Joint 48th IEEE Conference on Decision and Control and
28th Chinese Control Conference
Shanghai, P.R. China, December 16-18, 2009

Continuous Control of Hybrid Automata with Imperfect Mode Information Assuming Separation between State Estimation and Control

Rajeev Verma and Domitilla Del Vecchio

Abstract— **The safety control problem for hybrid automata with imperfect mode information and continuous control is addressed. When the controller does not have access to the mode of the system, available static feedback techniques cannot be applied. We propose a dynamic feedback strategy in which a mode estimator constructs the set of possible current system modes. A control map is designed that on the basis of the current mode estimates returns the set of all possible safe control inputs. This dynamic feedback map implicitly assumes separation between state estimation and control. Termination conditions are provided. The proposed control technique is applied to a semi-autonomous cooperative active safety system.**

I. I

In this paper, we address the safety control problem for hybrid automata in which the mode is not known and only continuous control inputs are available. This problem naturally arises in a variety of applications, including intent-based conflict detection and avoidance for aircrafts [15], robotic games with imperfect information [7], and semi-autonomous cooperative active safety systems to prevent vehicle collisions [17]. In these systems, the presence of human-driven vehicles that do not communicate or cooperate introduces a large degree of uncertainty. An approach in which this uncertainty is treated as an adversary in a game theoretic fashion would lead to solutions that are too conservative to be realistically considered for collision warning or active control [14, 16]. A promising approach is instead to construct simple decision models for the non-communicating agents in the form of a hybrid automaton. This hybrid automaton has unknown modes as the decisions of the non-communicating agents are unknown and thus it leads to a control problem with imperfect mode information.

While there is a wealth of literature studying safety control for hybrid automata assuming perfect state information [1, 12, 14, 16], the same problem when the state is not fully measured has been rarely addressed. Some works on this problem have recently appeared [6, 19]. In particular, [19] proposes a solution to the control problem for rectangular hybrid automata that admit a finite-state abstraction. Dynamic control of block triangular order preserving hybrid automata under imperfect continuous state information is considered in [6] for discrete time systems and extended in [8] for continuous time systems. However, mode uncertainty is not considered.

In this paper, we consider hybrid automata subject to continuous and discrete disturbance inputs and with only continuous control inputs. The mode of the system is unknown while the continuous state is measured. The problem considered is to design a dynamic feedback map that on the basis of the available sensory information guarantees that the system state is kept outside a bad set of states. Our approach relies on transforming this problem of imperfect information to an equivalent problem with perfect information. This equivalent problem is obtained under suitable observability assumptions on the mode of the system. Within this problem a new system that updates the set of all possible current system states, i.e., the estimator, is constructed and controlled for safety. The mode estimator updates the set of all possible current system modes. A feedback map is then designed that for each set of possible current modes returns the set of possible continuous control inputs that maintain the system state outside a bad set. An iterative procedure for computing this map is provided and it is shown to terminate under conditions that can be directly checked on the mode estimator. By construction, the obtained dynamic feedback map is the least restrictive for the chosen discrete state estimator.

This paper is organized as follows. The model and problem are introduced in Section II, the solution is proposed in Section III. In Section IV, we present an application example.

II. S M P D

We consider hybrid automaton $H = (Q, X, \mathcal{U}, \Delta, \Sigma, R, f)$, in which Q is a finite set of modes, X is a vector space, $\mathcal{U}$ is a continuous set of control inputs, Δ is a continuous set of disturbances, Σ is a finite set of disturbance events, $R : Q \times \Sigma \to Q$ is the discrete state update map, $f : X \times Q \times \mathcal{U} \times \Delta \to X$ is the vector field, which is allowed to be discontinuous in the first argument to model autonomous discrete transitions. We represent such a system by the equations

$$\begin{aligned} q(t^+) &= R(q(t), \sigma(t)), \quad \sigma(t) \in \Sigma \\ \dot{x}(t) &= f(x(t), q(t), u(t), d(t)), \quad d(t) \in \Delta, \end{aligned} \tag{1}$$

in which $q(t^+)$ denotes the value of the mode immediately after a transition taking place at time t. We assume there is

The authors are with the Systems Laboratory, University of Michigan, Ann Arbor. Supported in part by NSF CAREER Award Number CNS-0642719. E-mail: rajverma@umich.edu

no continuous state reset, i.e. $x(t^+) = x(t)$. In this system, x is measured and available for control, while q is not. Given initial conditions $(x_0, q_0) \in X \times Q$ and piecewise continuous input signals $\tilde{u}_t : [0,t) \to \mathcal{U}$, $\tilde{d}_t : [0,t) \to \Delta$, $\tilde{\sigma}_t : [0,t) \to \Sigma$, the corresponding trajectory (or flow) of H is denoted $\phi(t, (x_0, q_0), \tilde{u}_t, \tilde{d}_t, \tilde{\sigma}_t)$ with $\phi_x(t, (x_0, q_0), \tilde{u}_t, \tilde{d}_t, \tilde{\sigma}_t)$ being its continuous part and $\phi_q(t, q_0, \tilde{\sigma}_t)$ being its discrete part. When the initial conditions and inputs are clear from the context, we will denote such trajectories by $x(t)$ and $q(t)$.

Let 2^Q denote the set of all subsets of Q. The information that we have about the system state at time t comprises information on the initial state $\eta_0 := (x_0, \hat{q}_0)$ with $\hat{q}_0 \in 2^Q$, the continuous control input signal $\tilde{u}_t$, and the continuous state signal $\tilde{x}_t : [0,t] \to X$. We call this information the *information state* of the system, and denote it by $\eta_t = (\eta_0, \tilde{u}_t, \tilde{x}_t)$. We denote the set of all observation histories up to time t as $\tilde{X}_t$ and the set of all control input histories up to time t as $\tilde{\mathcal{U}}_t$. We denote the *information space up to time t* as $\mathcal{I}_t = X \times 2^Q \times \tilde{\mathcal{U}}_t \times \tilde{X}_t$ and the *information space* as $\mathcal{I} := \bigcup_{t \geq 0} \mathcal{I}_t$ [13]. A *dynamic feedback* map is a map with memory $\pi : \mathcal{I} \to \mathcal{U}$ that on the basis of the current information state establishes control inputs. Given H and the map π, the closed loop hybrid automaton is denoted $H^\pi := (H, \pi)$ and is represented by (1), in which $u(t) = \pi(\eta_t)$. Its state trajectories are denoted with a π superscript. Let $B \subseteq X$ be an unsafe set of states, we seek to solve the following problem.

Problem 1: Compute the set C of all initial information states η_0 for which no dynamic feedback map $\pi : \mathcal{I} \to \mathcal{U}$ exists that guarantees $\phi_x^\pi(t, (x_0, q_0), \tilde{d}_t, \tilde{\sigma}_t) \notin B$, for all $t \geq 0$, $\tilde{d}_t$, $\tilde{\sigma}_t$, and $(x_0, q_0) \in \eta_0$.

The set C is referred to as the capture set for system H. Once set C has been determined, the set of all dynamic feedback maps that keep the information state outside it is computed. In order to simplify the information state representation, which consists of system histories, we consider the *non-deterministic information state*. This represents the set of all possible current system states compatible with the history of the system and it is denoted $(\hat{x}_t(\eta_t), \hat{q}_t(\eta_t))$, in which $\hat{x}_t(\eta_t) = x(t)$. Thus, we have that $C = \{\eta_0 \in X \times 2^Q \mid \forall\ \pi\ \exists\ t,\ \tilde{x}_t,\ \text{s. t. } \hat{x}_t^\pi(\eta_t) \in B\}$. This set can also be expressed as $C = \bigcup_{\hat{q} \in 2^Q} \left(C_{\hat{q}}, \hat{q}\right)$, in which $C_{\hat{q}} = \{x \in X \mid \forall\ \pi\ \exists\ t,\ \tilde{x}_t,\ \text{s. t. } \hat{x}_t^\pi(\eta_t) \in B \text{ with } \eta_0 = (x, \hat{q})\}$. The set $C_{\hat{q}}$ represents the set of all continuous initial states x that are mapped to B for some nature action independently of the controller when the flow starts in a mode contained in $\hat{q}$. Problem 1 is thus solved by computing all such sets $C_{\hat{q}}$ for all $\hat{q} \in 2^Q$.

