Impulse Differential Inclusions: A Viability Approach to Hybrid Systems

Jean-Pierre Aubin, John Lygeros, Marc Quincampoix, Shankar Sastry, *Fellow, IEEE*, and Nicolas Seube

***Abstract*—Impulse differential inclusions are introduced as a framework for modeling hybrid phenomena. Connections to standard problems in the area of hybrid systems are discussed. Conditions are derived that allow one to determine whether a set of states is viable or invariant under the action of an impulse differential inclusion. For sets that violate these conditions, methods are developed for approximating their viability and invariance kernels, that is the largest subset that is viable or invariant under the action of the impulse differential inclusion. The results are demonstrated on examples.**

***Index Terms*—Differential inclusions, hybrid systems, invariance, reachability, set valued analysis, viability theory.**

I. Introduction

HYBRID systems, that is dynamical systems with interacting continuous and discrete dynamics, are a convenient modeling abstraction that has been used extensively to describe systems in a wide range of applications including robotics, automotive electronics, manufacturing, automated highway systems, air traffic management systems, integrated circuit design, and multi-media [1]–[4]. A substantial part of the literature on hybrid systems has been devoted to the problem of *reachability*, that is the question of whether, under the dynamics of a hybrid system, a given set of states can be reached from a given set of initial conditions. Techniques have been developed for establishing whether the set of reachable states is contained in a certain set [5]–[9], or, in the case of hybrid control systems, for synthesizing controllers that satisfy such *safety* specifications [10]–[16]. Since the reachability problem quickly becomes computationally infeasible, approximation techniques have been proposed to facilitate the analysis [17]–[19]. Based on the theoretical results, computational tools been developed to exactly compute the reachable set of states whenever possible [20]–[23], compute conservative approximations for it [24]–[28], or at least help establish some of its properties deductively [29].

For continuous dynamical systems described by differential inclusions, questions of reachability have been addressed in the context of *viability theory* [30]. Viability theory deals with two fundamental properties of sets of states of a dynamical system. Roughly speaking, a set of states, K, is called *viable* if for all initial conditions in K there exists a solution of the dynamical system that remains in K; it is called *invariant* if for all initial conditions in K all solutions of the system remain in K. In the case where a set, K, is not viable (respectively invariant), viability theory techniques can also be used to establish the largest subset of K which is viable (respectively, invariant), which is known as the *viability kernel* (respectively, *invariance kernel*) of K. Numerical algorithms have been developed to compute these kernels (see [31] and the references therein), and have been used to compute, for example, basins of attraction for equilibria [32].

In this paper, we extend viability theory concepts to a wider class of systems, which we call *impulse differential inclusions*. Impulse differential inclusions capture a broad range of hybrid phenomena and allow one to model nondeterminism in the discrete evolution, in the continuous evolution and in the choice between the two. We formulate a mathematical framework to precisely and concisely characterize the properties of sets of states that are viable or invariant under the dynamics of an impulse differential inclusion. In cases where the viability and invariance conditions are violated, we also provide a procedure for establishing the viability and invariance kernels of a set of states. Numerical algorithms for implementing the procedure have been developed recently in a parallel study [33].

The material is arranged in five sections. In Section II, the impulse differential inclusion framework is introduced, and the basic concepts of viability theory are extended to it. Some examples are presented, to motivate subsequent discussion. In Section III we establish necessary and sufficient conditions for a set of states to be viable or invariant under the dynamics of an impulse differential inclusion. Procedures for establishing the viability and invariance kernels of a set (in cases where the conditions of Section III are violated) are developed in Section IV, and applied to examples in Section V. To maintain the flow of the paper, the more technical proofs are given in the Appendix.

Manuscript received February 2, 2001; revised June 20, 2001. Recommended by Associate Editor A. Bemporad. This work was supported in part by ONR under Grant N00014-97-1-0946, by DARPA under Contract F33615-98-C-3614, and by the EPSRC under Research Grant GR/R51575/01. The work of J. Lygeros was partially carried out during his visit at the Laboratoire de Mathématiques de l'Université de Bretagne Occidentale in June 1999.

J.-P. Aubin is with the Centre de Recherche Viabilité, Jeux, Contrôle, Université Paris-Dauphine, F-75005 Paris, France (e-mail: J.P.Aubin@wanadoo.fr).

J. Lygeros is with the Department of Engineering, University of Cambridge, Cambridge, CB2 1PZ, U.K. (e-mail: jl290@eng.cam.ac.uk).

M. Quincampoix is with the Départment de Mathématiques, Faculté des Sciences, Université de Bretagne Occidentale, BP 809 29285 Brest cedex, France (e-mail: Marc.Quincampoix@univ-brest.fr).

S. Sastry is with the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Berkeley, CA 94720 USA (e-mail: sastry@eecs.berkeley.edu).

N. Seube is with ENSIETA, rue Francois Verny, 29200 Brest, France (e-mail: seube@ensieta.fr).

Publisher Item Identifier S 0018-9286(02)01099-1.

II. Impulse Differential Inclusions

A. Notation and Terminology

We start with a brief overview of some standard definitions from nonsmooth and set valued analysis; for a more thorough treatment the reader is referred to [34], [35]. For an arbitrary set, K, 2^K is used to denote the power set of K, i.e., the set of all subsets of K. For a set valued map R: $X \to 2^Y$ and a set $K \subseteq Y$ we use $R^{-1}(K)$ to denote the *inverse image* of K under R and $R^{\ominus 1}(K)$ to denote the *extended core* of K under R, defined by

$$R^{-1}(K) = \{x \in X | R(x) \cap K \neq \emptyset\}$$

and

$$R^{\ominus 1}(K) = \{x \in X | R(x) \subseteq K\} \cup \{x \in X | R(x) = \emptyset\}.$$

The inverse image and extended core are equivalent to the notions of relation pre-image operators, discussed, for example, in [36] in the context of modal logics. Notice that $R^{-1}(Y)$ is the set of $x \in X$ such that $R(x) \neq \emptyset$. We call the set $R^{-1}(Y)$ the *domain* of R and the set $\{(x, y) \in X \times Y | y \in R(x)\}$ the *graph* of R.

We use X to denote a finite dimensional vector space with the standard Euclidean metric, denoted by d. We use $\|\cdot\|$ to denote the corresponding norm. The metric notation is extended to sets $K \subseteq X$ by setting

$$d(x, K) = \inf_{x' \in K} d(x, x').$$

For $x \in X$, we use $B(x, \eta)$ to denote the closed unit ball of radius $\eta \geq 0$ about x

$$B(x, \eta) = \{x' \in X | d(x, x') \leq \eta\}.$$

The notation is extended to subsets $K \subseteq X$ by setting

$$B(K, \eta) = \bigcup_{x \in K} B(x, \eta).$$

We define the sum of two subsets, K and L, of a finite dimensional vector space as the set

$$K + L = \{x + y | x \in K \text{ and } y \in L\}.$$

A set valued map R: $X \to 2^X$ is called *upper semicontinuous at* $x \in X$ if for every $\epsilon > 0$ there exists $\delta > 0$ such that

$$\forall x' \in B(x, \delta), \quad R(x') \subseteq B(R(x), \epsilon).$$

R is called *lower semicontinuous at* $x \in X$ if for all $x' \in R(x)$ and for all sequences x_n converging to x, there exists a sequence $x'_n \in R(x_n)$ converging to x'. R is called *upper semicontinuous* (respectively *lower semicontinuous*) if it is upper semicontinuous (respectively, lower semicontinuous) at all $x \in X$. It should be noted that, unlike single valued functions, these two notions of continuity are not equivalent for set valued maps. It can be shown [34] that if R is upper semicontinuous with closed domain and $K \subseteq X$ is a closed set, then $R^{-1}(K)$ is closed, whereas if R is lower semicontinuous and $U \subseteq X$ is an open set, then $R^{-1}(U)$ is open. Notice that the last statement also implies that if R is lower semicontinuous and $K \subseteq X$ is closed, $R^{\ominus 1}(K)$ is closed, since $R^{\ominus 1}(K) = X \backslash R^{-1}(X \setminus K)$.

