^{j+1})] \neq \emptyset$ for all $j \in \{1, ..., N-1\}$. Hence, it follows that $\bigcup_{k\in\{1,...,N\}}[\phi_i(T, x_o, \theta_L^k), \phi_i(T, x_o, \theta_U^k)] = [\phi_i(T, x_o, \theta_L^1), \phi_i(T, x_o, \theta_U^N)]$. Since $\overline{x_i} \in [\phi_i(T, x_o, \theta_L^1), \phi_i(T, x_o, \theta_U^N)]$, this implies that there is $k \in \{1, ..., N\}$ such that $\overline{x_i} \in [\phi_i(T, x_o, \theta_L^k), \phi_i(T, x_o, \theta_U^k)]$. Since $\phi$ is a continuous map from the space of input signals to $\mathbb{R}^n$, it maps the connected set $\mathcal{S}([\theta_L^k, \theta_U^k])$ for all $k$ to the connected set $\phi_i(T, x_o, \mathcal{S}([\theta_L^k, \theta_U^k]))$. Since all connected sets in $\mathbb{R}$ are intervals, we have that $\phi_i(T, x_o, \mathcal{S}([\theta_L^k, \theta_U^k])) = [\phi_i(T, x_o, \theta_L^k), \phi_i(T, x_o, \theta_U^k)]$. Hence, $\overline{x_i} \in \phi_i(T, x_o, \mathcal{S}([\theta_L^k, \theta_U^k]))$, which implies that there is $\boldsymbol{\theta}'$ with $\theta'(t) \in [\theta_L^k, \theta_U^k]$ for $t < T$ such that $\phi_i(T, x_o, \boldsymbol{\theta}') = \overline{x_i}$. ■

This proposition states that for a system defined on partial orders whose flow preserves the order and whose set of inputs is a connected union of intervals, any point reachable by a coordinate of the flow through an arbitrary input signal can also be reached by an input signal that takes values in one only of the possible intervals.

**Proposition 18.** *Let $x, L^k, U^k \in \mathbb{R}^n$ for $k \in \{1, ..., N\}$ and consider a differential inclusion of the form $\dot{x} \in [L^1, U^1] \cup ... \cup [L^N, U^N]$. Assume that there are $L, U \in \mathbb{R}^n$ such that $[L^1, U^1] \cup ... \cup [L^N, U^N] = [L, U]$. Then, for all $x_o, \overline{x} \in \mathbb{R}^n$ and $T > 0$ such that $x_o + \int_0^T \dot{x}(t)dt = \overline{x}$, there is $k \in \{1, ..., N\}$ such that $x_o + \int_0^T \dot{x}(t)dt = \overline{x}$ with $\dot{x}(t) \in [L^k, U^k]$ for $t < T$.*

*Proof:* Let $\overline{x} = x_o + \int_0^T \dot{x}(t)dt$ for $\dot{x}(t) \in [L, N]$ for all $t \leq T$. Re-writing this equality component-wise, we have that for all $i \in \{1, ..., n\}$ $\overline{x_i} - x_{0i} = \int_0^T \dot{x}_i(t)dt$ for $\dot{x}_i(t) \in [L_i, U_i]$ for all $t \leq T$. Then, there is $c_i \in [L_i, U_i]$ such that $\int_0^T \dot{x}_i(t)dt = c_i T$ and hence such that $\overline{x_i} - x_{0i} = c_i T$. The constant vector $c := (c_1, ..., c_n)'$ is thus such that $\overline{x} - \overline{x_o} = cT$, in which $c \in [L, U]$. Since $[L, U] = [L^1, U^1] \cup ... \cup [L^N, U^N]$, there is $k \in \{1, ..., N\}$ such that $c \in [L^k, U^k]$. Hence, there is $k \in \{1, ..., N\}$ such that $\overline{x} - \overline{x_o} = \int_0^T \dot{x}(t)dt$ for $\dot{x}(t) \in [L^k, N^k]$ for all $t \leq T$. ■

This proposition states that any point that can be reached under a rectangular differential inclusion in the form of a union of "smaller" rectangular differential inclusions can also be reached under at least one of these smaller rectangular differential inclusions.

**Proposition 19.** *Let $(H, Bad)$ be in the form of a two-agent game. Assumption 1 is satisfied if for all $\overline{q} \in \hat{Q}$ with $\overline{q} = \{q_1, ..., q_N\}$ either one of the two following properties are satisfied by $H^2$:*

- (i) *for all $q_k \in \overline{q}$ there are $L^k, U^k \in \mathbb{R}^n$ such that $\{f^2(x^2, q_k, d) \mid d \in D^2\} = [L^k, U^k]$, there are $L, U \in \mathbb{R}^n$ such that $\{f^2(x^2, \overline{q}, d) \mid d \in D^2\} = [L, U]$, and $[L^1, U^1] \cup ... \cup [L^N, U^N] = [L, U]$;*
- (ii) *for all $q_k \in \overline{q}$ there are $\theta_L^k, \theta_U^k \in \Theta$ with $(\Theta, \leq)$ a lattice and a function $f : \mathbb{R}^n \times \Theta \to \mathbb{R}^n$ such that $\{f^2(x^2, q_k, d) \mid d \in D^2\} = \{f(x^2, \theta) \mid \theta \in [\theta_L^k, \theta_U^k]\}$ and $\{f^2(x^2, \overline{q}, d) \mid d \in D^2\} = \{f(x^2, \theta) \mid \theta \in \cup_{k\in\{1,...,N\}}[\theta_L^k, \theta_U^k]\}$, $\dot{x} = f(x, \theta)$ with $\theta \in \cup_{k\in\{1,...,N\}}[\theta_L^k, \theta_U^k]$ satisfies (i) and (ii) of Proposition 17, and $B^2 = B_1^2 \times \mathbb{R}^n$.*

*Proof:* Let $(x_0^1, x_0^2) \in \text{Pre}(\overline{q}, Bad)$, we show that when either (i) or (ii) is satisfied there is $q_k \in \overline{q}$ such that $(x_0^1, x_0^2) \in \text{Pre}(q_k, Bad)$. We consider first case (i). Then, for all feedback maps $\pi$ there is a $T > 0$ such that $\phi_{x^1}^{\pi}(T, x_0^1) \in B^1$ and $x_0^2 + \int_0^T \dot{x}^2(t) = x^2(T) \in B^2$ for $\dot{x}^2(t) \in [L, U]$ for all $t < T$. Let $\overline{x}^2 := x^2(T)$, then by Proposition 18 there is $k \in \{1, ..., N\}$ such that $x_0^2 + \int_0^T \dot{x}^2(t)dt = \overline{x}^2 \in B^2$ with $\dot{x}(t) \in [L^k, U^k]$ for $t < T$. Hence, $(x_0^1, x_0^2) \in \text{Pre}(q_k, Bad)$.