Note that the controller uses *all* the information it gathers from the information state in order to make choices against nature. For example, if $\hat{q} = \{q_1, q_2\}$ and the information state cannot distinguish between the two modes, it means that the disturbance action may be playing in a range so to generate an $\tilde{x}_t$ trajectory that is compatible both under q_1 and under q_2. This fact implicitly restricts the set of disturbance actions that the controller should counter act. Also, note that if at time zero the disturbance action $d(0)$ is such that the two modes are distinguishable, the information state can immediately switch from the initial value $\hat{q}_t(\eta_0) = \{q_1, q_2\}$ to $\hat{q}_t(\eta_{0^+}) = \{q_1\}$. It is thus useful to introduce the following mode observability notion for system H.

Definition 1: System H is said *immediate mode observable* provided for all $q_i \in \hat{q}_0$, there is a nature action $d(0)$ such that (i) $\hat{q}(\eta_{0^+}) = q_i$; (ii) for all $t > 0$, we have that $\hat{q}(\eta_t) = q_i$ implies $\tilde{x}_t$ is *any* signal that can be generated by H when $q(t) = q_i$.

Item (ii) specifies that once the non-deterministic information state has converged to q_i, any continuous state trajectory compatible with q_i can be generated. This last requirement implies that while $\hat{q}(\eta_t) = q_i$, the disturbance choices can span in their entire range Δ.

III. P S

In order to solve Problem 1, we introduce update laws for the non-deterministic information state. By introducing these update laws we translate an imperfect state information problem to a perfect state information one, in which the non-deterministic information state is the new (measured) state. Such update laws should be such that at any time t the set of possible current modes contains *only* modes that are compatible with the entire history of the system up to time t. In general, this requirement cannot be satisfied when a separation structure is assumed between state estimation and control. However, a separation structure enables computationally tractable solutions and the use of mode estimators that are available in the literature [4, 9]. In what follows, we thus propose a separation structure between mode estimation and control.

Let the current estimate of the discrete non-deterministic information state be denoted (with abuse of notation) by $\hat{q}(t) \in 2^Q$. Let $T > 0$ and $\mathcal{F}(\tilde{x}_{[t-T,t]})$ be a filtering function that returns a set of possible current modes compatible with the measured continuous signal between times $t - T$ and t (see [4, 9], for example). Let all such possible sets of modes be denoted by $Y_1, ..., Y_m$. Define the new function $\hat{R}(\hat{q}, Y) := \bigcup_{t \geq 0} \bigcup_{\tilde{\sigma}_t} \phi_q(t, \hat{q}, \tilde{\sigma}_t) \cap Y$, in which $\bigcup_{t \geq 0} \bigcup_{\tilde{\sigma}_t} \phi_q(t, \hat{q}, \tilde{\sigma}_t)$ is the reachable set of modes from $\hat{q}$ under all possible disturbance sequences, $Y \in \mathcal{Y} := \{\epsilon, Y_1, ..., Y_m\}$, and ϵ is defined such that $\hat{R}(\hat{q}, \epsilon) := \hat{q}$. We consider a mode estimator of the form $\hat{q}(t^+) = \hat{R}(\hat{q}(t), Y(t))$, $Y(t) \in \mathcal{Y}$, in which $Y(t) = \mathcal{F}(\tilde{x}_{[t-T,t]})$. Switches are triggered by a change in the value of $Y(t)$, which are determined by nature (the measured signal $\tilde{x}_t$). This estimator is by construction correct, meaning that $q(t) \in \hat{q}(t)$ for all t. The estimate of the non-deterministic discrete information state $\hat{q}(t)$ restricts the set of possible dynamics of the continuous state $\hat{x}(t) \in X$ to $\dot{\hat{x}}(t) = f(\hat{x}(t), \alpha(t), u(t), d(t))$ where now $\alpha(t)$ is restricted to lie

in $\hat{q}(t)$ at all time t. As a consequence, we have

$$\hat{q}(t^+) = \hat{R}(\hat{q}(t), Y(t)),\ Y(t) \in \mathcal{Y}$$
$$\dot{\hat{x}}(t) = f(\hat{x}(t), \alpha(t), u(t), d(t)),\ d(t) \in \Delta,\ \alpha(t) \in \hat{q}(t), \quad (2)$$

with initial conditions $(\hat{x}(0), \hat{q}(0)) = \eta_0$. The state of such a system lies in $X \times \hat{Q}$ with $\hat{Q} \subseteq 2^Q$, and it is exactly known because $\hat{q}(t)$ is known by construction and $\hat{x}(t) = x(t)$. We will refer to this hybrid automaton as $\hat{H} = (\hat{Q}, X, \mathcal{U}, \Delta, \mathcal{Y}, \hat{R}, \hat{f})$, in which $\hat{f}(\hat{x}, \hat{q}, u, d) := \{f(x, \alpha, u, d),\ \alpha \in \hat{q}\}$. We denote a trajectory of $\hat{H}$ by $\hat{\phi}(t, \eta_0, \tilde{u}_t, \tilde{d}_t, \tilde{Y}_t)$. Its discrete part will be denoted by $\phi_{\hat{q}}(t, \hat{q}_0, \tilde{Y}_t)$ and its continuous part by $\phi_{\hat{x}}(t, (x_0, \hat{q}_0), \tilde{u}_t, \tilde{d}_t, \tilde{Y}_t)$. We will also denote such trajectories by $\hat{x}(t)$ and $\hat{q}(t)$ when the inputs are clear from the context. By construction, any trajectory of H starting at a state in η_0 is possible for the same control input in $\hat{H}$. Therefore, the set of trajectories of $\hat{H}$ contains the one of H. The other way around is not true unless $(\hat{x}(t), \hat{q}(t))$ is exactly equal to the nondeterministic information state, meaning that η_t cannot restrict further such sets. Nevertheless, we next show that system $\hat{H}$ can be employed for solving Problem 1. When $u = \pi(x, \hat{q})$, we denote the hybrid automaton by $\hat{H}^\pi$ and its trajectories with a superscript π.

Problem 2: Given hybrid automaton $\hat{H}$, determine its capture set, $\hat{C} = \{\eta_0 \in X \times \hat{Q} \mid \forall\ \pi\ \exists\ t,\ \tilde{d}_t,\ \tilde{Y}_t,\ \text{s. t. some } \phi^\pi_{\hat{x}}(t,\ \eta_0, \tilde{d}_t, \tilde{Y}_t) \in B\}$.

Proposition 1: The set $\hat{W} := (X \times \hat{Q})/\hat{C}$ is the *maximal controlled invariant* set of $\hat{H}$ contained in $(X \times \hat{Q})/B \times \hat{Q}$.

Proof: (Sketch.) The proof of this proposition draws from the fact that $\hat{W}$ is closed under union [14]. ■

Since $\hat{C} = \bigcup_{\hat{q} \in \hat{Q}} (\hat{C}_{\hat{q}}, \hat{q})$ in which $\hat{C}_{\hat{q}} = \{x_0 \in X \mid \forall\ \pi\ \exists\ t,\ \tilde{d}_t,\ \tilde{Y}_t \text{ s. t. some } \phi^\pi_{\hat{x}}(t, (x_0, \hat{q}), \tilde{d}_t, \tilde{Y}_t) \in B\}$, we focus on the computation of the sets $\hat{C}_{\hat{q}}$ for all $\hat{q} \in \hat{Q}$.

Definition 2: We say that Problem 2 is *equivalent* to Problem 1 provided $\hat{C}_{\hat{q}} = C_{\hat{q}}$ for all $\hat{q} \in \hat{Q}$.