For a closed subset, $K \subseteq X$, of a finite-dimensional vector space, and a point $x \in K$, we use $T_K(x)$ to denote the *contingent cone* to K at x, i.e., the set of $v \in X$ such that there exists a sequence of real numbers $h_n > 0$ converging to 0 and a sequence of $v_n \in X$ converging to v satisfying

$$\forall n \geq 0, \quad x + h_n v_n \in K.$$

Notice that, if x is in the interior of K, $T_K(x) = X$. The contingent cone is one of many notions of tangent set in nonsmooth analysis; for a full treatment of these notions the reader is referred to [34], [35].

Subsequently we will be dealing with differential inclusions of the form $\dot{x} \in F(x)$, where F: $X \to 2^X$. A *solution* to this differential inclusion over an interval $[0, T]$ starting at $x_0 \in X$ is an absolutely continuous function x: $[0, T] \to X$, such that $x(0) = x_0$ and almost everywhere $\dot{x}(t) \in F(x(t))$. To ensure existence of solutions we will need to impose some standard regularity assumptions on the map F, for example require F to be Marchaud and/or Lipschitz. We say that a map F: $X \to 2^X$ is *Marchaud* if and only if

1) the graph and the domain of F are nonempty and closed;
2) for all $x \in X$, $F(x)$ is convex, compact and nonempty:
3) the growth of F is linear, that is there exists $c > 0$ such that for all $x \in X$

$$\sup\{\|v\| | v \in F(x)\} \leq c(\|x\| + 1).$$

We say F is *Lipschitz* if and only if there exists a constant $\lambda > 0$ (known as the *Lipschitz constant*) such that for all x, $x' \in X$

$$F(x) \subseteq F(x') + \lambda \|x - x'\| B(0, 1).$$

B. Basic Definitions and Assumptions

We will consider hybrid phenomena, in the sense of dynamical phenomena that involve both continuous evolution and discrete transitions. To distinguish the times at which discrete transitions take place we recall the notion of a hybrid time trajectory [12], [37].

Definition 1 (Hybrid Time Trajectory): A hybrid time trajectory $\tau = \{I_i\}_{i=0}^N$ is a finite or infinite sequence of intervals of the real line, such that

- for $i < N$, $I_i = [\tau_i, \tau'_i]$;
- if $N < \infty$, then either $I_N = [\tau_N, \tau'_N]$, or $I_N = [\tau_N, \tau'_N[$, possibly with $\tau'_N = \infty$;
- for all i, $\tau_i \leq \tau'_i = \tau_{i+1}$.

Since the dynamical systems we will consider will be time invariant, we assume, without loss of generality, that $\tau_0 = 0$. The interpretation is that τ_i are the times at which discrete transitions take place. Notice that discrete transitions are assumed to be instantaneous, and therefore multiple discrete transitions may take place at the same time instant (since it is possible for $\tau_i = \tau_{i+1}$). Each hybrid time trajectory, τ, is linearly ordered by the relation $\prec$, which for $t \in [\tau_i, \tau'_i] \in \tau$ and $t' \in [\tau_j, \tau'_j] \in \tau$ is defined by $t \prec t'$ if and only if $t < t'$ or $i < j$; we use $t \preceq t'$ to denote $t \prec t'$, or $t = t'$ and $i = j$. For $t \in \mathbb{R}$, we use $t \in \tau$ as a shorthand notation for "there exists a j such that $t \in [\tau_j, \tau'_j] \in \tau$." For a topological space K we use k: $\tau \rightsquigarrow K$ as a shorthand notation for a map assigning values from K to all $t \in \tau$. Notice that k: $\tau \rightsquigarrow K$ is *not a function* over the interval $\bigcup_i I_i$, since it assigns multiple values to the times $t = \tau_i = \tau'_{i-1}$.

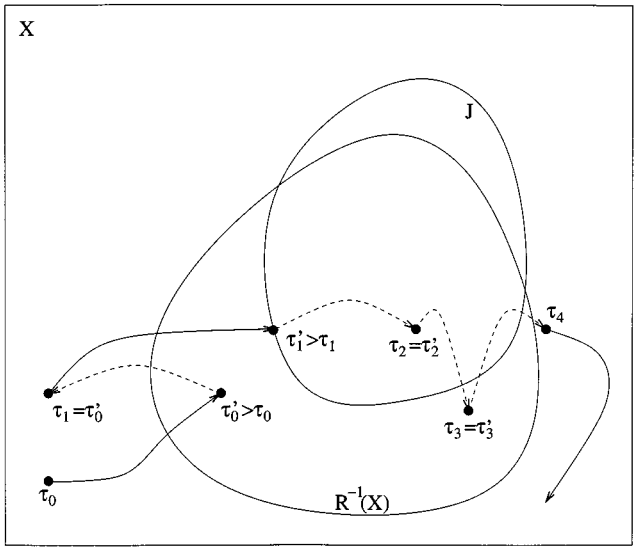

Fig. 1. A run of an impulse differential inclusion (X, F, R, J).

Definition 2 (Impulse Differential Inclusion): An impulse differential inclusion is a collection $H = (X, F, R, J)$, consisting of a finite-dimensional vector space X, a set valued map F: $X \to 2^X$, regarded as a *differential inclusion* $\dot{x} \in F(x)$, a set valued map R: $X \to 2^X$, regarded as a *reset map*, and a set $J \subseteq X$, regarded as a *forced transition set*.

We call $x \in X$ the *state* of the impulse differential inclusion. Subsequently, $I = X \backslash J$ will be used to denote the complement of J.

Impulse differential inclusions can be used to describe hybrid phenomena in the following sense.

Definition 3 (Run of an Impulse Differential Inclusion): A run of an impulse differential inclusion, $H = (X, F, R, J)$, is a pair, (τ, x), consisting of a hybrid time trajectory τ and a map x: $\tau \rightsquigarrow X$, that satisfies

- *Discrete Evolution*: for all i, $x(\tau_{i+1}) \in R(x(\tau_i'))$;
- *Continuous Evolution*: if $\tau_i < \tau_i'$, $x(\cdot)$ is a solution to the differential inclusion $\dot{x} \in F(x)$ over the interval $[\tau_i, \tau_i']$ starting at $x(\tau_i)$, with $x(t) \notin J$ for all $t \in [\tau_i, \tau_i'[$.

We will use $\mathcal{R}_H(x_0)$ to denote the set of all runs of an impulse differential inclusion $H = (X, F, R, J)$ starting at a state $x(\tau_0) = x_0 \in X$. An example of a run of an impulse differential inclusion is shown in Fig. 1; the solid arrows indicate continuous evolution while the dotted arrows indicate discrete transitions. Definition 3 dictates that, along a run the state can evolve continuously according to the differential inclusion $\dot{x} \in F(x)$ until the set J is reached. Moreover, whenever $R(x) \neq \emptyset$, a discrete transition from state x to some state in $R(x)$ may take place. In other words R *enables* discrete transitions [transitions may happen when $R(x) \neq \emptyset$ but do not have to], while J *forces* discrete transitions (transitions must happen when $x \in J$). Notice that if at a state $x \in X$ a transition must happen ($x \in J$) but is not able to ($R(x) = \emptyset$) the system *blocks*, in the sense that there does not exist a run of the impulse differential inclusion starting at x [other than the trivial run $([0, 0], x)$]. Regularity assumptions that prevent such behavior are discussed in detail below.