Consider now case (ii). We have that for all feedback maps $\pi$ there are $T > 0$ and $\boldsymbol{\theta}$ with $\theta(t) \in \cup_{k\in\{1,...,N\}}[\theta_L^k, \theta_U^k]$ for all $t < T$ such that $\phi_{x^1}^{\pi}(T, x^1) \in B^1$ and $\phi_{x_1^2}(T, x^2, \boldsymbol{\theta}) \in B_1^2$. Let $\overline{x}_1^2 := \phi_{x_1^2}(T, x^2, \boldsymbol{\theta})$, then by Proposition 17 there are also $k \in \{1, ..., N\}$ and $\boldsymbol{\theta}'$ with $\theta'(t) \in [\theta_L^k, \theta_U^k]$ for all $t < T$ such that $\overline{x}_1^2 := \phi_{x_1^2}(T, x^2, \boldsymbol{\theta}')$. Hence, $(x^1, x^2) \in \text{Pre}(q_k, Bad)$. ■

This proposition states that if $(H, Bad)$ is in the form of a two-agent game and the continuous dynamics of $H^2$ (the uncontrolled agent) have either the order preserving properties established by the assumptions of Proposition 17 or can be modeled by a family of differential inclusions according to Proposition 18, then Assumption 1 is satisfied. In turn, the assumptions of Propositions 17 and 18 are simple to check. Note that modeling the uncontrolled agent by a family of switching differential inclusions is often a practical approach when an accurate dynamical model of such an agent is missing. In this case, rectangular differential inclusions can be effectively employed to approximate the agent dynamics for safety control purposes. Similarly, systems whose dynamics have order preserving properties are found in several application domains, including biological networks [2, 3] and networks of agents evolving on pre-specified paths such as trains on rails [32, 41], aircrafts on their routes [33, 42], and vehicles in their lanes [22, 24].

Assumption 2 requires that for all values $(x, u)$, the possible vector fields generated by any given mode $q_i$ cannot be all generated by modes that do not belong to the indistinguishable set for $q_i$. In the case in which $f(x,q_i,u,d)$ is affine in the disturbance $d$, that is, $f(x,q_i,u,d) = h(x,q_i,u) + g(x,u)d$, in which $h(x,q_i,u)$ can be regarded as the "nominal" dynamics, a sufficient condition for weak distinguishability of mode $i$ is given, for example, when the nominal dynamics of mode $q_i$ are not possible dynamics in any other mode. This can, in turn, be ensured if $||h(x,q_i,u) - h(x,q_j,u)|| > \sup_{d\in D}||g(x,u)d||$. As an example, consider $f$ in the form of a chain of integrators, that is, $f(x,q_i,u,d) = (x_2,...,x_n,\beta_i + u + d)$. Letting $d \in [-\overline{d},\overline{d}]$ for some $\overline{d} > 0$, one can verify that any mode $q_i$ is weakly distinguishable if $|\beta_i - \beta_j| > \overline{d}$ for all $j \neq i$. For the special case in which $f$ is linear, one can obtain the following general sufficient condition for weak distinguishability.

**Proposition 20.** *Let $f(x,q_i,u,d) = A_i x + B_i u + M_i d$ with $u \in U \subseteq \mathbb{R}^m$ and $d \in D \subseteq \mathbb{R}^p$ for all $q_i \in Q$. Then, mode $q_i$ is weakly distinguishable if ColSpan$\{M_i\}\cap$ColSpan$\{A_i - A_j \mid B_i - B_j \mid M_j\} = 0$ for all $j \neq i$.*

*Proof:* If ColSpan$\{M_i\}\cap$ColSpan$\{A_i - A_j \mid B_i - B_j \mid M_j\} = 0$ for all $j \neq i$, then for all $d, d^*, u, x$ with $M_i d \neq 0$ we have that $M_i d \neq (A_i - A_j)x + (B_i - B_j)u + M_j d^*$, which is equivalent to having $M_i d + A_i x + B_i u \neq M_j d^* + A_j x + B_j u$. This, in turn, is equivalent to having that there is $d$ such that $f(x,q_i,u,d) \neq f(x,q_j,u,d^*)$ for all $x,u,d^*$, which implies weak distinguishability. ■

Finally, consider the class of systems introduced in Proposition 15, in which for all $\hat{q} = q_k \in Q$ we have $\theta \in [\theta_L^k, \theta_U^k]$. If for every $k$ we have that $[\theta_L^k, \theta_U^k] \not\subseteq \bigcup_{j\neq k}[\theta_L^j, \theta_U^j]$ and the map $f^2 : X \times \Theta \to X$ is strongly order preserving with respect to the second argument, then Assumption 2 is satisfied. Similarly, consider case (i) of Proposition 19. If for all $k$ such that $q_k \in Q$ we have that $[L^k, U^k] \not\subseteq \bigcup_{j\neq k}[L^j, U^j]$, then Assumption 2 is satisfied.