Define the *uncontrollable predecessor* of a set $S \subseteq X$, given $\hat{q} \in \hat{Q}$, as $\text{Pre}(\hat{q}, S) := \{x \in X \mid \forall \pi,\ \exists\ t,\ \tilde{d}_t,\ \text{s. t. some } \phi^\pi_{\hat{x}}(t, (x_0, \hat{q}), \tilde{d}_t, \epsilon) \in S\}$. The following properties of the Pre operator follow from the fact that it is an order preserving map [5] in both of its arguments, where order is according to set inclusion.

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

Proposition 3: Assume that (i) system H is immediate mode observable; (ii) for all $\hat{q} = \{q_1, ..., q_n\} \in \hat{Q}$, we have that $\text{Pre}(\hat{q}, B) = \text{Pre}(q_1, B) \cup ... \cup \text{Pre}(q_n, B)$; (iii) any trajectory of $\hat{H}$ is such that $\hat{q}(t') \subseteq \hat{q}(t)$ for all $t' \geq t$. Then, Problem 1 and Problem 2 are equivalent.

Proof: It suffices to show that for all $\hat{q} \in \hat{Q}$, we have $\hat{C}_{\hat{q}} \subseteq C_{\hat{q}}$. The fact that $C_{\hat{q}} \subseteq \hat{C}_{\hat{q}}$ derives from the fact that the set of $\hat{x}$ trajectories of $\hat{H}$ contains the set of x trajectories of H. By virtue of assumption (iii) and the definition of the Pre operator, we have that $\hat{C}_{\hat{q}} = \text{Pre}(\hat{q}, B)$, which by assumption (ii) leads to $\hat{C}_{\hat{q}} = \text{Pre}(q_1, B) \cup ... \cup \text{Pre}(q_n, B)$. Take $x \in \hat{C}_{\hat{q}}$. Then, there is $q_i \in \hat{q}$ such that $x \in \text{Pre}(q_i, B)$. By assumption (i), the set $\text{Pre}(q_i, B)$ is contained in $C_{\hat{q}}$ for all $q_i \in \hat{q}$. This in turn implies that $x \in C_{\hat{q}}$. ■

If Problem 1 and Problem 2 are not equivalent, the sets $\hat{C}_{\hat{q}}$ will be overapproximating the sets $C_{\hat{q}}$.

A. Computation of the Capture Set

Proposition 4: The sets $\hat{C}_{\hat{q}_i}$ for all $\hat{q}_i \in \hat{Q}$ satisfy

$$\hat{C}_{\hat{q}_i} = \text{Pre}\left(\hat{q}_i, \bigcup_{\{\hat{q}_j \in \hat{R}(\hat{q}_i, Y), Y \in \mathcal{Y}\}} \hat{C}_{\hat{q}_j} \cup B\right).$$

Proof: Define $D := B \cup_{\{\hat{q}_j \in \hat{R}(\hat{q}_i, \mathcal{Y})\}} \hat{C}_{\hat{q}_j}$ and $A := \text{Pre}(\hat{q}_i, D)$, in which $\{\hat{q}_j \in \hat{R}(\hat{q}_i, \mathcal{Y})\} := \{\hat{q}_j \in \hat{R}(\hat{q}_i, Y), Y \in \mathcal{Y}\}$. Take $x_0 \in A$. This implies, by the definition of Pre that for all π, there exists t and signal $\tilde{d}_t$ such that some $\phi^\pi_{\hat{x}}(t, (x_0, \hat{q}_i), \tilde{d}_t, \epsilon) \in \bigcup_{\{\hat{q}_j \in \hat{R}(\hat{q}_i, \mathcal{Y})\}} \hat{C}_{\hat{q}_j}$. This implies that for all π, there exists time t^1, a signal $\tilde{d}_{t^1}$, and $\hat{q}_j \in \hat{R}(\hat{q}_i, \mathcal{Y})$ such that $\hat{x}(t^1) = \phi^\pi_{\hat{x}}(t^1, (x_0, \hat{q}_i), \tilde{d}_{t^1}, \epsilon) \in \hat{C}_{\hat{q}_j}$. Let nature choose $\tilde{Y}_{t^1}$ such that $\hat{q}(t^1) = \phi^\pi_{\hat{q}}(t^1, \hat{q}_i, \tilde{Y}_{t^1}) = \hat{q}_j$. Then, $(\hat{x}(t^1), \hat{q}(t^1)) \in \hat{C}$. Therefore for all π, there exists t, and signals $\tilde{d}_t, \tilde{Y}_t$, such that some $\phi^\pi_{\hat{x}}(t, (x_0, \hat{q}_i), \tilde{d}_t, \tilde{Y}_t) \in B$. This in turn implies, by the definition of $\hat{C}_{\hat{q}}$, that $x_0 \in \hat{C}_{\hat{q}_i}$.

Now consider $x_0 \in \hat{C}_{\hat{q}_i}$. By definition of $\hat{C}$, we also have that $(x_0, \hat{q}_i) \in \hat{C}$. If $(x_0, \hat{q}_i) \in \hat{C}$, then for all π there exists $\tilde{d}_t,\ \tilde{Y}_t$ such that some $\hat{\phi}(t, (x_0, \hat{q}_i), \tilde{d}_t, \tilde{Y}_t) \in \hat{C}$, for all t. If $\tilde{Y}_t$ makes $\hat{q}_i$ switch to some $\hat{q}_j \in \hat{R}(\hat{q}_i, \mathcal{Y})$ at time t^1, it must be that $\phi^\pi_{\hat{x}}(t^1, (x_0, \hat{q}_i), \tilde{d}_t, \epsilon) \in \hat{C}_{\hat{q}_j}$. If instead $\tilde{Y}_t$ does not make $\hat{q}_i$ switch, then it must be that $\phi^\pi_{\hat{x}}(t^2, (x_0, \hat{q}_i), \tilde{d}_t, \epsilon) \in B$ for some t^2. Combining the last two statements, we obtain that for all π, there exists $t,\ \tilde{d}_t,$ and $\tilde{Y}_t$ such that either $\phi^\pi_{\hat{x}}(t, (x_0, \hat{q}_i), \tilde{d}_t, \epsilon) \in \hat{C}_{\hat{q}_j}$ or $\phi^\pi_{\hat{x}}(t, (x_0, \hat{q}_i), \tilde{d}_t, \epsilon) \in B$, which implies $x_0 \in A$. ■

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

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

Proposition 5: Let $S := (S_1, ..., S_M)$ be a tuple of sets $S_i \subseteq X$ such that $S = G(S)$. Then, $(X \times \hat{Q})/\bigcup_{\hat{q}_i \in \hat{Q}} (S_i, \hat{q}_i)$ is a controlled invariant set for $\hat{H}$.

Proof: Let $(x_0, \hat{q}) \notin \bigcup_{\hat{q}_i \in \hat{Q}} (S_i, \hat{q}_i)$ for $\hat{q} = \hat{q}_i \in \hat{Q}$. Then $x_0 \notin S_i$, where $S_i = \text{Pre}\left(\hat{q}_i, \bigcup_{\{j \mid \hat{q}_j \in \hat{R}(\hat{q}_i, \mathcal{Y})\}} S_j \cup B\right)$. By the definition of Pre, this implies that while $\hat{q}(t) = q_i$ (i.e., $\tilde{Y}_t = \epsilon$) there is a feedback map $\pi(\cdot, \hat{q}_i)$ such that $\phi^\pi_{\hat{x}}(t, (x_0, \hat{q}_i), \tilde{d}_t, \tilde{Y}_t) \notin S_i$. Let t^* be such that $\hat{q}(t^*)$

switches to $\hat{q}_j \in \hat{R}(\hat{q}_i, \mathcal{Y})$. At time t^*, we also have that any $\hat{x}(t^*) := \phi^{\pi}_{\hat{x}}(t^*, (x_0, \hat{q}_i), \tilde{d}_t, \tilde{Y}_t)$ is not in S_i and thus $\hat{x}(t^*) \notin S_j$ which implies $(\hat{x}(t^*), \hat{q}(t^*)) \notin \bigcup_{\hat{q}_i \in \hat{Q}}(S_i, \hat{q}_i)$. Proceeding iteratively on the mode switch, we obtain that the flows of $\hat{H}$ starting from any $(x_0, \hat{q}) \notin \bigcup_{\hat{q}_i \in \hat{Q}}(S_i, \hat{q}_i)$ stay outside $\bigcup_{\hat{q}_i \in \hat{Q}}(S_i, \hat{q}_i)$ for a proper control map. Thus, the set $(X \times \hat{Q}) / \bigcup_{\hat{q}_i \in \hat{Q}}(S_i, \hat{q}_i)$ is a controlled invariant set. ■

Define the partial order $(Z, \subseteq)$, where $\subseteq$ is defined component-wise. This is a complete partial order [5]. One can verify that G is an order preserving map on $(Z, \subseteq)$.