Definitions 2 and 3 suggest that impulse differential inclusions are intimately related to other modeling languages found in the literature, such as different variants of hybrid automata (HA) [9], [13], [36], [38] and hybrid input/output automata (HIOA) [7]. Many of the properties studied here for impulse differential inclusions can be easily extended to these different classes of models by assuming that the discrete states of the HA and the HIOA are embedded in a finite dimensional vector space and evolve in continuous time under a trivial differential inclusion ($\dot{x} \in \{0\}$). In this context, impulse differential inclusions are more general than the hybrid automata of [36], [38], since they allow nondeterministic evolution in continuous time. They are comparable to the hybrid automata of [9] (without the restrictions imposed for decidability) and [13] (without differentiating between controls and disturbances). Finally, impulse differential inclusions are not as general as HIOA [7], since the latter allow continuous states that take values in infinite dimensional spaces (e.g., can be used to model systems with delays).

C. Classification of Runs

Definition 3 allows for runs defined over finite or infinite "time horizons," runs that take a finite or infinite number of discrete transitions, etc. To distinguish these cases we introduce the following classification.

Definition 4 (Run Classification): A run, (τ, x), of an impulse differential inclusion, H, is called

- *finite*, if τ is a finite sequence ending with a compact interval;
- *finite-open*, if τ is a finite sequence ending with an interval of the form $[\tau_N, \tau_N'[$ with $\tau_N' < \infty$;
- *infinite*, if either τ is an infinite sequence, or $\sum_i (\tau_i' - \tau_i) = \infty$;
- *Zeno*, if it is infinite and $\sum_i (\tau_i' - \tau_i) < \infty$.

We will use $\mathcal{R}_H^\infty(x_0)$ to denote the set of all infinite runs of H starting at x_0 (some of which may be Zeno while others not). Ideally, one would like to be able to extend all runs of an impulse differential inclusion over arbitrarily long time horizons. In certain cases, however, this may not be possible; an impulse differential inclusion may produce runs that escape to infinity in finite time along continuous evolution, runs that block, and Zeno runs (refer to Fig. 2).

In the case of *finite escape time*, the run is defined over a finite sequence τ ending in a right open interval, $[\tau_N, \tau_N'[$ with $\tau_N' < \infty$ and $\lim_{t \to \tau_N} \|x(t)\| = \infty$. This situation can be prevented by imposing regularity assumptions on F.

Proposition 1: If F is Marchaud, every finite-open run of the impulse differential inclusion $H = (X, F, R, J)$ can be extended to a finite run.

The proof is straight forward: the claim follows from standard results for existence of solutions of differential inclusions [30], and the fact that along continuous evolution over an interval $[\tau_i, \tau_i']$ with $\tau_i < \tau_i'$, $x(t) \notin J$ is only required for $t \in [\tau_i, \tau_i'[$. The Marchaud assumption on F will be imposed throughout this paper to ensure the existence of runs. In Section III, additional technical requirements will be imposed on the map R and the set J to allow us to characterize viability and invariance.

In the case of *blocking*, the run is defined over a finite sequence τ, ending in a closed interval $[\tau_N, \tau_N']$ such that at

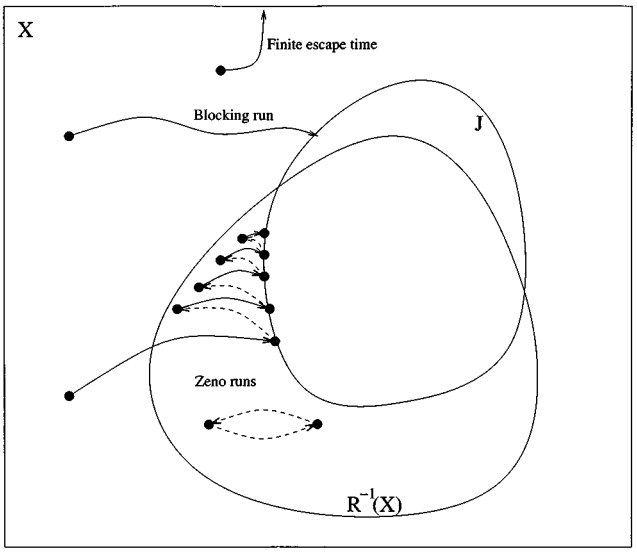

Fig. 2. Examples of Zeno, blocking and finite escape runs.

$x(\tau'_N)$ neither continuous nor discrete evolution are possible, i.e., $x(\tau'_N) \in J$ and $R(x(\tau'_N)) = \emptyset$. To prevent this situation we introduce the following assumption.

Assumption 1: An impulse differential inclusion (X, F, R, J) is said to satisfy *Assumption 1* if $J \subseteq R^{-1}(X)$ and, if J is open (hence, $I = X \backslash J$ is closed), $F(x) \cap T_I(x) \neq \emptyset$, for all $x \in I \backslash R^{-1}(X)$.

Roughly speaking, Assumption 1 implies that if for some $x \in X$ continuous evolution is not possible (because x is either in J or is forced to enter J along all solutions of the differential inclusion) then a discrete transition has to be possible ($R(x) \neq \emptyset$). It can be shown that under Assumption 1 and some additional technical requirements, every finite run of the impulse differential inclusion can be extended to an infinite run. The proof will be deferred for the time being, since it follows as a corollary of the viability theorems given below. Assumption 1 will not be imposed as a standing assumption, whenever it is invoked it will be clearly stated.

Finally, in the case of a *Zeno run*, the system takes an infinite number of discrete transitions in a finite amount of time. This is, in a sense, a discrete version of finite escape time since the run can effectively be defined only over a time horizon of the form $[\tau_0, \lim_{i \to \infty} \tau'_i[$. Zeno runs are somewhat more difficult to characterize and eliminate [38], [39]; some sufficient conditions will be given in Section III.

D. Viability Definitions

Questions of reachability have been widely studied in the hybrid system literature. Roughly speaking, a verification problem for a *reachability* (or *safety*) specification involves proving that the state of the system never leaves a certain "good" part, $G \subseteq X$, of the state space (or, equivalently, never enters a "bad" part, $B \subseteq X$, of the state space). The solution to this problem involves computing the set of states that can be reached from a set of initial conditions by finite runs of the hybrid system. Theoretical methods have been developed for performing these computations [5], [6], [17], [7], [8], [18], [9], some of them supported by automated or semi-automated tools [20], [22], [23], [26], [24], [25], [29], [21]. If control inputs are available, one can also define reachability controller synthesis problems, where the objective is to choose the values of the control inputs such that the run of the system never leaves the good set, G [15], [10]–[14], [16]. The solution to reachability controller synthesis problems comes down to computing controlled invariant subsets of G [12], [30], that is subsets of G for which there exist a choice for the control such that the runs of the system that start in the set stay in the set for ever.

For impulse differential inclusions, reachability questions can be characterized by viability constraints.

Definition 5 (Viable Run): A run, (τ, x) of an impulse differential inclusion, $H = (X, F, R, J)$, is called viable in a set $K \subseteq X$ if for all $t \in \tau$, $x(t) \in K$.

Notice that the definition of a viable run requires the state to remain in the set K throughout the run, along continuous evolution up until and including the state before discrete transitions, as well as after discrete transitions. Based on the notion of a viable run, one can define two different classes of sets.

Definition 6 (Viable and Invariant Set): A set $K \subseteq X$ is called viable under an impulse differential inclusion, $H = (X, F, R, J)$, if for all $x_0 \in K$ there exists an infinite run, $(\tau, x) \in \mathcal{R}_H^\infty(x_0)$, viable in K. K is called invariant under the impulse differential inclusion, if for all $x_0 \in K$ all runs $(\tau, x) \in \mathcal{R}_H(x_0)$ are viable in K.