## VIII. Application Example: Control Design

Consider the application example described in Section IV-B and depicted in Figure 1. Here, we construct an estimator, calculate the mode-dependent capture sets, and determine the feedback map. An estimator $\hat{H} = (\hat{Q}, X, U, D, Y, \hat{R}, \hat{f})$ is uniquely determined by $\hat{Q}, \hat{R}$, and $Y$. We set $\hat{Q} = \{\hat{q}_1, \hat{q}_2, \hat{q}_3\}$, in which $\hat{q}_1 = \{a,b,c\}$, $\hat{q}_2 = \{c,b\}$, and $\hat{q}_3 = \{b\}$. To determine $\hat{R}$ and $Y$, consider the estimate $\hat{\beta}(t) = \frac{1}{T}\int_{t-T}^{t} \dot{v}_2(\tau)d\tau,\ \ t > T$. For each possible value of $q(t)$, we compute the interval in which $\hat{\beta}(t)$ must lie. Thus, we have to consider three cases: (1) $q(t) = a$; (2) $q(t) = c$; (3) $q(t) = b$.

Case (1): $q(t) = a$. Then, in the interval of time $[t - T, t]$, the mode $q(t)$ can only have been equal to $a$. Since it is still possible that $\dot{v}_2(t) = 0$ when $v_{max}$ is exceeded, we have that $\dot{v}_2(\tau) = \beta_a + \tilde{d}(\tau)$ with $|\tilde{d}(\tau)| \leq \beta_a$ for $\tau \in [t - T, t]$. This, in turn, leads to having $|\hat{\beta}(t) - \beta_a| \leq \beta_a$.

Case (2): $q(t) = c$. Then, in the interval of time $[t - T, t]$, the mode $q(t)$ can be $c$ for all time or be first equal to $a$ and then be equal to $c$. In this case, we have that $\dot{v}_2(\tau) = \frac{\beta_a}{2} + \tilde{d}(\tau)$ for some $\tilde{d}(\tau)$ such that $|\tilde{d}(\tau)| \leq \frac{\beta_a}{2} + \overline{d}$. As a consequence, we have that $\hat{\beta}(t) \in [-\overline{d}, \beta_a + \overline{d}]$.

Case (3): $q(t) = b$. Then, in the interval of time $[t - T, t]$, the mode $q(t)$ can be in $b$ for all time, or also in $c$ for some time, or also in $a$ and then $c$ for some time. It is easy to verify that this implies that $\hat{\beta}(t) \in [-|\beta_b| - \overline{d}, \beta_a + \overline{d}]$, that is, $\hat{\beta}(t)$ can be anywhere.

Hence, we have that if $\hat{\beta}(t) \in [-|\beta_b| - \overline{d}, -\overline{d}]$ then necessarily $q(t) = b$. Similarly, if $\hat{\beta}(t) \in [-\overline{d}, 0]$ then, $a$ is not currently possible and thus we must have that $q(t) \in \{c, b\}$. As a consequence, we let $Y = \{y_{cb}, y_b, \epsilon\}$ and define for $t > T$ $y(t) = y_{cb}$ if $\hat{\beta}(t) \in [-\overline{d}, 0]$, $y(t) = y_b$ if $\hat{\beta}(t) \in [-|\beta_b| - \overline{d}, -\overline{d}]$, and $y(t) = \epsilon$ otherwise. Thus, $\hat{R}$ is such that $\hat{R}(\hat{q}_1, y_{cb}) = \hat{q}_2$, $\hat{R}(\hat{q}_1, y_b) = \hat{q}_3$, and $\hat{R}(\hat{q}_2, y_b) = \hat{q}_3$. System $\hat{H}$ is represented in the top left diagram of Figure 3. The properties of an estimator are satisfied as when $a$ or $\{a, c\}$ are ruled out, the structure of $R$ guarantees that $q(t)$ cannot take again those values. By Theorem 3, Algorithm 1 terminates and by Lemma 1 we have that $\hat{C}_{\hat{q}_1} = \mathrm{Pre}(\hat{q}_1, Bad)$, $\hat{C}_{\hat{q}_2} = \mathrm{Pre}(\hat{q}_2, Bad)$, and $\hat{C}_{\hat{q}_3} = \mathrm{Pre}(\hat{q}_3, Bad)$. Since for all $\hat{q} \in \hat{Q}$, the assumptions of Proposition 15 are satisfied, we employ such a proposition to determine whether $x \in \mathrm{Pre}(\hat{q}_i, Bad)$ for all $i \in \{1,2,3\}$ and to determine the feedback map $\hat{\pi}$. Assumption 1 is satisfied and Assumption 2 is also satisfied for $x_4 \in (v_{min}, v_{max})$. Simulation results are shown in panels (a)-(e) of Figure 3.

## IX. Conclusions

In this paper, we have addressed the safety control problem for hybrid systems in which the mode is not available for control (HMHS). We have adopted an approach inspired by the theory of games with imperfect information. Specifically, we have introduced the notion of non-deterministic discrete information state and formulated the control problem on its basis (Problem 1). We have introduced the notion of an estimator and we have formulated a control problem with perfect state information on a new hybrid automaton $\hat{H}$ (Problem 2). We have provided an algorithm for the computation of the capture set for $\hat{H}$ and for the least restrictive control map. We have provided conditions for the termination of the iterative algorithm that computes the capture set. We have also shown how to construct an abstraction of $\hat{H}$ for which the algorithm always terminates and has as fixed point the capture set of $\hat{H}$. We showed that Problem 2 is equivalent to Problem 1 under suitable assumptions and provided classes of systems for which these assumptions are satisfied. Accordingly, an application example in the context of cooperative active safety systems has been presented. Future research will include removing Assumptions 1 and 2 by employing a dynamic feedback design that does not impose separation between estimation and control. Also, we will consider the case in which there is a non-zero minimum dwell time associated with the modes in $Q$.

## References


[1] U.S. DOT Joint Program Office ITS. http://www.its.dot.gov.

[2] D. Angeli and E.D. Sontag. Interconnections of monotone systems with steady-state characteristics. *Optimal control, stabilization and nonsmooth analysis. Lecture Notes in Control and Inform. Sci. Springer*, 301:135–154, 2004.

[3] D. Angeli and E.D. Sontag. Oscillations in I/O monotone systems. *IEEE Transactions on Circuits and Systems*, 55:166–176, 2008.

[4] J. Aubin. *Viability Theory*. Birkhäuser, 1991.