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 $S^{K^*} = S^{K^*+1}$, we denote the fixed point by S^*. The next theorem states that this fixed point is equal to $(\hat{C}_{\hat{q}_1}, \ldots, \hat{C}_{\hat{q}_M})$.

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: We first show that if Algorithm 1 terminates, then S^* is the least fixed point of G (lfp(G)), which exists by Knaster-Tarski fixed point theorem because G is an order preserving map on a complete partial order [5]. Then we show that $(\hat{C}_{\hat{q}_1}, ..., \hat{C}_{\hat{q}_M}) = \text{lfp}(G)$. If Algorithm 1 terminates, then there is $N^* > 0$ such that $G(\perp)^{N^*} = G(\perp)^{N^*+1} = S^*$, in which $\perp = \emptyset$. 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 β. Since $\perp \leq \beta$, we have that $G(\perp) \leq G(\beta) = \beta$, $G^2(\perp) \leq G(\beta) = \beta$,...., $G^{N^*}(\perp) \leq \beta$. Since $G^{N^*}(\perp) = S^*$, we have that $S^* \leq \beta$.

Proposition 4 indicates that the set $\hat{C} = \bigcup_{\hat{q}_i \in \hat{Q}}(\hat{C}_{\hat{q}_i}, \hat{q}_i)$ 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 $\hat{W} = (X \times \hat{Q}) / \bigcup_{\hat{q}_i \in \hat{Q}}(\hat{C}_{\hat{q}_i}, \hat{q}_i)$ and the new set $\hat{W}'$ defined as $\hat{W}' := (X \times \hat{Q}) / \bigcup_{\hat{q}_i \in \hat{Q}}(S_i, \hat{q}_i)$. By Proposition 5, these two sets are both controlled invariant and are both contained in $X \times \hat{Q} / (B \times \hat{Q})$. Since $\hat{W} \subseteq \hat{W}'$, we have that $\hat{W}$ is not the maximal controlled invariant set contained in the complement of $B \times \hat{Q}$. This contradicts Proposition 1, which states that $\hat{W}$ is the maximal controlled invariant set contained in the complement of $B \times \hat{Q}$. Therefore, the tuple $\hat{C}_{\hat{q}_1}, ..., \hat{C}_{\hat{q}_M}$ must be the least fixed point of G. ■

B. Termination of Algorithm 1

Consider the transition system defined by the discrete state update law of $\hat{H}$ from equations (2), that is, $\hat{q}(t^+) = \hat{R}(\hat{q}(t), Y(t))$, $Y(t) \in \mathcal{Y}$, in which $\hat{q} \in \hat{Q} = \{\hat{q}_1, \ldots, \hat{q}_M\}$.

Definition 3: (Reachable set) The reachable set from a state $\hat{q}_i$ is defined as $Reach(\hat{q}_i) := \{\hat{q}_j \in \hat{Q} \mid \exists\, t,\ \exists\, \tilde{Y}_t \ s.t.\ \hat{q}_j = \phi_{\hat{q}}(t, \hat{q}_i, \tilde{Y}_t)\}$.

Definition 4: (Kernel set) The kernel set corresponding to a mode $\hat{q}_i$ is defined as $ker(\hat{q}_i) = \{\hat{q} \in \hat{Q} \mid \hat{q} \in Reach(\hat{q}_i)$ and $\hat{q}_i \in Reach(\hat{q})\}$.

The set $ker(\hat{q}_i)$ is the set of all modes that can be reached from $\hat{q}_i$ and from which $\hat{q}_i$ can be reached.

Definition 5: (Type of a kernel) A kernel is $type(1)$ if it does not transit to any other kernel. A kernel is $type(n)$ if it transits to $type(n-1)$ kernels and only to $type(n-1), \ldots, type(1)$ kernels.

Let $\hat{Q}^{ker} := \{ker(\hat{q}_1), \ldots, ker(\hat{q}_M)\}$. Let there be p distinct elements in $\hat{Q}^{ker}$, denoted $\Delta K_1, \ldots, \Delta K_p$. Note that $\Delta K_i \cap \Delta K_j = \emptyset$, for $i \neq j$. Let there be K_a elements in kernel ΔK_a.

Theorem 2: Algorithm 1 terminates if all the kernels $\Delta K_1, \ldots, \Delta K_p$ have a maximal element with respect to the partial order $(2^Q, \subseteq)$.

Proof: We first show that Algorithm 1 terminates for all $type(1)$ kernels. We use the induction argument to prove that if Algorithm 1 terminates for $type(1), \ldots, type(n)$ kernel, then it terminates for $type(n+1)$ kernels.

(Base case.) Consider a mode $\hat{q}_l \in \Delta K_a$, in which ΔK_a is $type(1)$ and let $\hat{q}_0 \in \Delta K_a$ be the maximal element of ΔK_a. We show that Algorithm 1 terminates by showing that $S^n_l = Pre(\hat{q}_0, B)$, for any $n > K_a$. From Algorithm 1, we have that for $k > 0$

$$S^k_l = \text{Pre}\left(\hat{q}_l, \bigcup_{\{\hat{q}_{l_1} \in \hat{R}(\hat{q}_l, \mathcal{Y})\}} \text{Pre}\left(\hat{q}_{l_1}, \bigcup_{\{\hat{q}_{l_2} \in \hat{R}(\hat{q}_{l_1}, \mathcal{Y})\}} \text{Pre}\left(\hat{q}_{l_2}, \ldots \bigcup_{\{\hat{q}_{l_k} \in \hat{R}(\hat{q}_{l_{k-1}}, \mathcal{Y})\}} \text{Pre}\left(\hat{q}_{l_k}, B\right)\right)\right)\right). \quad (3)$$

Let $k < n$ be such that $\hat{q}_0 \in \hat{R}(\hat{q}_{l_{k-1}}, \mathcal{Y})$. Then $S^k_l \supseteq \text{Pre}(\hat{q}_0, B)$ from a repeated application of Proposition 2 (i). Since $S^n_l \supseteq S^k_l$ for $k < n$, we have $S^n_l \supseteq \text{Pre}(\hat{q}_0, B)$. We obtain $S^n_l \subseteq \text{Pre}(\hat{q}_0, B)$ by repeatedly applying Propositions 2 (iv), with $\hat{q}_2 = \hat{q}_0$, and Proposition 2 (ii) to equation (3) with $k = n$.