In the cases where an impulse differential inclusion fails to satisfy a given viability or invariance requirement, one would like to establish sets of initial conditions (if any) for which the requirement will be satisfied. This notion can be characterized in terms of viability and invariance kernels.

Definition 7 (Viability and Invariance Kernel): The viability kernel, $Viab_H(K)$ of a set $K \subseteq X$ under an impulse differential inclusion $H = (X, F, R, J)$ is the set of states $x_0 \in X$ for which there exists an infinite run, $(\tau, x) \in \mathcal{R}_H^\infty(x_0)$, viable in K. The invariance kernel, $Inv_H(K)$ of $K \subseteq X$ under $H = (X, F, R, J)$ is the set of states $x_0 \in X$ for which all runs $(\tau, x) \in \mathcal{R}_H(x_0)$ are viable in K.

Notice that by definition $Viab_H(K) \subseteq K$ and $Inv_H(K) \subseteq X$, but in general the two sets are incomparable.

E. Special Cases and Alternative Characterizations

Impulse differential inclusions are extensions of differential inclusions and discrete time systems over finite dimensional vector spaces (see for example [30]). A differential inclusion

$$\dot{x} \in F(x)$$

over a finite dimensional vector space X can be thought of as an impulse differential inclusion, (X, F, R, J), with $R(x) = \emptyset$ for all $x \in X$ and $J = \emptyset$. Likewise, a discrete time system

$$x_{k+1} \in R(x_k)$$

can be thought of as an impulse differential inclusion, $H = (X, F, R, J)$, with $F(x) = \{0\}$ for all $x \in X$ and $J = X$. The situation where a nonzero amount of time elapses between two transitions of the discrete system can also be easily encoded,

by letting $J = \emptyset$. The two formulations are equivalent from the point of view of viability, under the assumption that the time between any two transitions is finite. As expected, the viability and invariance conditions developed below for impulse differential inclusions reduce to the corresponding conditions for differential inclusions and discrete systems, when restricted to these special cases.

In the control literature, differential inclusions and discrete-time systems are frequently used to model continuous and discrete control systems. The continuous control system

$$\dot{x} = f(x, v), \quad v \in V(x)$$

with $x \in \mathbb{R}^n$, $v \in \mathbb{R}^m$, f: $\mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ and V: $\mathbb{R}^n \to 2^{\mathbb{R}^m}$ can be though of as a differential inclusion

$$\dot{x} \in F(x) = \{f(x, v) | v \in V(x)\}.$$

Likewise, the discrete-time control system

$$x_{k+1} = r(x_k, v_k), \quad v_k \in V(x_k)$$

with $x_k \in \mathbb{R}^n$, $v_k \in \mathbb{R}^m$, r: $\mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ and V: $\mathbb{R}^n \to 2^{\mathbb{R}^m}$ can be though of as

$$x_{k+1} \in R(x_k) = \{r(x_k, v) | v \in V(x_k)\}.$$

Extending this interpretation to the hybrid domain, an impulse differential inclusion can be though of as a hybrid control system. In this context, the relation between invariance/viability and verification/controller synthesis for reachability specifications becomes clearer. Recall that a reachability specification is encoded by a "good" set of states, G; one would like to ensure that the state remains in G along all runs of the system (verification) or, if control inputs are available, choose the inputs so that the state remains in G (controller synthesis). If the inputs, v, represent uncontrollable disturbances and the good set, G, can be shown to be an invariant set (in the sense of Definition 6), then it is easy to check that the hybrid system satisfies the safety specification encoded by G, in the sense that any run that starts in G it remains in G for ever. If G is not invariant then its invariance kernel is the largest set of initial conditions for which the safety specification is satisfied. Alternatively, if the inputs, v, represent controls, viability of G can be interpreted as controlled invariance: if G is viable, then it is possible to design a controller for the hybrid control system such that all runs of the closed loop system that start in G remain in G for ever. If G is not viable, then its viability kernel is the maximal controlled invariant subset of G.

The runs of an impulse differential inclusion can also be interpreted in the context of impulse control by introducing the *switching map*, S: $X \to 2^X$, defined by

$$S(x) = \{x' \in X | \exists\, y \in R(x), \quad x' = y - x\}.$$

Proposition 2: If (τ, x) is a run of an impulse differential inclusion $H = (X, F, R, J)$, then for all $t \in \tau$

$$x(t) \in \{x(\tau_0)\} + \sum_{\{i | \tau_i' \prec t\}} S(x(\tau_i')) + \int_0^t F(x(t'))\, dt'. \quad (1)$$

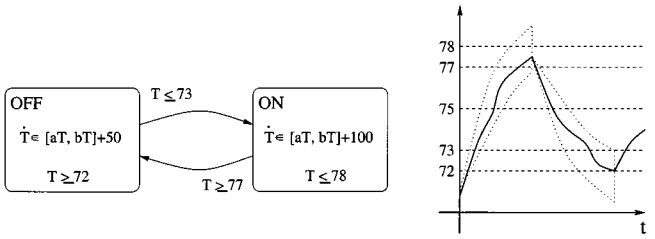

Fig. 3. Thermostat system.

Moreover, if $J = \emptyset$, then all pairs (τ, x) with τ a hybrid time trajectory and x: $\tau \rightsquigarrow X$, that satisfy (1) are runs of H.

If $J = \emptyset$ (there are no forced transitions), the impulse differential inclusion H can also be denoted symbolically as

$$\dot{x}(t) \in F(x(t)) + \sum_{i \geq 0} S(x(\tau_i'))\, \delta(\tau_i')$$

where $\delta(t)$ is the Dirac measure at time t and, as before, $\tau_0' \leq \tau_1' \leq \cdots \leq \tau_i' \leq \cdots$ denotes a sequence of switching times and $x(\tau_i')$ a sequence of elements of X. This notation can be misleading since it may convey the impression that switching times are prescribed *a priori*. We mention it, however, to establish a connection with the notation used in [40].

F. Examples

To illustrate how impulse differential inclusions can be used to characterize hybrid phenomena we consider two simple examples from the hybrid systems literature: a thermostat system and a bouncing ball system [41]. We will return to these examples in Section V, to illustrate the viability and invariance conditions for impulse differential inclusions.

1) Thermostat: The thermostat system (adapted from a simpler example given in [41]) models a room whose temperature, T, is controlled by a thermostat. The thermostat tries to keep the room temperature at 75 degrees by switching a heater on and off. When the heater is on the temperature of the room increases, while when the heater is off the temperature of the room decreases. To avoid modeling the details of the heat transfer process, we assume that the exact rate of increase or decrease of the temperature is unknown and may change with time, but that its value can be bounded by known constants at all times. To prevent the heater from chattering between on and off, the thermostat allows the temperature to fluctuate slightly about the desired set point. To avoid modeling the details of the switching process, we assume that the heater is switched on somewhere between 72 and 73 degrees and is switched off somewhere between 77 and 78 degrees, but the exact switching point is unknown and may change in time. A typical trajectory of the system, as well as a hybrid model in the intuitive directed graph notation, are shown in Fig. 3.