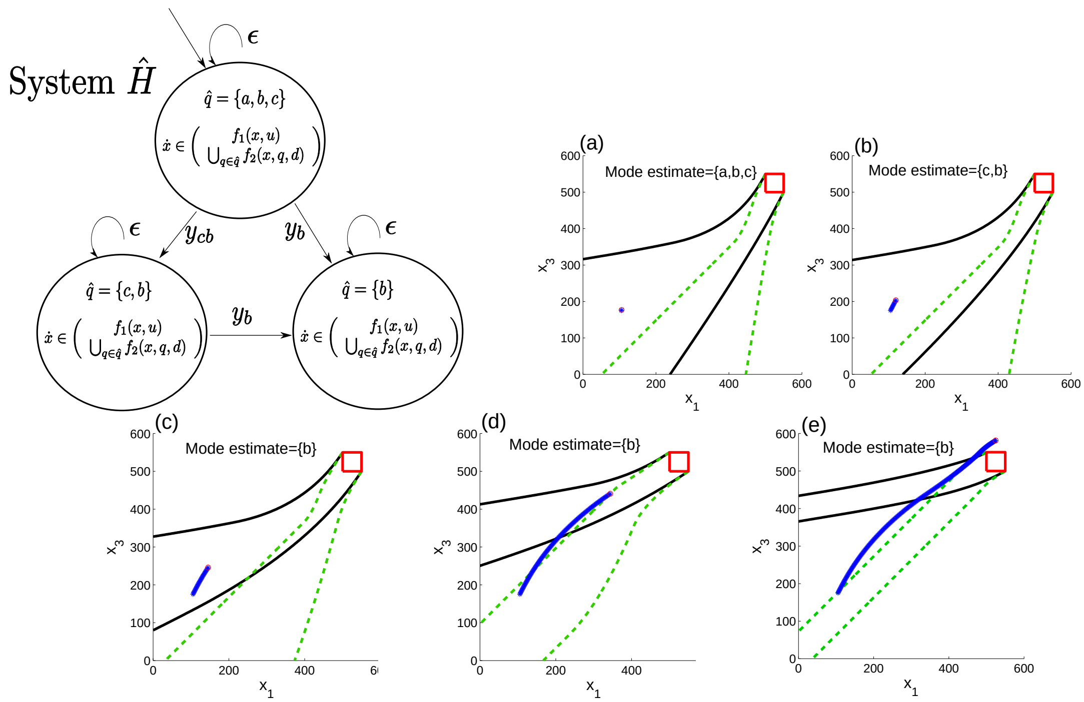


Fig. 3. (Top Left) Diagram representing $\hat{H}$. In each of the plots (a)–(e), the red box represents $[L_1, U_1] \times [L_2, U_2]$. In the simulation, we have $L_1 = L_2 = 500$, $U_1 = U_2 = 550$, $U = [-1, 1]$, $D = [-0.4, 0.4]$, $\beta_a = 0.6, \beta_c = 0$, and $\beta_b = -0.6$. The black solid lines delimit the slice of the set $\text{Pre}(\hat{q}, Bad)_H$ for the current speeds values $(x_2, x_4)$. Similarly, the green dashed lines delimit the slice of the set $\text{Pre}(\hat{q}, Bad)_L$ for the same current speeds values $(x_2, x_4)$. The intersection of these two slices delimits the slice of the current mode dependent capture set $\hat{C}_{\hat{q}}$ for the same current speeds values $(x_2, x_4)$. The red circle denotes the pair of current longitudinal displacements $x_1, x_3$, while the blue trace represents the trajectory of this pair. The initial (unknown) driving mode of the human driver is acceleration $a$ and it stays constant for the first 1 second, then from 1 to 3 seconds, the driving mode is coasting $c$, and finally after 3 seconds the mode is braking $b$. Plot (a) shows the pair of initial longitudinal displacements. Here, the current mode estimate is $\hat{q} = \{a, b, c\}$ and the current mode dependent capture set is $\hat{C}_{\hat{q}_1}$. Plot (b) shows the mode estimate switching to $\hat{q} = \{c, b\}$ and the current mode dependent capture set shrinks to $\hat{C}_{\hat{q}_2}$. Plot (c) shows the time at which the mode estimate becomes $\hat{q} = \{b\}$, so that the current mode dependent capture set further shrinks to $\hat{C}_{\hat{q}_3}$. Plot (d) shows when the continuous state hits the boundary of $\hat{C}_{\hat{q}_3}$ and thus control is applied. Plot (e) shows the vehicles passing the intersection.


[5] J. Aubin, J. Lygeros, M. Quincampoix, S. Sastry, and N. Seube. Impulse differential inclusions: A viability approach to hybrid systems. *IEEE Transactions on Automatic Control*, 47:2–20, 2002.

[6] R. J. Aumann and M. Maschler. *Repeated Games with Incomplete Information*. MIT Press, 1995.

[7] M. Baglietto, G. Battistelli, and L. Scardovi. Active mode observability of switching linear systems. *Automatica*, 43:1442–1449, 2007.

[8] A. Balluchi, L. Benvenuti, M. D. Di Benedetto, and A. Sangiovanni-Vincentelli. Design of observers for hybrid systems. In *Hybrid Systems: Computation and Control*, Lecture Notes in Computer Science vol. 2289, C. J. Tomlin and M. R. Greensreet (Eds.), Springer Verlag, pages 76–89, 2002.

[9] L. Blackmore, S. Rajamanoharan, and B. C. Williams. Active estimation for switching linear dynamic systems. In *Conf. on Decision and Control*, pages 137–144, 2006.

[10] F. H. Clarke. *Optimization and Nonsmooth Analysis*. John Wiley, New York, 1983.

[11] R. D'Andrea, R. M. Murray, J. A. Adams, A. T. Hayes, M. Campbell, and A. Chaudry. The RoboFlag Game. In *American Control Conference*, pages 661–666, 2003.

[12] B. A. Davey and H. A. Priesteley. *Introduction to Lattices and Order*. Cambridge University Press, 2002.