(Induction step.) We assume that Algorithm 1 terminates for all $type(1)$ to $type(n)$ kernels. Consider a mode $\hat{q}_l \in \Delta K_a$ where ΔK_a is a $type(n+1)$ kernel. Then for all J, we have

$$S^J_l = \text{Pre}(\hat{q}_l, \bigcup_{\{l_1 | \hat{q}_{l_1} \in \hat{R}(\hat{q}_l, \mathcal{Y}) \cap \Delta K_a\}} S^{J-1}_{l_1} \bigcup_{\{l^*_1 | \hat{q}_{l^*_1} \in \hat{R}(\hat{q}_l, \mathcal{Y}) \setminus \Delta K_a\}} S^{J-1}_{l^*_1}), \quad (4)$$

where $\hat{q}_{l^*_1}$ belongs to $type(1), \ldots, type(n)$ kernels. By the induction assumption, there exists N^* such that $S^N_{l^*_1} = S^{N+1}_{l^*_1} = S^{N^*}_{l^*_1}$ for all $N > N^*$. Let then $J > N^*$. Let $\hat{q}_0$ be the maximal element of ΔK_a and assume that we can transition from mode $\hat{q}_l$ to $\hat{q}_0$ in N_1 transitions. Starting from mode $\hat{q}_0$, the discrete flow can visit $\hat{q}_0$ again, since $\hat{q}_0$ is in ΔK_a. We consider the shortest path in which the discrete flow starts at $\hat{q}_0$ and reaches back to $\hat{q}_0$, in N_2 transitions, after visiting all the modes in ΔK_a. Let us

also assume that $J = i > N^* + N_1 + N_2$. Then, we have that $\hat{q}_0 \in \{\hat{R}(\hat{q}_{l_{N_1-1}}, \mathcal{Y}) \cap \Delta K_a\}$ and $\hat{q}_0 \in \{\hat{R}(\hat{q}_{l_{N_1+N_2-1}}, \mathcal{Y}) \cap \Delta K_a\}$.

Note that by Proposition 2 (iv), the right hand side of equation (4), with $\hat{q}_l$ replaced by $\hat{q}_0$ and $J = i$, contains S_l^i. In the resulting expression, we substitute $S_{l_1}^{i-1} = \text{Pre}(\hat{q}_{l_1}, \bigcup_{\{l_2|\hat{q}_{l_2}\in\hat{R}(\hat{q}_{l_1},\mathcal{Y})\cap\Delta K_a\}} S_{l_2}^{i-2} \bigcup_{\{l_2^*|\hat{q}_{l_2^*}\in\hat{R}(\hat{q}_{l_1},\mathcal{Y})\setminus\Delta K_a\}} S_{l_2^*}^{i-2})$ and obtain

$$S_l^i \subseteq \text{Pre}\Bigg(\hat{q}_0, \bigcup_{\{l_1^*|\hat{q}_{l_1^*}\in\hat{R}(\hat{q}_l,\mathcal{Y})\setminus\Delta K_a\}} S_{l_1^*}^{i-1} \bigcup_{\{l_1|\hat{q}_{l_1}\in\hat{R}(\hat{q}_l,\mathcal{Y})\cap\Delta K_a\}} \text{Pre}\Bigg(\hat{q}_{l_1}, \bigcup_{\{l_2|\hat{q}_{l_2}\in\hat{R}(\hat{q}_{l_1},\mathcal{Y})\cap\Delta K_a\}} S_{l_2}^{i-2} \bigcup_{\{l_2^*|\hat{q}_{l_2^*}\in\hat{R}(\hat{q}_{l_1},\mathcal{Y})\setminus\Delta K_a\}} S_{l_2^*}^{i-2}\Bigg)\Bigg). \tag{5}$$

Employing Proposition 2 (vi) to the right hand side of (5), we obtain

$$S_l^i \subseteq \text{Pre}\Bigg(\hat{q}_0, \bigcup_{\{l_1^*|\hat{q}_{l_1^*}\in\hat{R}(\hat{q}_l,\mathcal{Y})\setminus\Delta K_a\}} S_{l_1^*}^{i-1} \bigcup_{\{\hat{q}_{l_1}\in\hat{R}(\hat{q}_l,\mathcal{Y})\cap\Delta K_a\}} \bigcup_{\{l_2^*|\hat{q}_{l_2^*}\in\hat{R}(\hat{q}_{l_1},\mathcal{Y})\setminus\Delta K_a\}} S_{l_2^*}^{i-2} \bigcup_{\{\hat{q}_{l_1}\in\hat{R}(\hat{q}_l,\mathcal{Y})\cap\Delta K_a\}} \bigcup_{\{l_2|\hat{q}_{l_2}\in\hat{R}(\hat{q}_{l_1},\mathcal{Y})\cap\Delta K_a\}} S_{l_2}^{i-2}\Bigg). \tag{6}$$

To simplify notation, let us define $\mathcal{S}_{l_1^*} := \bigcup_{\{l_1^*|\hat{q}_{l_1^*}\in\hat{R}(\hat{q}_l,\mathcal{Y})\setminus\Delta K_a\}} S_{l_1^*}^{i-1}$ and $\mathcal{S}_{l_m^*} := \bigcup_{\{\hat{q}_{l_1}\in\hat{R}(\hat{q}_l,\mathcal{Y})\cap\Delta K_a\}} \cup \ldots \cup \bigcup_{\{\hat{q}_{l_{m-1}}\in\hat{R}(\hat{q}_{l_{m-2}},\mathcal{Y})\cap\Delta K_a\}} \bigcup_{\{l_m^*|\hat{q}_{l_{m-1}^*}\in\hat{R}(\hat{q}_{l_{m-2}},\mathcal{Y})\setminus\Delta K_a\}} S_{l_m^*}^{i-m}$ for $1 < m < i$. Equation (6) becomes $S_l^i \subseteq \text{Pre}(\hat{q}_l, \mathcal{S}_{l_1^*} \cup \mathcal{S}_{l_2^*} \bigcup_{\{\hat{q}_{l_1}\in\hat{R}(\hat{q}_l,\mathcal{Y})\cap\Delta K_a\}} \bigcup_{\{l_2|\hat{q}_{l_2}\in\hat{R}(\hat{q}_{l_1},\mathcal{Y})\cap\Delta K_a\}} S_{l_2}^{i-2})$.

Employing equation (4) with $J = i - 2$ for $S_{l_2}^{i-2}$ in the above expression and employing Proposition 2 (vi), we obtain $S_l^i \subseteq \text{Pre}(\hat{q}_l, \mathcal{S}_{l_1^*} \cup \mathcal{S}_{l_2^*} \cup \mathcal{S}_{l_3^*} \bigcup_{\{\hat{q}_{l_1}\in\hat{R}(\hat{q}_l,\mathcal{Y})\cap\Delta K_a\}} \bigcup_{\{\hat{q}_{l_2}\in\hat{R}(\hat{q}_{l_1},\mathcal{Y})\cap\Delta K_a\}} \bigcup_{\{l_3|\hat{q}_{l_3}\in\hat{R}(\hat{q}_{l_2},\mathcal{Y})\cap\Delta K_a\}} S_{l_3}^{i-3})$. Proceeding by repeatedly expanding $S_{l_m}^{i-m}$ for $m = 3, \ldots, i-1$ and employing Proposition 2 (vi), we obtain

$$S_l^i \subseteq \text{Pre}\Bigg(\hat{q}_0, \mathcal{S}_{l_1^*} \cup \ldots \mathcal{S}_{l_i^*} \bigcup_{\{\hat{q}_{l_1}\in\hat{R}(\hat{q}_l,\mathcal{Y})\cap\Delta K_a\}} \bigcup_{\{\hat{q}_{l_2}\in\hat{R}(\hat{q}_{l_1},\mathcal{Y})\cap\Delta K_a\}} \ldots \bigcup_{\{l_i|\hat{q}_{l_i}\in\hat{R}(\hat{q}_{l_{i-1}},\mathcal{Y})\cap\Delta K_a\}} \text{Pre}(\hat{q}_{l_i}, B)\Bigg), \tag{7}$$

in which $\mathcal{S}_{l_m^*} := \bigcup_{\{\hat{q}_{l_1}\in\hat{R}(\hat{q}_l,\mathcal{Y})\cap\Delta K_a\}} \ldots \bigcup_{\{\hat{q}_{l_{m-1}}\in\hat{R}(\hat{q}_{l_{m-2}},\mathcal{Y})\cap\Delta K_a\}} \bigcup_{\{l_m^*|\hat{q}_{l_m^*}\in\hat{R}(\hat{q}_{l_{m-1}},\mathcal{Y})\setminus\Delta K_a\}} S_{l_m^*}^{i-m}$ for $m \leq i$. Note that since $\hat{q}_{l_m^*} \notin \Delta K_a$, it belongs to a kernel of type less than or equal to n which implies that $\mathcal{S}_{l_m^*}$ is a fixed point of Algorithm 1 for $i - m \geq N^*$ (in particular for $m \leq N_1 + N_2$). According to our assumption, starting from $\hat{q}_l$ we can reach $\hat{q}_0$ in N_1 transitions and from $\hat{q}_0$ we can reach $\hat{q}_0$ again in N_2 transitions after visiting all the modes in ΔK_a. Thus we have for $m = N_1 + N_2$ that $\{\bigcup_{\{\hat{q}_{l_1}\in\hat{R}(\hat{q}_l,\mathcal{Y})\cap\Delta K_a\}} \cdots \bigcup_{\{l_{m-1}|\hat{q}_{l_{m-1}}\in\hat{R}(\hat{q}_{l_{m-2}},\mathcal{Y})\cap\Delta K_a\}} \hat{q}_{l_{m-1}}\} = \Delta K_a$.