The thermostat system can be modeled by an impulse differential inclusion, $H_T = (X_T, F_T, R_T, J_T)$ with two state variables, $x = (x_1, x_2)$: the current room temperature $x_1 = T$ and the steady state toward which the temperature is converging x_2

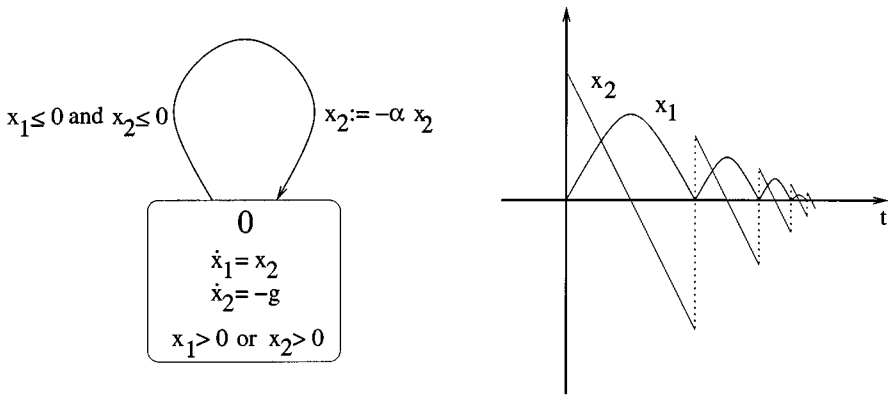

Fig. 4. Bouncing ball.

(which of course depends on whether the heater is on or off). Therefore, $X_T = \mathbb{R}^2$, and

$$F_T(x_1, x_2) = ([a(x_1 - x_2), b(x_1 - x_2)], 0)$$

$$R_T(x_1, x_2) = \begin{cases} (x_1, 150 - x_2) & \text{if } (x_1 \geq 77 \text{ and } x_2 \geq 75) \\ & \text{or } (x_1 \leq 73 \text{ and } x_2 \leq 75) \\ \emptyset & \text{otherwise} \end{cases}$$

$$J_T = \{x \in X_T | (x_1 \geq 78 \text{ and } x_2 \geq 75) \text{ or } (x_1 \leq 72 \text{ and } x_2 \leq 75)\}$$

with $a \leq b < 0$. Notice that the resulting impulse differential inclusion can exhibit many more behaviors than the physical system in question, since x_2 is not restricted to the set $\{50, 100\}$. However, under the additional assumption that $x(\tau_0) \in \mathbb{R} \times \{50, 100\}$ it is easy to show that the behavior of the impulse differential inclusion is indeed the expected (see Section V).

2) Bouncing Ball: The bouncing ball system [38], [41] models an elastic ball bouncing on a level surface under the effect of gravity (Fig. 4). We assume that the ball looses a fraction of its kinetic energy with each bounce.

The vertical motion of the ball can be captured by an impulse differential inclusion, $H_B = (X_B, F_B, R_B, J_B)$ with two state variables, the height of the ball, x_1 and its velocity in the vertical direction, x_2. Therefore, $X_B = \mathbb{R}^2$ and

$$F_B(x_1, x_2) = (x_2, -g)$$

$$R_B(x_1, x_2) = \begin{cases} (x_1, -\alpha x_2) & \text{if } x_1 \leq 0 \text{ and } x_2 \leq 0 \\ \emptyset & \text{otherwise} \end{cases}$$

$$J_B = \{x \in X_B | x_1 \leq 0 \text{ and } x_2 \leq 0\}$$

where g represents the acceleration due to gravity and $\alpha^2 \in [0, 1]$ the fraction of energy lost with each bounce. Again the impulse differential inclusion can demonstrate many more behaviors than the physical system in question, since x_1 is not assumed to be nonnegative. However, under the additional assumption that $x(\tau_0) \in [0, \infty) \times \mathbb{R}$ it is easy to show that the behavior of the impulse differential inclusion is indeed the expected (see Section V).

III. Viability and Invariance Conditions

Having motivated the importance of viability and invariance properties of impulse differential inclusions to the analysis and controller synthesis of hybrid systems, we give conditions that allow one to determine whether a given set of states is viable or invariant. The viability conditions naturally lead to conditions under which the existence of infinite runs of an impulse differential inclusion is guaranteed for all initial conditions.

A. Viability Conditions

The viability conditions for impulse differential inclusions involve the notion of "viability with target." This notion was introduced in [42] for continuous differential inclusions, motivated partly by target optimal control problems (see for example [43]). Viability with target provides conditions under which solutions of $\dot{x} \in F(x)$ that remain viable in a set K until they reach a target set C exist. For completeness, conditions are summarized below.

Lemma 1: Consider a Marchaud map $F\colon X \to 2^X$ and two closed sets $K \subseteq X$ and $C \subseteq X$. For all $x_0 \in K$, there exists a solution of $\dot{x} \in F(x)$ starting at x_0 which is either

1) defined over $[0, \infty[$ with $x(t) \in K$ for all $t \geq 0$;
2) defined over $[0, T]$ for some $T \geq 0$, with $x(T) \in C$ and $x(t) \in K$ for all $t \in [0, T]$;

if and only if for all $x \in K \backslash C$, $F(x) \cap T_K(x) \neq \emptyset$.

The proof when F is Lipschitz is given in [42]. The proof when F is Marchaud can be found in the Appendix. Notions related to viability with target have also been studied in the context of branching time temporal logics, such as CTL, primarily from a discrete point of view. The most closely related notion is *weak until*, sometimes denoted by $\exists \mathcal{W}$. The more common notion of *possibly until* (usually denoted by $\exists \mathcal{U}$) is slightly stronger; in our context it would exclude solutions that stay in K forever, without ever reaching C (see, for example [9]). (Ab)using the CTL notation, one could think of the property "K is viable with target C" in terms of the CTL formula $\{\exists \Box (x \in K)\} \vee \{(x \in K) \exists \mathcal{U} (x \in C)\}$.

The conditions characterizing viable sets depend on whether the set J is open or closed. In the case where J is closed, we have the following.

Theorem 1 (Viability Conditions, J Closed): Consider an impulse differential inclusion $H = (X, F, R, J)$ such that F

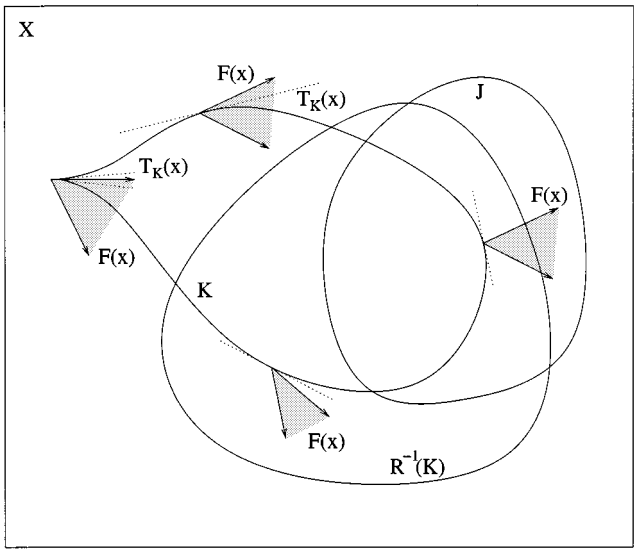

Fig. 5. K viable under $H = (X, F, R, J)$.

is Marchaud, R is upper semicontinuous with closed domain and J is closed. A closed set $K \subseteq X$ is viable under H if and only if

1) $K \cap J \subseteq R^{-1}(K)$;
2) $\forall x \in K \backslash R^{-1}(K), F(x) \cap T_K(x) \neq \emptyset$.

In words, the conditions of the theorem require that for any state $x \in K$, whenever a discrete transition has to take place ($x \in K \cap J$), a transition back into K is possible ($R(x) \cap K \neq \emptyset$), and whenever a discrete transition to another point in K is not possible ($R(x) \cap K = \emptyset$) continuous evolution that remains in K has to be possible [encoded by the local viability condition $F(x) \cap T_K(x) \neq \emptyset$]. Just as with viability conditions for differential inclusions, this last condition can equivalently be given in terms of the *proximal normal cone* [30]. Going through the proof of Theorem 1 it becomes apparent that the assumptions on R are only used to show that the set $R^{-1}(K)$ is closed. Therefore, the theorem still holds even if R is not upper semicontinuous with closed domain, but $R^{-1}(K)$ happens to be closed.