[13] D. Del Vecchio. A partial order approach to discrete dynamic feedback in a class of hybrid systems. In *Hybrid Systems: Computation and Control*, Lecture Notes in Computer Science, vol. 4416, A. Bemporad, A. Bicchi, and G. Buttazzo (Eds.), Springer Verlag, pages 159–173, Pisa, Italy, 2007.

[14] D. Del Vecchio. Cascade estimators for systems on a partial order. *Systems and Control Letters*, 57(10):842–850, 2008.

[15] D. Del Vecchio. Observer-based control of block triangular discrete time hybrid automata on a partial order. *International Journal of Robust and Nonlinear Control*, 19(14):1581–1602, 2009.

[16] D. Del Vecchio and E. Klavins. Observation of guarded command programs. In *Conf. on Decision and Control*, pages 3353–3359, 2003.

[17] 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*, pages 3638–3643, 2009.

[18] D. Del Vecchio, R. M. Murray, and E. Klavins. Discrete state estimators for systems on a lattice. *Automatica*, 42(2):271–285, 2006.

[19] D. Del Vecchio, R. M. Murray, and P. Perona. Primitives for human motion: A dynamical approach. In *IFAC World Congress*, Barcelona, 2002.

[20] D. Del Vecchio, R. M. Murray, and P. Perona. Decomposition of human motion into dynamics-based primitives with application to drawing tasks. *Automatica*, 39(12):2085–2098, 2003.

[21] Y. Demiris. Prediction of intent in robotics and multi-agent systems. *Cognitive Processes*, 8:151–158, 2007.

[22] V. Desaraju, M H. C. Ro, E. Tay Yang, S. Roth, and D. Del Vecchio. Partial order techniques for vehicle collision avoidance: Application to an autonomous roundabout test-bed. In *Proc. of International Conference on Robotics and Automation*, pages 82–87, 2009.

[23] E. A. Domlan, J. Ragot, and D. Maquin. Active mode estimation for switching systems. In *acc*, 2007.

[24] J. Duperret, M. Hafner, and D. Del Vecchio. Formal design of a provably safe robotic roundabout system. In *Proc. of International Conference on Intelligent Robots and Systems*, pages 2006–2011, 2010.

[25] O. Maler E. Asarin and A. Pnueli. Symbolic controller synthesis for discrete and timed systems. In *Hybrid Systems II,* Lecture Notes in Computer Science, vol. 999, P. Antsaklis, W. Kohn, A. Nerode, and S. Sastry (Eds.), Springer Verlag, pages 1–20, 1995.

[26] Y. Gao, J. Lygeros, and M. Quincampoix. The reachability problem for

uncertain hybrid systems revisited: A viability theory perspective. In *Lecture Notes in Computer Science LNCS, no. 3927*, pages 242–256, 2006.
[27] A. Gilpin and T. Sandholm. Solving two-person zero-sum repeated games of incomplete information. In *Proc. of 7th Int. Conf. on Autonomous Agents and Multiagent Systems*, 2008.
[28] M. Hafner and D. Del Vecchio. Computation of safety control for uncertain piecewise continuous systems on a partial order. In *Conference on Decision and Control*, pages 1671–1677, 2009.
[29] T. A. Henzinger. The theory of hybrid automata. In *Proceedings of the 11th Annual Symposium on Logic in Computer Science*, pages 278–292. IEEE press, 1996.
[30] T. A. Henzinger, P. H. Ho, and H. Wong-Toi. A user guide to HyTech. In *TACAS 95: Tools and Algorithms for the construction and analysis of systems*, Lecture Notes in Computer Science, vol. 1019, E. Brinksma, W. Cleaveland, K. Larsen, T. Margaria, and B. Steffen (Eds.), Springer-Verlag, pages 41–71, 1995.
[31] T. A. Henzinger, B. Horowitz, R. Majumdar, and H. Wong-Toi. Beyond HyTech: Hybrid systems analysis using interval numerical methods. In *Hybrid Systems: Computation and Control*, Lecture Notes in Computer Science, vol. 1790, B. Krogh and N. Lynch (Eds.), Springer Verlag, pages 130–144, 2000.
[32] R. J. Hill. Electric railway traction tutorial, part 1: Electric traction and dc traction motor drives. *Power Engineering Journal*, (1):47–56, 1994.
[33] J. Hu, M. Prandini, and S. Sastry. Aircraft conflict prediction in the presence of a spatially correlated wind field. *IEEE Transactions on Intelligent Transportation Systems*, (3):326–340, 2005.
[34] S. Istrail. Generalization of the Ginsburg-Rice Schützenberger fixed-point theorem for context-sensitive and recursive-enumerable languages. *Theoretical Computer Science*, 18:333–341, 1982.
[35] J.-H. Kim, Y.-W. Kim, and D.-H. Hwang. Modeling of human driving behavior based on piecewise linear model. *AUTOMATIKA*, 46:29–37, 2005.
[36] H. W. Kuhn. Extensive games and the problem of information. In H. W. Kuhn and A. W. Tucker, editors, *Contributions to the Theory of Games*. Princeton University Press, pages 196–216, 1953.
[37] A. B. Kurzhanski and P. Varaiya. Ellipsoidal techniques for hybrid dynamics: the reachability problem. In *New Directions and Applications in Control Theory*, Lecture Notes in Control and Information Sciences, vol 321, W.P. Dayawansa, A. Lindquist, and Y. Zhou (Eds.), pages 193–205, 2005.
[38] S. M. LaValle. *Planning Algorithms*. Cambridge University Press, 1st edition, 2006.
[39] J. Lygeros, C. J. Tomlin, and S. Sastry. Controllers for reachability specifications for hybrid systems. *Automatica*, 35(3):349–370, 1999.
[40] M. Oishi, I. Mitchell, A. Bayen, and C. Tomlin. Invariancepreserving abstractions of hybrid systems: Application to user interface design. *IEEE Transactions on Control Systems Technology*, 16(2):229–244, 2008.
[41] J. Pachl. *Railway operation and control*. VTD Rail Publishing, 2002.
[42] R. Raffard, S. Waslander, A. Bayen, and C. Tomlin. A cooperative distributed approach to multi-agent eulerian network control: Application to air traffic management. In *AIAA Guidance, Navigation, and Control Conference and Exhibit*, 2005.
[43] J. H. Reif. The complexity of two-player games of incomplete information. *Journal of Computer System Sciences*, 29(2):274–301, 1984.
[44] E. De Santis, M. D. Di Benedetto, and L. Berardi. Computation of maximal safe sets for switching systems. *IEEE Trans. Automatic Control*, 49(2):184–195, 2004.
[45] C.-E. Seah and I. Hwang. Terminal-area aircraft tracking by hybrid estimation. *AIAA Journal of Guidance, Control and Dynamics*, 32(3):836–849, 2009.
[46] O. Shakernia, G. J. Pappas, and S. Sastry. Decidable controller synthesis for classes of linear systems. In *Hybrid Systems: Computation and Control*, Lecture Notes in Computer Science, vol. 1790, Springer Verlag, 2000.
[47] O. Shakernia, G. J. Pappas, and S. Sastry. Semidecidable controller synthesis for classes of linear hybrid systems. In *Proc. of Conf. on Decision and Control*, 2000.
[48] O. Shakernia, G. J. Pappas, and S. Sastry. Semi-decidable synthesis for triangular hybrid systems. In *Hybrid Systems: Computation and Control*, Lecture Notes in Computer Science, vol. 2034, M. D. Di Benedetto and A. Sangiovanni-Vincentelli (Eds.), Springer Verlag, 2001.
[49] C. J. Tomlin, J. Lygeros, and S. Sastry. A game theoretic approach to controller design for hybrid systems. *Proceedings of the IEEE*, 88(7):949–970, 2000.
[50] C. J. Tomlin, I. Mitchell, A. M. Bayen, and M. Oishi. Computational techniques for the verification of hybrid systems. *Proceedings of the IEEE*, 91(7):986–1001, 2003.
[51] R. Verma and D. Del Vecchio. Continuous control of hybrid automata with imperfect mode information assuming separation between state estimation and control. In *Conference on Decision and Control*, pages 3175–3181, 2009.
[52] R. Verma, D. Del Vecchio, and H. Fathy. Development of a scaled vehicle with longitudinal dynamics of a HMMWV for an ITS testbed. *IEEE/ASME Transactions on Mechatronics*, 13:46–57, 2008.
[53] R. Vidal, A. Chiuso, and S. Soatto. Observability and identifiability of jump linear systems. In *Conf. on Decision and Control*, pages 3614 – 3619, 2002.
[54] M. De Wulf, L. Doyen, and J.-F. Raskin. A lattice theory for solving games of imperfect information. *Hybrid Systems: Computation and Control*, Lecture Notes in Computer Science, vol. 3927, J. Hespanha and A. Tiwari (Eds.), Springer-Verlag, pages 153–168, 2006.