The set $K := \{\bigcup_{\{\hat{q}_{l_1}\in\hat{R}(\hat{q}_l,\mathcal{Y})\cap\Delta K_a\}} \cdots \bigcup_{\{\hat{q}_{l_{m-1}}\in\hat{R}(\hat{q}_{l_{m-2}},\mathcal{Y})\cap\Delta K_a\}} \bigcup_{\{l_m^*|\hat{q}_{l_m^*}\in\hat{R}(\hat{q}_{l_{m-1}},\mathcal{Y})\setminus\Delta K_a\}} \hat{q}_{l_m^*}\}$ consists of all the modes not in ΔK_a that can be reached in one transition from modes in ΔK_a. This implies that the sets in $\{\mathcal{S}_{l_1^*}, \ldots, \mathcal{S}_{l_{N_1+N_2}^*}\}$ are the fixed points of Algorithm 1 for the modes that can be reached from each mode in kernel ΔK_a in one transition. Let us denote these sets by $\{\mathcal{S}_{1^*}, \mathcal{S}_{2^*}, \ldots, \mathcal{S}_{K_a{}^*}\}$. The elements of $\{\mathcal{S}_{l_{N_1+N_2+1}^*}, \ldots, \mathcal{S}_{l_i^*}\}$ are the sets obtained in each iteration of Algorithm 1 for the modes that can be reached from each mode in kernel ΔK_a in one transition, and thus are subsets of the fixed points $\{\mathcal{S}_{1^*}, \mathcal{S}_{2^*}, \ldots, \mathcal{S}_{K_a{}^*}\}$. Thus equation (7) simplifies to $S_l^i \subseteq \text{Pre}(\hat{q}_0, \bigcup_{\{j|\hat{q}_j\in\Delta K_a\}}(\mathcal{S}_{j^*} \cup \text{Pre}(\hat{q}_j, B)))$, which further simplifies to $S_l^i \subseteq \text{Pre}(\hat{q}_0, \bigcup_{\{j|\hat{q}_j\in\Delta K_a\}} \mathcal{S}_{j^*})$ by Proposition 2 (vi).

Now, $S_l^i \supseteq S_{l_{N_1}}^{i-N_1} = \text{Pre}(\hat{q}_{l_{N_1}}, \bigcup_{\{l_{N_1+1}|\hat{q}_{l_{N_1+1}}\in\hat{R}(\hat{q}_{l_{N_1}},\mathcal{Y})\cap\Delta K_a\}} S_{l_{N_1+1}}^{i-N_1+1} \bigcup_{\{l_{N_1+1}^*|\hat{q}_{l_{N_1+1}^*}\in\hat{R}(\hat{q}_{l_{N_1}},\mathcal{Y})\setminus\Delta K_a\}} S_{l_{N_1+1}^*}^{i-N_1+1})$. Since $\hat{q}_0$ is reachable from $\hat{q}_l$ in N_1 transitions, we have that $\hat{q}_0 \in \bigcup_{\{l_{N_1} \mid \hat{q}_{l_{N_1}} \in \hat{R}(\hat{q}_{l_{N_1-1}},\mathcal{Y})\cap\Delta K_a\}} \hat{q}_{l_{N_1}}$. Thus $S_l^i \supseteq \text{Pre}(\hat{q}_0, \bigcup_{\{l_{N_1-1} \mid \hat{q}_{l_{N_1-1}}\in\hat{R}(\hat{q}_{l_{N_1}},\mathcal{Y})\cap\Delta K_a\}} S_{l_{N_1-1}}^{i-N_1-1} \bigcup_{\{l_{N_1-1}^* \mid \hat{q}_{l_{N_1-1}^*}\in\hat{R}(\hat{q}_{l_{N_1}},\mathcal{Y})\setminus\Delta K_a\}} S_{l_{N_1-1}^*}^{i-N_1-1})$. Simplifying the right hand side of this equation by repeatedly applying equation (4) and Proposition 2 (vi), we obtain $S_l^i \supseteq \text{Pre}(\hat{q}_0, \bigcup_{\{j^*|\hat{q}_{j^*}\in\Delta K_a\}} \mathcal{S}_{j^*})$.

Thus $S_l^i = Pre(\hat{q}_0, \bigcup_{\{j^*|\hat{q}_{j^*}\in\Delta K_a\}} \mathcal{S}_{j^*})$, in which $\mathcal{S}_{j^*}$ can be computed in a finite iteration. As a consequence, also S_l^i can be computed in a finite iteration. Since the algorithm terminates for kernels of any type, it terminates for the transition system described in (2). ■

C. Control Map

Once the sets $\hat{C}_{\hat{q}_i}$ are computed for all $\hat{q}_i$ as uncontrollable predecessors of a suitable set (Theorem 1), we mathematically characterize the set of all control maps that keep the state of $\hat{H}$ outside $\hat{C}$ by employing viability theory [2]. Let X be a normed space and let $K \subset X$ be nonempty. The *contingent cone* to K at $x \in K$ is the set given by $T_K(x) := \{v \in K \mid \liminf_{h\to 0+} \frac{d_K(x+hv)}{h} = 0\}$, in which $d_K(y)$ denotes the distance of y from set K, that is, $d_K(y) := \inf_{z\in K}\|y - z\|$. Thus, when K is an open set, the contingent cone to K at any point in K is always equal to the whole space. If K is a differentiable manifold, $T_K(x)$ coincides with the tangent space to K at x. A set valued map $F : X \to 2^X$ is said *Marchaud* if (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 $\sup\{\|v\| \mid c \in F(x) \leq c(\|x\| + 1)\}$. Further, we say that F is *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. We say that F is 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 $i \neq j$.

Proposition 6: Let $F : X \to 2^X$ be a set-valued Marchaud map. Assume that F is piecewise Lipschitz continuous on X. A closed set $K \subseteq X$ is invariant under F if and only if $F(x) \subseteq T_K(x)$ for all $x \in K$.

Proof: (Sketch) 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 [3] to the resulting impulse differential inclusion to conclude invariance of K. ■

To simplify notation, for $\hat{q} \in \hat{Q}$ define a map $\bar{f}$ such that $\{f(x, \alpha, u, d), \alpha \in \hat{q}, d \in \Delta\} = \{\bar{f}(x, u, \theta), \theta \in \Theta(\hat{q})\}$. That is, we incorporate all the uncertainty introduced by $\alpha \in \hat{q}$ and $d \in \Delta$ in one parameter θ that varies in a set $\Theta(\hat{q})$ dependent on the mode $\hat{q}$. Let then $L_{\hat{q}} := X \backslash \hat{C}_{\hat{q}}$ for all $\hat{q} \in \hat{Q}$ and consider the set valued map defined as $\Pi(x, \hat{q}) := \{u \in \mathcal{U} \mid \bar{f}(x, u, \theta) \in T_{L_{\hat{q}}}(x) \ \forall \theta \in \Theta(\hat{q})\}$.