Similar conditions characterize viability when the set J is open, or, in other words, the set $I = X \backslash J$ is closed.

Theorem 2 (Viability Conditions, J Open): Consider an impulse differential inclusion $H = (X, F, R, J)$ such that F is Marchaud, R is upper semicontinuous with closed domain and J is open. A closed set $K \subseteq X$ is viable under H if and only if

1) $K \cap J \subseteq R^{-1}(K)$, and
2) $\forall x \in (K \cap I) \backslash R^{-1}(K), F(x) \cap T_{K \cap I}(x) \neq \emptyset$.

The first condition is the same as for the case where J is closed: whenever a discrete transition has to take place from a point in K, a transition back into K must be possible. The second condition requires that whenever a discrete transition into K is not possible, there should be a solution to the differential inclusion that stays in K and avoids J. The second condition can again be given equivalently in terms of the proximal normal cone and the requirements on R can be relaxed, as noted above. Fig. 5 suggests how the conditions of Theorems 1 and 2 can be interpreted pictorially.

As noted in Section II , continuous differential inclusions and discrete time systems can be thought of as special cases of impulse differential inclusions. Therefore, one would expect that the viability conditions of Theorems 1 and 2 will reduce to the standard viability conditions given in the literature for these special cases. Indeed, one can show that the conditions of the above theorems imply the following version of the conditions of [30].

Corollary 1: Consider a Marchaud map F: $X \rightarrow 2^X$, an arbitrary map R: $X \rightarrow 2^X$, and a closed set $K \subseteq X$.

1) K is viable under the differential inclusion $\dot{x} \in F(x)$ if and only if for all $x \in K$, $F(x) \cap T_K(x) \neq \emptyset$.
2) K is viable under the discrete time system $x_{k+1} \in R(x_k)$ if and only if for all $x \in K$, $R(x) \cap K \neq \emptyset$.

B. Existence of Runs

Notice that Assumption 1 does not need to be added explicitly to Theorems 1 and 2, since the part of it that is essential to guarantee the existence of a run viable in K is implied by the conditions of the theorems. Conditions that guarantee the existence of runs for impulse differential inclusions can be deduced as a corollary of Theorems 1 and 2.

Corollary 2: Consider an impulse differential inclusion $H = (X, F, R, J)$ such that F is Marchaud, and R is upper semicontinuous with closed domain and J is either open or closed. Every finite run of H can be extended to an infinite run if and only if H satisfies Assumption 1.

To see this, replace K by the (closed) set X in Theorems 1 and 2. The first condition of both theorems is then part of Assumption 1. In the case where J is closed, the second condition of Theorem 1 is trivially satisfied, since for all $x \in X$, $T_X(x) = X$ and $F(x) \neq \emptyset$ (recall that F is Marchaud). In the case were J is open, the second condition of Theorem 2 is part of Assumption 1.

Corollary 2 can be used to ensure that a model for a physical process given in the impulse differential inclusion framework produces infinite runs for all initial conditions. Ideally, one would also like these runs to be non-Zeno. Set valued analysis techniques can be used to derive conditions under which this is indeed the case. A condition for a simple case that will be useful in the examples is given below; more general conditions are the topic of on-going research.

Proposition 3: Consider an impulse differential inclusion $H = (X, F, R, J)$ such that F is Marchaud and R has closed domain. Assume that H satisfies Assumption 1, that $R^{-1}(X) \cap R(X) = \emptyset$, and that $R(X)$ is compact. Then all infinite runs of H (which exist thanks to Corollary 2) are non-Zeno.

Analogs of Proposition 3 can be obtained with any other set of conditions that provide a lower bound between transition times.

C. Invariance Conditions

The conditions for invariance make use of the notion of "invariance with target" for continuous differential inclusions. Invariance with target involves conditions ensuring that all solutions of $\dot{x} \in F(x)$ remain in a set K until they reach a target set, C (in subsequent discussion, J will play the role of C). The in-

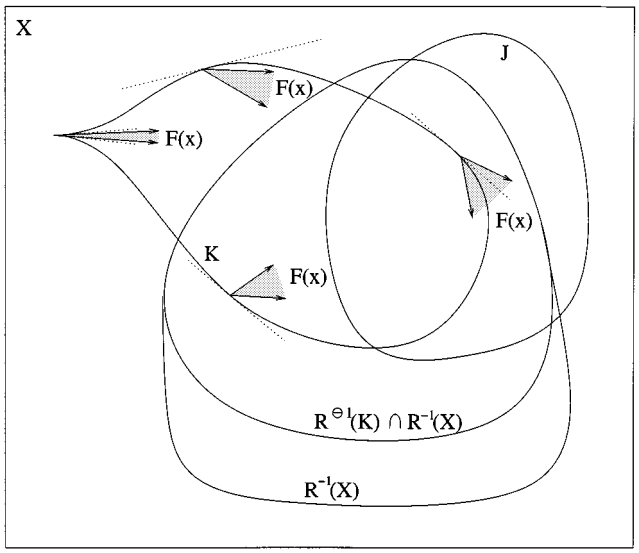

Fig. 6. K invariant under (X, F, R, J).

variance with target conditions are interesting in their own right, so they are summarized separately in the following lemma.

Lemma 2: Consider a Marchaud and Lipschitz map F: $X \to 2^X$ and two closed sets K and C. All solutions of $\dot{x} \in F(x)$ starting at some $x_0 \in K$ are either

1) defined over $[0, \infty[$ with $x(t) \in K$ for all $t \geq 0$;
2) defined over $[0, T]$ with $x(T) \in C$ and $x(t) \in K$ for all $t \in [0, T]$;

if and only if for all $x \in K \backslash C$, $F(x) \subseteq T_K(x)$.

Lemma 2 allows us to prove the following invariance theorem for impulse differential inclusions.

Theorem 3 (Invariance Conditions): Consider an impulse differential inclusion $H = (X, F, R, J)$ such that F is Marchaud and Lipschitz and J is closed. A closed set $K \subseteq X$ is invariant under H if and only if

1) $R(K) \subseteq K$;
2) $\forall x \in K \backslash J$, $F(x) \subseteq T_K(x)$.

In words, the conditions of the theorem require that for all $x \in K$, if a discrete transition is possible ($x \in R^{-1}(X)$), then all states after the transition are also in K ($R(x) \subseteq K$), whereas if continuous evolution is possible ($x \notin J$) then all possible solutions of the differential inclusion $\dot{x} \in F(x)$ remain in K [characterized here by the invariance condition $F(x) \subseteq T_K(x)$]. As for continuous differential inclusions, the second condition can also be characterized equivalently in terms of the proximal normal cone. Fig. 6 suggests how the conditions of Theorem 3 can be interpreted pictorially.

Notice that no assumptions need to be imposed on R. Strictly speaking, Theorem 3 remains true even without Assumption 1; if the impulse differential inclusion has no runs for certain initial conditions in K, then, vacuously, all runs that start at these initial conditions are viable in K. In practice, it may be prudent to impose Assumption 1, to ensure the results are meaningful.

As before, one would expect the above invariance conditions to reduce to the standard invariance conditions for continuous differential inclusions and discrete time systems found in the literature. Indeed, one can show that the above conditions imply the following conditions of [30].

Corollary 3: Consider a Marchaud and Lipschitz map F: $X \to 2^X$, a map R: $X \to 2^X$, and a closed set $K \subseteq X$.