## Appendix

(*Proof of Proposition 5*) Property (i) follows directly from the definition of Pre, in which $t = 0$. To show property (ii), let $x_o \in \text{Pre}(\hat{q}, \text{Pre}(\hat{q}, S))$. By the definition of Pre, we have that for all $\hat{\pi}$ there is $\mathbf{d}_1$ and a time $t_1$ such that some $\phi^{\hat{\pi}}_{\hat{x}}(t_1, (x_o, \hat{q}), \mathbf{d}_1, \epsilon) \in \text{Pre}(\hat{q}, S)$. Define $x'_o := \phi^{\hat{\pi}}_{\hat{x}}(t_1, (x_o, \hat{q}), \mathbf{d}_1, \epsilon)$. Since $x'_o \in \text{Pre}(\hat{q}, S)$, we have by the definition of Pre that for all $\hat{\pi}$ there is $\mathbf{d}_2$ and $t_2 > 0$ such that some $\phi^{\hat{\pi}}_{\hat{x}}(t_2, (x'_o, \hat{q}), \mathbf{d}_2, \epsilon) \in S$. Let $t = t_1 + t_2$ and define $\mathbf{d}$ such that $d(\tau) = d_1(\tau)$ for $\tau < t_1$ and $d(\tau) = d_2(\tau - t_1)$ for $\tau \geq t_1$. Then, we have that $\phi^{\hat{\pi}}_{\hat{x}}(t_2, (x'_o, \hat{q}), \mathbf{d}_2, \epsilon) = \phi^{\hat{\pi}}_{\hat{x}}(t, (x_o, \hat{q}), \mathbf{d}, \epsilon)$. Since for all $\hat{\pi}$ there is $\mathbf{d}$ such that $\phi^{\hat{\pi}}_{\hat{x}}(t, (x_o, \hat{q}), \mathbf{d}, \epsilon) \in S$, we also have that $x_o \in \text{Pre}(\hat{q}, S)$. Property (iii) is an immediate consequence of the definition of Pre. Property (iv) follows from the fact that if for all $\pi$ a trajectory $\hat{x}(t)$ such that $\dot{\hat{x}}(t) \in \hat{f}(\hat{x}(t), \hat{q}_1, \hat{\pi}(\hat{q}_1, \hat{x}(t)), d(t))$ enters $S$, then also a trajectory such that $\dot{\hat{x}}(t) \in \hat{f}(\hat{x}(t), \hat{q}_2, \hat{\pi}(\hat{q}_2, \hat{x}(t)), d(t))$ with $\hat{q}_2 \supseteq \hat{q}_1$ enters $S$. Property (v) follows from the fact that (a) $\text{Pre}(\hat{q}_1, \text{Pre}(\hat{q}_2, S)) \supseteq \text{Pre}(\hat{q}_1, S)$ by property (i) and (iii); and from the fact that (b) $\text{Pre}(\hat{q}_1, \text{Pre}(\hat{q}_2, S)) \subseteq \text{Pre}(\hat{q}_1, \text{Pre}(\hat{q}_1, S))$ by properties (iv) and (iii); and from the fact that (c) $\text{Pre}(\hat{q}_1, \text{Pre}(\hat{q}_1, S)) = \text{Pre}(\hat{q}_1, S)$ by property (ii). Finally, we show property (vi). By property (i), we have that $S_1 \cup \ldots \cup S_n \subseteq \text{Pre}(\hat{q}_1, S_1) \cup \ldots \cup \text{Pre}(\hat{q}_n, S_n)$. Thus, applying property (iii), we have that $\text{Pre}(\hat{q}_0, S_0 \cup S_1 \cup \ldots \cup S_n) \subseteq \text{Pre}(\hat{q}_0, S_0 \cup \text{Pre}(\hat{q}_1, S_1) \cup \ldots \cup \text{Pre}(\hat{q}_n, S_n))$. Also, applying property (iv) and property (iii), we have that $\text{Pre}(\hat{q}_0, S_0 \cup \text{Pre}(\hat{q}_0, S_1) \cup \ldots \cup \text{Pre}(\hat{q}_0, S_n)) \supseteq \text{Pre}(\hat{q}_0, S_0 \cup \text{Pre}(\hat{q}_1, S_1) \cup \ldots \cup \text{Pre}(\hat{q}_n, S_n))$. However, $\text{Pre}(\hat{q}_0, S_0 \cup \text{Pre}(\hat{q}_0, S_1) \cup \ldots \cup \text{Pre}(\hat{q}_0, S_n)) = \text{Pre}(\hat{q}_0, S_0 \cup S_1 \cup \ldots \cup S_n)$ by the definition of Pre (using the same strategy as used for proving property (ii)). Hence $\text{Pre}(\hat{q}_0, S_0 \cup \text{Pre}(\hat{q}_1, S_1) \cup \ldots \cup \text{Pre}(\hat{q}_n, S_n)) = \text{Pre}(\hat{q}_0, S_0 \cup S_1 \cup \ldots \cup S_n)$ for $\hat{q}_i \subseteq \hat{q}_0$ for all $i$.