Theorem 3: Assume that $\pi(x, \hat{q})$ for any mode $\hat{q}$ is such that the set-valued map $F(x) := \{\bar{f}(x, \pi(x, \hat{q}), \theta), \theta \in \Theta(\hat{q})\}$ is Marchaud and piecewise Lipschitz on X. Then, the set $(X \times \hat{Q}) \backslash \hat{C}$ is invariant for $\hat{H}^\pi$ if and only if $\pi(x, \hat{q}) \in \Pi(x, \hat{q})$.

Proof: ($\Leftarrow$) Assume that $\pi(x, \hat{q}) \in \Pi(x, \hat{q})$ and that $(\hat{x}(t_0), \hat{q}(t_0)) \notin \hat{C}$, we show that all $(\hat{x}(t), \hat{q}(t)) \notin \hat{C}$ for all $t \geq t_0$. Let $\{t_k\}_{k>0}$ be the sequence of times at which there is a mode shift, we show that $(\hat{x}(t), \hat{q}(t)) \notin \hat{C}$ for all $t \in [t_k, t_{k+1}]$ for all $k \geq 0$. This is shown by induction argument on k. (Base case) By assumption we have that $(\hat{x}(t_0), \hat{q}(t_0)) \notin \hat{C}$. (Induction step) Assume that $(\hat{x}(t_k), \hat{q}(t_k)) \notin \hat{C}$. We show that this implies $(\hat{x}(t), \hat{q}(t)) \notin \hat{C}$ for all $t \in (t_k, t_{k+1}]$. This in turn is equivalent to show that $\hat{x}(t) \notin \hat{C}_{\hat{q}(t_k)}$ for all $t \in (t_k, t_{k+1})$ and $\hat{x}(t_{k+1}) \notin \hat{C}_{\hat{q}(t_{k+1})}$. Since $\hat{C}_{\hat{q}(t_{k+1})} \subseteq \hat{C}_{\hat{q}(t_k)}$ by the properties of the Pre operator and by Proposition 4, it is enough to show that $\hat{x}(t) \notin \hat{C}_{\hat{q}(t_k)}$ for all $t \in (t_k, t_{k+1}]$. For $t \in (t_k, t_{k+1})$, the trajectory $\hat{x}(t)$ of $\hat{H}^\pi$ satisfies $\dot{\hat{x}} = \bar{f}(\hat{x}, \pi(\hat{x}, \hat{q}(t_k)), \theta), \ \theta \in \Theta(\hat{q}(t_k))$, in which we denote $F(\hat{x}) := \{\bar{f}(\hat{x}, \pi(\hat{x}, \hat{q}(t_k)), \theta), \ \theta \in \Theta(\hat{q}(t_k))\}$. Since $\pi(\hat{x}, \hat{q}) \in \Pi(\hat{x}, \hat{q})$, it follows that $\bar{f}(\hat{x}, \pi(\hat{x}, \hat{q}(t_k)), \theta) \in T_{L_{\hat{q}(t_k)}}(\hat{x})$ for all $\theta \in \Theta(\hat{q}(t_k))$, which in turn implies that $F(\hat{x}) \subseteq T_{L_{\hat{q}(t_k)}}(\hat{x})$. Proposition 6 thus implies that $L_{\hat{q}(t_k)}$ is invariant by F. Therefore, we have that $\hat{x}(t) \in L_{\hat{q}(t_k)}$ for all $t \in (t_k, t_{k+1}]$. Thus, $\hat{x}(t) \notin \hat{C}_{\hat{q}(t_k)}$ for all $t \in (t_k, t_{k+1}]$.

($\Rightarrow$) The fact that if $\pi(x, \hat{q}) \notin \Pi(x, \hat{q})$ the set $(X \times \hat{Q})/C$ is not invariant for $\hat{H}^\pi$ follows from Proposition 6. ■

IV. A E

Consider two vehicles merging on an intersection (Fig. 1). In this paper, we assume that one of the two vehicles does not have an on-board controller and the two vehicles do not communicate. We model the non-communicating vehicle as a hybrid automaton with modes that undergo non-autonomous transitions due to the discrete disturbance control input from the human driver. These modes model the vehicle in either braking or acceleration maneuver. In the proximity of the intersection, we assume that the human driver either decides to brake or accelerate and that the mode remains the same.

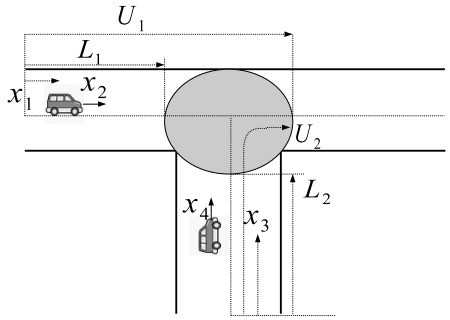

Fig. 1. Two vehicles merging on an intersection. If two vehicles are both in the shaded region, a collision occurs.

The hybrid automaton that models the above system is $H = (Q, X, \mathcal{U}, \Delta, \Sigma, R, f)$, in which $X \subseteq \mathbb{R}^4, Q = \{q_1, q_2\}$. The X coordinate system is taken along the path of the vehicles. The bad set is given as $B = \{x \in X \mid (x_1, x_3) \in (L_1, U_1) \times (L_2, U_2)\}$, where L_1, U_1, L_2 and U_2 are shown in Fig. 1, (x_1, x_3) are the positions of the vehicles along their paths and (x_2, x_4) are their longitudinal speeds. Longitudinal dynamics of the vehicle is modeled as a second order system [18]. Since the mode cannot switch, $\dot{x} = f(x, q, u, d)$, $x = (x_1, x_2, x_3, x_4)$, and $f(x, q, u, d) = (f_1(x, q, d), \ f_2(x, u))$, with

$$f_1(x, q, d) = \begin{cases} (x_2, b_q + d), & \text{if } x_2 \in [x_{2min}, x_{2max}] \\ (x_2, 0), & \text{if } x_2 \leq x_{2min} \text{ and } b_q + d < 0 \\ & \text{or } x_2 \geq x_{2max} \text{ and } b_q + d > 0, \end{cases} \tag{8}$$

$$f_2(x, u) = \begin{cases} (x_4, u), & \text{if } x_4 \in [x_{4min}, x_{4max}] \\ (x_4, 0), & \text{if } x_4 \leq x_{4min} \text{ and } u < 0 \\ & \text{or } x_4 \geq x_{4max} \text{ and } u > 0, \end{cases} \tag{9}$$

$d \in [-D, D]$ and $u \in [u_L, u_H]$. The continuous state can be measured, for example by road side speed sensors, and communicated by the infrastructure. In this example, since the mode does not switch and the continuous dynamics are linear in the parameters, we can use the least squares method to construct $\mathcal{F}(\tilde{x}_{[t-T,t]})$.

Assume $0 \in [b_{q_i} - D, b_{q_i} + D]$. Consider system (8) with $q = q_i$ and let $\hat{b} = \frac{1}{T} \int_{\tau - T}^{\tau} \dot{x}_2(\tau) d\tau, \ \tau \geq T$ [1]. Then one can show that $|\hat{b} - b_{q_i}| \leq D$. Thus, we define

$$\mathcal{F}(\tilde{x}_{[t-T,t]}) = \begin{cases} \{q_1, q_2\} & if \ |\hat{b} - b_{q_i}| \leq D, i \in \{1, 2\} \\ \{q_i\} & if \ |\hat{b} - b_{q_j}| > D, j \neq i \end{cases}$$ (see [10] for more details).

Since $0 \in [b_{q_i} - D, b_{q_i} + D], i \in \{1, 2\}$ we define $\bar{f}_1(\hat{x}, \theta) \triangleq (\hat{x}_2, \theta)$ with $\theta \in \begin{cases} [b_{q_1} - D, b_{q_2} + D], \text{if } \hat{q} = \hat{q}_1 \\ [b_{q_1} - D, b_{q_1} + D], \text{if } \hat{q} = \hat{q}_2 \\ [b_{q_2} - D, b_{q_2} + D], \text{if } \hat{q} = \hat{q}_3 \end{cases}$.