1) K is invariant under the differential inclusion $\dot{x} \in F(x)$ if and only if for all $x \in K$, $F(x) \subseteq T_K(x)$.
2) K is invariant under the discrete-time system $x_{k+1} \in R(x_k)$ if and only if for all $x \in K$, $R(x) \subseteq K$.

IV. Viability and Invariance Kernels

A. Characterization of the Viability Kernel

If K is not viable under an impulse differential inclusion H, one would like to characterize the largest subset of K which is viable under H. This set turns out to be the viability kernel of K under the impulse differential inclusion. The viability kernel of an impulse differential inclusion can be characterized in terms of the notion of the viability kernel with target for a continuous differential inclusion. For a differential inclusion $\dot{x} \in F(x)$, the viability kernel of a set K with target C, $Viab_F(K, C)$, is defined as the set of states for which there exists a solution to the differential inclusion that remains in K either forever, or until it reaches C. The following lemma summarizes the basic properties of the viability kernel with target.

Lemma 3: Consider a Marchaud map F: $X \to 2^X$ and two closed subsets of X, K and C. $\mathrm{Viab}_F(K, C)$ is the largest closed subset of K satisfying the conditions of Lemma 1.

For the proof, the reader is referred to the Appendix and, for the Lipschitz case, to [42] [where an approximation scheme for computing $Viab_F(K, C)$ is also given]. Notice that, by definition

$$K \cap C \subseteq Viab_F(K, C) \subseteq K.$$

Using this notion, one can give an alternative characterization of the sets that are viable under an impulse differential inclusion, as fixed points of an appropriate operator. For an impulse differential inclusion $H = (X, F, R, J)$, consider the operator $Pre_H^{\exists}$: $2^X \to 2^X$ defined by

$$Pre_H^{\exists}(K) = Viab_F\left(K \cap I, R^{-1}(K)\right) \cup \left(K \cap R^{-1}(K)\right).$$

Recall that $I = X \backslash J$.

Lemma 4: Consider an impulse differential inclusion $H = (X, F, R, J)$ such that F is Marchaud, R is upper semicontinuous with closed domain, and J is open. A closed set $K \subseteq X$ is viable under H if and only if it is a fixed point of the operator $Pre_H^{\exists}$.

Theorem 4 (Viability Kernel): Consider an impulse differential inclusion $H = (X, F, R, J)$ such that F is Marchaud, R is upper semicontinuous with closed domain and compact images, and J is open. The viability kernel of a closed set $K \subseteq X$ under H is the largest closed subset of K viable under H, that is, the largest closed fixed point of $Pre_H^{\exists}$ contained in K.

The assumption can again be modified somewhat, by requiring that R has compact images and $R^{-1}(K)$ is closed for all closed sets $K \subseteq X$. It should be stressed that the conditions of Theorem 4 ensure that for all initial conditions in the viability kernel infinite runs of the impulse differential inclusion exist,

but do not ensure that these runs will extend over an infinite time horizon; all runs starting at certain initial conditions in the viability kernel may turn out to be Zeno. To ensure that the runs extend over an infinite time horizon, assumptions like the ones listed in Proposition 3 need to be added to the theorem.

The proof of Theorem 4 is based on the following abstract algorithm, which follows the standard iterative characterization of the greatest fixed point of a monotone operator on a complete lattice [44].

Algorithm 1 (Viability Kernel Approx.)
initialization: $K_0 = K,\ i = 0$
repeat
$K_{i+1} = Pre_H^{\exists}(K_i)$
$i = i + 1$
until $K_i = K_{i-1}$

As shown in the proof of Theorem 4, the sets K_i form a sequence of nested closed sets. Given a set K_i it may, in general, be impossible to compute its successor, K_{i+1} effectively (i.e., in finite time). An in depth study of numerical methods for approximating the computation can be found in [33]. Even in cases where exact computation of the sets K_i is possible, the Viability Kernel Approximation algorithm may still fail to terminate in a finite number of steps. However, the sets K_i generated by the algorithm provide successively better estimates of the viability kernel in the following sense.

Lemma 5: Consider an impulse differential inclusion $H = (X, F, R, J)$ such that F is Marchaud, R is upper semicontinuous with closed domain and J is open. Let $K \subseteq X$ be a closed set and K_i be the sequence of sets generated by the Viability Kernel Approximation algorithm. Then $x_0 \in K_N$ if and only if there exists a run $(\tau, x) \in \mathcal{R}_H(x_0)$ that remains in K for at least N jumps.

"Remains in K for at least N jumps" is meant to be interpreted as "either (τ, x) is infinite and $x(t) \in K$ for all $t \in \tau$, or the sequence τ consists of at least $N+1$ intervals and $x(t) \in K$ for all $t \preceq \tau_{N+1}$" (up to and including τ_{N+1}).

Ideally, one would also like to be able to characterize the viability kernel when J is closed. Unfortunately, a precise characterization like the one given in Theorem 4 turns out to be much more difficult in this case. For example, it is easy to show that if J is closed, the viability kernel may be neither an open nor a closed set. Consider the impulse differential inclusion $H = (X, F, R, J)$ with $X = \mathbb{R}$, $F(x) = \{0\}$ for all x, $R(x) = \{2\}$ if $x = 1$, $R(x) = \emptyset$ if $x \neq 1$ and $J = [1, \infty[$. It is easy to check that F is Marchaud and R is upper semicontinuous with closed domain, but J is closed. One can see that the viability kernel of the closed set $K = [0, 1]$ is $Viab_H(K) = [0, 1[$, which is neither open nor closed.

B. Characterization of the Invariance Kernel

If K is not invariant under an impulse differential inclusion H, one would like to characterize the largest subset of K which is invariant under H. This turns out to be the invariance kernel of K under the impulse differential inclusion. The invariance kernel can be characterized using the notion of the invariance kernel with target for continuous differential inclusions. For a differential inclusion $\dot{x} \in F(x)$, the invariance kernel of a set K with target C, $Inv_F(K, C)$ is defined as the set of states for which all solutions to the differential inclusion remain in K either for ever, of until they reach C. The following lemma summarizes the basic properties of the invariance kernel with target.

Lemma 6: Consider a Marchaud and Lipschitz map $F: X \to 2^X$ and two closed subsets of X, K and C. $Inv_F(K, C)$ is the largest closed subset of K satisfying the conditions of Lemma 2.

Notice that, by definition

$$K \cap C \subseteq Inv_F(K, C) \subseteq K.$$

Using the notion of invariance kernel with target, one can give an alternative characterization of the sets that are invariant under an impulse differential inclusion, as fixed points of an operator. Given an impulse differential inclusion $H = (X, F, R, J)$, consider the operator $Pre_H^{\forall}: 2^X \to 2^X$ defined by

$$Pre_H^{\forall}(K) = Inv_F(K, J) \cap R^{\ominus 1}(K).$$

Lemma 7: Consider an impulse differential inclusion $H = (X, F, R, J)$ such that F is Marchaud and Lipschitz, R is lower semicontinuous, and J is closed. A closed set $K \subseteq X$ is invariant under H if and only if it is a fixed point of the operator $Pre_H^{\forall}$.

Theorem 5 (Invariance Kernel): Consider an impulse differential inclusion $H = (X, F, R, J)$ such that F is Marchaud and Lipschitz, R is lower semicontinuous and J is closed. The invariance kernel of a closed set $K \subseteq X$ under H is the largest closed subset of K invariant under H, that is, the largest, closed fixed point of $Pre_H^{\forall}$ contained in K.

Again the proof of Theorem 5 makes use of the sequence of sets generated by the following abstract algorithm.