(*Proof of Proposition 6*) See Proposition 4 of [51].

(*Proof of Proposition 7*) Let $(\hat{q}_i, x_i) \in \hat{W}$. Then, by the definition of $\hat{C}$ we have that there is a feedback map $\hat{\pi}_i$ such that <u>all</u> $\hat{\phi}^{\hat{\pi}_i}(t, (\hat{q}_i, x_i), \mathbf{d}, \mathbf{y}) \in \hat{W}$ for all $\mathbf{d}, \mathbf{y}$ and $t \geq 0$. Define the set $W_i := \bigcup_{\mathbf{d},\mathbf{y},t\geq 0} \hat{\phi}^{\hat{\pi}_i}(t, (\hat{q}_i, x_i), \mathbf{d}, \mathbf{y}) \subseteq \hat{W}$, which is controlled invariant with feedback map $\hat{\pi}_i$. Since the class of controlled invariant sets contained in $\hat{W}$ is closed under union (see the proof of Proposition 3 of [39]), there is a feedback map $\hat{\pi}$ that makes the union $\bigcup_{\{i \mid (\hat{q}_i, x_i) \in \hat{W}\}} \bar{W}_i \subseteq \hat{W}$ controlled invariant. Therefore $\hat{W}$ is also controlled invariant. It is the maximal controlled invariant set contained in $(\hat{Q} \times X)/(\hat{Q} \times Bad)$ because if $(\hat{q}, x) \notin \hat{W}$ then $(\hat{q}, x) \in \hat{C}$, which implies that for all maps $\hat{\pi}$ some flow $\hat{\phi}^{\hat{\pi}}(t, (\hat{q}, x), \mathbf{d}, \mathbf{y})$ enters $\hat{Q} \times Bad$ for some $\mathbf{d}, \mathbf{y}$, and $t \geq 0$.

(*Proof of Proposition 8*) See Proposition 5 of [51].

(*Proof of Proposition 9*) We construct from $F$ an impulse differential inclusion whose $x$ trajectories are the same as the ones of the system $\dot{x} \in F(x)$ and then apply Theorem 3 from [5] to the resulting impulse differential inclusion to conclude invariance of $S$. An impulse differential inclusion is a tuple $\bar{H} = (\bar{X}, \bar{F}, \bar{R}, \bar{J})$, in which $\bar{X}$ is a finite dimensional space, $\bar{F} : \bar{X} \rightarrow 2^{\bar{X}}$ is a set valued map regarded as a differential inclusion $\dot{\bar{x}} \in \bar{F}(\bar{x})$, $\bar{R} : \bar{X} \rightarrow 2^{\bar{X}}$ is a reset map, and $\bar{J} \subset \bar{X}$ is a forced discrete transition set. Since $F$ is piecewise Lipschitz continuous on $X$, there are sets $X_i \subset X$ for $i = 1, ..., N$ that cover $X$ on which $F$ is Lipschitz. Define for each $i \in \{1, ..., N\}$ the maps $F_i : X \rightarrow 2^X$ such that $F_i(x) = F(x)$ for all $x \in X_i$ and for $x \notin X_i$ the map $F_i(x)$ is extended so that it is Lipschitz continuous on $X$. Then, $F_i : X \rightarrow 2^X$ is Marchaud and Lipschitz continuous. Let $z_i \in \{1, 0\}$ for $i \in \{1, ..., N\}$ and define $\bar{X} := X \times \{1, 0\}^N$. Let $z = (z_1, ..., z_N)$ and define the new map $\bar{F} : \bar{X} \rightarrow 2^{\bar{X}}$ as $\bar{F}(x, z) := \begin{pmatrix} z_1 F_1(x) + ... + z_N F_N(x) \\ 0_{N\times 1} \end{pmatrix}$, $\forall (x, z) \in \bar{X}$. Define a reset map $\bar{R} : \bar{X} \rightarrow \bar{X}$ by $\bar{R}(x, z) = (x, e_i)$, if $x \in X_i$. Define the set of forced transitions $\bar{J} \subset \bar{X}$ as $\bar{J} = \{(x, z) \in \bar{X} \mid x \in X_i \text{ and } z \neq e_i\}$. By construction, the $x$ trajectories of $\bar{H}$ starting from initial conditions $z = e_i$ and $x \in X_i$ for all $i$ coincide with the trajectories of $\dot{x} \in F(x)$ starting with the same $x \in X_i$.