Employing Algorithm 1, we obtain $\hat{C}_{\hat{q}_1} = \text{Pre}(\hat{q}_1, B \cup \text{Pre}(\hat{q}_2, B) \cup \text{Pre}(\hat{q}_3, B)), \hat{C}_{\hat{q}_2} = \text{Pre}(\hat{q}_2, B), \hat{C}_{\hat{q}_3} = \text{Pre}(\hat{q}_3, B)$. Using Proposition 2, these expressions further simplify to $\hat{C}_{\hat{q}_1} = \text{Pre}(\hat{q}_1, B), \hat{C}_{\hat{q}_2} = \text{Pre}(\hat{q}_2, B), \hat{C}_{\hat{q}_3} = \text{Pre}(\hat{q}_3, B)$.

[1] In practice, measurement of acceleration will not be required as discrete time models will be considered for implementation.

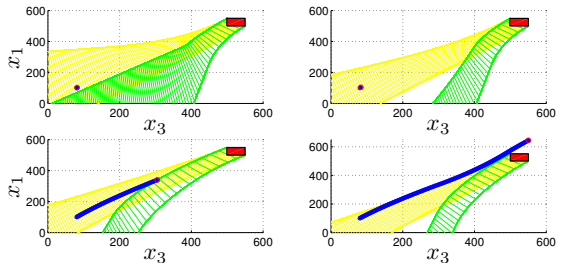

Fig. 2. The yellow set, green set and intersection of these sets represent the slice, corresponding to the current speeds, of $\text{Pre}(\hat{q}, B)_H, \text{Pre}(\hat{q}, B)_L$ and the capture set, $\text{Pre}(\hat{q}, B)$ in the (x_3, x_1) plane, respectively. The current position of the two vehicles (x_3, x_1) is shown as a red circle and set $[L_1, U_1] \times [L_2, U_2]$ is shown as a red rectangle in the figures above.

In order to calculate $\text{Pre}(\hat{q}_1, B), \text{Pre}(\hat{q}_2, B)$ and $\text{Pre}(\hat{q}_3, B)$ numerically, we use the following relationship [11] $\text{Pre}(\hat{q}, B) = \text{Pre}(\hat{q}, B)_L \cap \text{Pre}(\hat{q}, B)_H$, where, $\text{Pre}(\hat{q}, B)_L = \{x \in X \mid \exists\, t,\ \exists\, \tilde{d}_t \ \ s.t.$ some $\phi_{\hat{x}}(t, (x, \hat{q}), \tilde{d}_t, u_L, \epsilon) \in B\}$ and $\text{Pre}(\hat{q}, B)_H = \{x \in X \mid \exists\, t, \exists\, \tilde{d}_t \ \ s.t.$ some $\phi_{\hat{x}}(t, (x, \hat{q}), \tilde{d}_t, u_H, \epsilon) \in B\}$. Since B is an open box in the (x_1, x_3) coordinates, the sets $\text{Pre}(\hat{q}, B)_L$ and $\text{Pre}(\hat{q}, B)_H$ can be easily computed with a linear complexity discrete time algorithm [6].

A feedback map $\pi(x, \hat{q})$, that satisfies Theorem 3 is given by

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

A. Simulation Results

The bad set B is such that $L_i = 500, U_i = 550$ for $i \in \{1, 2\}$. We consider a discrete time model with time step $\Delta t = 0.1$ seconds, $u \in [-1, 1], b_{q_1} = -0.4, b_{q_2} = 0.4$ and $d \in [-0.6, 0.6]$. We take $T = 0.5$ seconds to generate the least square estimate $\hat{b}$. If $\hat{b} \in [-1, -0.2], \hat{q} = \{q_1\}$, if $\hat{b} \in [0.2, 1], \hat{q} = \{q_2\}$, and if $\hat{b} \in [-0.2, .2], \hat{q} = \{q_1, q_2\}$. Simulation results are presented in Fig. 2 for the case when the vehicle controlled by nature is running in mode q_2. The initial estimated mode is $\hat{q}_1 = \{q_1, q_2\}$. At the beginning, the measurement data is not sufficient to determine which mode the system is in, thus the estimated mode is the same as the initial mode, $\hat{q}_1$ (Fig. 2, top left). At 1.3 seconds, the mode shifts from $\hat{q}_1$ to $\hat{q}_3$. Correspondingly, in Fig. 2 top right, the capture set changes and we also note that the new capture set is a subset of $\text{Pre}(\hat{q}_1, B)$. The system flow hits the boundary of the capture set $\text{Pre}(\hat{q}_3, B)$ at 11.4 seconds (Fig. 2 bottom left) and a control input $u = -1$ is applied by the controller that keeps the continuous state flow outside the capture set (Fig. 2 bottom right).

V. C

We have addressed a continuous control problem for a hybrid automaton with unknown discrete state. We have provided an algorithmic procedure for computing the capture set in the non-deterministic information state space. We have then provided the dynamic feedback map that renders the complement of the capture set invariant. Termination conditions were provided. The proposed algorithm has been illustrated on a collision avoidance scenario involving two non-communicating vehicles at a traffic intersection. In our future work, we will incorporate discrete control inputs and continuous state uncertainty. Furthermore, we will identify classes of systems for which the assumptions of the termination theorem (Theorem 2) hold and investigate connections with bisimulation techniques.

R

[1] E. Asarin, O. Maler, and A. Pnueli. Symbolic controller synthesis for discrete and timed systems. In *Hybrid Systems: Computation and Control*, volume 999, pages 1–20. Springer-Veralg, 1995.

[2] J.-P. Aubin. *Viability Theory*. Birkhuser Boston, 1st edition, 1991.

[3] J.-P. Aubin, J. Lygeros, M. Quincampoix, S. Sastry, and N. Seube. Impulse differential inclusions: a viability approach to hybridsystems. *IEEE Trans. Automatic Control*, 47(1):2–20, 2002.

[4] A. Balluchi, L. Benvenuti, M. D. Di Benedetto S, and A. L. Sangiovanni-vincentelli. Design of observers for hybrid systems. In *In Hybrid Systems: Computation and Control, volume 2289 of LNCS*, pages 76–89. Springer-Verlag, 2002.

[5] B. A. Davey and H. A. Priestley. *Introduction to lattices and order*. Cambridge University Press, 2nd edition, 2002.

[6] D. Del Vecchio. Observer-based control of block-triangular discrete time hybrid automata on a partial order. *International Journal of Robust and Nonlinear Control*, 2008.

[7] D. Del Vecchio and E. Klavins. Observation of guarded command programs. In *Conference on Decision and Control*, 2003.

[8] D. Del Vecchio, M. Malisoff, and R. Verma. A separation principle for a class of hybrid automata on a partial order. In *American Control Conference*, 2009.

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

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

[11] 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*, 2009 (To Appear).

[12] A.B. Kurzhanski and P. Varaiya. Ellipsoidal techniques for hybrid dynamics: the rechability problem. In *New Directions and Applications in Control Theory*, volume 321, pages 193–205, 2005.

[13] S. M. LaValle. *Planning Algorithms*. Cambridge University Press, 1st edition, 2006.

[14] J. Lygeros, C. J. Tomlin, and S. Sastry. Controllers for reachability specifications for hybrid systems. *Automatica*, 35(3):349 – 370, 1999.

[15] 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.

[16] O. Shakernia, G. J. Pappas, and S. Sastry. Semi-decidable synthesis for triangular hybrid ststems. In *Hybrid Systems: Computation and Control*, volume 2034, pages 949–970. Springer Veralg, 2001.

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

[18] R. Verma, D. Del Vecchio, and H. K. Fathy. Development of a scaled vehicle with longitudinal dynamics of a HMMWV for an ITS testbed. *IEEE/ASME Transactions on Mechatronics*, 13(1):46–57, 2008.

[19] M. D. Wulf, L. Doyen, and J. F. Raskin. A lattice theory for solving games of imperfect information. In *Hybrid Systems: Computation and Control*, volume 3927, pages 153–173. Springer-Veralg, 1984.