Let $E := \{e_1, ..., e_N\} \subset \{1, 0\}^N$ and define the set $\bar{S} \subset \bar{X}$ as $\bar{S} = S \times E$. This is a closed set. Theorem 3 from [5] states that if $\bar{F}$ is Marchaud and Lipschitz and $\bar{J}$ is closed, then $\bar{S}$ is invariant under $\bar{H}$ if and only if (1) $\bar{R}(\bar{S}) \subseteq \bar{S}$ and (2) $\forall (x, z) \in \bar{S} \backslash \bar{J}$ we have $\bar{F}(x, z) \subseteq T_{\bar{S}}(x, z)$. Notice that $\bar{R}(\bar{S}) \subseteq \bar{S}$ by the way $\bar{R}$ is constructed. Let then $F(x) \subseteq T_S(x)$ for all $x \in S$. We show that this implies that also $\bar{F}(x, z) \subseteq T_{\bar{S}}(x, z)$ for all $(x, z) \in \bar{S} \backslash \bar{J}$. By the way $\bar{F}$, $\bar{S}$, and $\bar{J}$ have been defined, for all $(x, z) \in \bar{S} \backslash \bar{J}$ we have that $\bar{F}(x, z) = (F_i(x), 0_{N\times 1})$ with $x \in X_i$. Since also $x \in S$, we have $F_i(x) \subseteq T_S(x)$ because $x \in X_i$ and $F_i(x) = F(x)$ for $x \in X_i$. Since $z \in E$, we have that $T_E(z) = 0_{N\times 1}$. As a consequence, $\bar{F}(x, z) \subseteq T_S(x) \times T_E(z)$. Given that $T_{S\times E}(x, z) = T_S(x) \times T_E(z)$ [10], it follows that $\bar{F}(x, z) \subseteq T_{S\times E}(x, z)$ for all $(x, z) \in \bar{S} \backslash \bar{J}$. By Theorem 3 in [5], set $\bar{S}$ is invariant under $\bar{H}$, which implies that set $S$ is invariant by $F$ as the $x$ trajectories of the first system starting in $(x_o, z_o) \in \bar{S}$ are the same as the $x$ trajectories of the second system starting at $x_o \in S$.

Conversely, if $F(x) \nsubseteq T_S(x)$ for some $x \in S$, then for some $i$ such that $x \in X_i$ we have that $F_i(x) \nsubseteq T_S(x)$. This in turn implies that for $(x, z) \in \bar{S} \backslash \bar{J}$ (that is, for $z = e_i$) we have $\bar{F}(x, z) \nsubseteq T_{\bar{S}}(x, z)$. By Theorem 3 in [5] set $\bar{S}$ is thus not invariant under $\bar{H}$. This implies that there is a time $t$ at which either $x(t) \notin S$ or $z(t) \notin E$. However, if $z(0) \in E$ we must have that $z(t) \in E$ for all $t$ as $z$ can change its value only through $\bar{R}$, which always maps $z$ back in $E$. Therefore, there must be a time $t$ such that $x(t) \notin S$ for system $\bar{H}$. Since the $x$ trajectories of $\bar{H}$ starting at $(x_o, z_o) \in \bar{S}$ are the same as those of $\dot{x} \in F(x)$ starting at $x_o \in S$, it must be that $x(t) \notin S$ also for system $\dot{x} \in F(x)$, implying that $S$ cannot be invariant for $F$.

**Definition 24.** (Type of a kernel set) We say that a kernel set $ker_1 \subseteq \hat{Q}$ *transits* to a kernel set $ker_2 \subseteq \hat{Q}$ if there is $\hat{q}_1 \in ker_1$, $\hat{q}_2 \in ker_2$, and $y \in Y$ such that $\hat{q}_2 = \hat{R}(\hat{q}_1, y)$. A kernel set is *type*(1) if it does not transit to any other kernel set. A kernel set is *type*($n$) if it transits to *type*($n-1$) kernel sets and only to *type*($n-1$), . . . , *type*(1) kernel sets.

**Proposition 21.** *Let $\hat{q}_i$ for $i \in \{1, ..., M\}$ be in a type(1) kernel set. Then, Algorithm 1 is such that there is a $K^* \geq 0$ for which $S_i^{K^*} = S_i^{K^*+1}$.*

(*Proof*) See Theorem 2 of [51].

(*Proof of Theorem 3*) See Theorem 2 of [51].

## Acknowledgment

This work was supported by NSF CAREER Award Number CNS-0642719.

**Rajeev Verma** Rajeev Verma received the Bachelor's degree in mechanical engineering in 2003 from National Institute of Technology, Warangal, India and Master's degree in electrical engineering : systems in 2008 from University of Michigan, Ann Arbor. He is currently a PhD candidate at University of Michigan, Ann Arbor. From 2003 to 2005, he was with Ashok Leyland Ltd., India. Since January 2005, he has been a Graduate student at the University of Michigan, Ann Arbor. His research interests include hybrid systems and system modeling and control.

**Domitilla Del Vecchio** Domitilla Del Vecchio received the Ph. D. degree in Control and Dynamical Systems from the California Institute of Technology, Pasadena, and the Laurea degree in Electrical Engineering from the University of Rome at Tor Vergata in 2005 and 1999, respectively. From 2006 to 2010, she was an Assistant Professor in the Department of Electrical Engineering and Computer Science and in the Center for Computational Medicine and Bioinformatics at the University of Michigan, Ann Arbor. In 2010, she joined the Department of Mechanical Engineering and the Laboratory for Information and Decision Systems (LIDS) at the Massachusetts Institute of Technology (MIT), where she is currently the W. M. Keck Career Development Assistant Professor in Biomedical Engineering. She is a recipient of the Donald P. Eckman Award from the American Automatic Control Council (2010), the NSF Career Award (2007), the Crosby Award, University of Michigan (2007), the American Control Conference Best Student Paper Award (2004), and the Bank of Italy Fellowship (2000). Her research interests include analysis and control of nonlinear and hybrid dynamical systems and the analysis and design of biomolecular networks.