Algorithm 2 (Invariance Kernel Approx.)
initialization: $K_0 = K,\ i = 0$
repeat
$K_{i+1} = Pre_H^{\forall}(K_i)$
$i = i + 1$
until $K_i = K_{i-1}$

At each step, the algorithm computes the set of states for which all solution of the differential inclusion $\dot{x} \in F(x)$ stay in the K_i until they reach J. K_{i+1} is then the subset of those states for which if a transition is possible, the state after the transition is also in K_i.

Lemma 8: Consider an impulse differential inclusion $H = (X, F, R, J)$ such that F is Marchaud and Lipschitz, R is lower semicontinuous and J is closed. Let $K \subseteq X$ be a closed set and K_i be the sequence of sets generated by the Invariance Kernel Approximation algorithm. If $x_0 \in K_N$, then all runs $(\tau, x) \in \mathcal{R}_H(x_0)$ remain in K for at least $\lfloor N/2 \rfloor$ jumps.

$\lfloor N/2 \rfloor$ is the greatest integer not exceeding $N/2$. "Remain in K for at least $\lfloor N/2 \rfloor$ jumps" is to be interpreted as in Lemma 5.

Ideally, one would also like to characterize the invariance kernel in the case where J is open. Unfortunately a precise characterization in this case turns out to be difficult. One can

again construct counter examples that suggest that the invariance kernel may be neither an open nor a closed set. Consider the impulse differential inclusion $H = (X, F, R, J)$ with $X = \mathbb{R}$, $F(x) = \{1\}$ for all x, $R(x) = \{x\}$ and $J =]-\infty, 1[$. F is Marchaud and Lipschitz and R is lower semicontinuous, but J is open. One can see that the invariance kernel of the closed set $K = [0, 1]$ is $Inv_H(K) = [0, 1[$, which is neither open nor closed.

V. Examples

We now return to the examples introduced in Section II and show how the viability and invariance conditions can be used to establish useful properties of the impulse differential inclusion models of these systems. The examples are simple and do not allow us to demonstrate the full power of the theoretical results presented above. More challenging examples are studied in [33] using numerical implementations of the abstract algorithms presented above. We are currently applying the same techniques to examples from collision avoidance and aerodynamic envelope protection for aircraft.

A. The Thermostat System

The viability and invariance conditions can be used to show that the impulse differential inclusion H_T proposed for modeling the thermostat system is indeed a reasonable model for the underlying physical process. First note that F is both Marchaud and Lipschitz and R is both upper and lower semicontinuous and has closed domain.

Proposition 4: The impulse differential inclusion H_T satisfies the following properties:

1) for all $x_0 \in X_T$, $\mathcal{R}^{\infty}_{H_T}(x_0) \neq \emptyset$;
2) the set $K = \{x \in X_T | x_2 \in \{50, 100\}\}$ is invariant;
3) for all $x_0 \in K$, all $(\tau, x) \in \mathcal{R}^{\infty}_{H_T}(x_0)$ are non-Zeno.

Proof: To show that infinite runs exist for all initial conditions recall that J_T is closed and

$$\begin{aligned} R^{-1}(X) &= \{x \in X_T | x_1 \geq 77 \text{ and } x_2 \geq 75\} \\ &\cup \{x \in X_T | x_1 \leq 73 \text{ and } x_2 \leq 75\} \\ &\supseteq \{x \in X_T | x_1 \geq 78 \text{ and } x_2 \geq 75\} \\ &\cup \{x \in X_T | x_1 \leq 72 \text{ and } x_2 \leq 75\} = J_T. \end{aligned}$$

Therefore, H_T satisfies Assumption 1, and the claim follows by Corollary 2.

To show that K is invariant notice that R_T leaves x_1 unchanged and maps $x_2 = 50$ to $x_2 = 100$ and vice versa. Moreover

$$\begin{aligned} K \backslash J_T = &\{x \in X_T | x_1 > 72 \text{ and } x_2 = 50\} \\ &\cup \{x \in X_T | x_1 < 78 \text{ and } x_2 = 100\}. \end{aligned}$$

Therefore, for all $x \in K \backslash J_T$, $T_K(x) = \{v \in X_T | v_2 = 0\} \supseteq F_T(x)$. The claim follows by Theorem 3. ∎

Finally, to show that all infinite runs starting in K are non-Zeno let

$$D = \inf_{x \in R(X) \cap K,\, y \in R^{-1}(X) \cap K} \|x - y\|.$$

It is easy to check that $D > 0$. From this point on the proof is the same as the proof of Proposition 3. ∎

Using the viability tools one can also show that the thermostat manages to keep the temperature of the room within the desired levels.

Proposition 5: The set $L = \{x \in X_T | x_1 \in [73, 77]\}$ is viable, while the set $M = \{x \in X_T | x_1 \in [72, 78]\}$ is invariant.

Proof: $L \cap J_T = \emptyset$, therefore the first condition of Theorem 1 is vacuously satisfied for L. Moreover

$$\begin{aligned} L \backslash R^{-1}(L) = &\{x \in X_T | x_1 > 73 \text{ or } x_1 = 73 \text{ and } x_2 > 75\} \\ &\cup \{x \in X_T | x_1 < 77 \text{ or } x_1 = 77 \text{ and } x_2 < 75\}. \end{aligned}$$

For x such that $73 < x_1 < 77$, $T_L(x) = X_T$ and therefore $F_T(x) \cap T_L(x) = F_T(x) \neq \emptyset$. For x such that $x_1 = 73$ and $x_2 > 75$

$$\begin{aligned} F_T(x) &= \{v \in X_T | v_1 \in [a(x_1 - x_2), b(x_1 - x_2)]\} \\ &\subseteq \{v \in X_T | v_1 > 0\} = T_K(x) \end{aligned}$$

(recall that $a \leq b < 0$). A similar conclusion holds if $x_1 = 77$ and $x_2 < 75$. The claim that L is viable follows by Theorem 1.

To see that M is invariant, recall that R_T leaves x_1 unchanged, therefore $R(M) \subseteq M$. Moreover

$$\begin{aligned} M \backslash J_T = &\{x \in X_T | x_1 > 72 \text{ or } x_1 = 72 \text{ and } x_2 > 75\} \\ &\cup \{x \in X_T | x_1 < 78 \text{ or } x_1 = 78 \text{ and } x_2 < 75\}. \end{aligned}$$

The above argument shows that for all $x \in K \backslash J_T$, $F_T(x) \subseteq T_K(x)$. The claim follows by Theorem 3.

B. The Bouncing Ball System

It is easy to check that F_B is both Marchaud and Lipschitz and that R_B is upper and lower semicontinuous and has closed domain. Moreover, H_B also satisfies Assumption 1, since $R^{-1}(X) = J$. Therefore, we can immediately draw the following conclusion.

Proposition 6: For all $x_0 \in X_T$, $\mathcal{R}^{\infty}_{H_B}(x_0) \neq \emptyset$.

The proposition suggests that the impulse differential inclusion H_B does not deadlock. However, it is easy to show that for all $x_0 \in X_T$ all $(\tau, x) \in \mathcal{R}^{\infty}_{H_B}(x_0)$ are Zeno (see, for example, [38] and [41]). As expected, H_B violates the conditions of Proposition 3, in particular $R(0, 0) = \{(0, 0)\}$.

Despite the Zeno behavior, H_B is in many ways a reasonable model of the bouncing ball system. For example, one can show that the ball never falls below the surface on which it bounces, and that the system dissipates energy.

Proposition 7: The set $K = \{x \in X_T | x_1 \geq 0\}$ is viable and invariant. For all $C > 0$ the set $L = \{x \in X_T | gx_1 + x_2^2/2 \leq C\}$ is invariant.

Proof: For the first part, notice that $K \cap J_B = \{x \in X_T | x_1 = 0 \text{ and } x_2 \leq 0\}$. Since R_B does not affect x_1, $K \cap J_B \subseteq R^{-1}(K)$ and $R(K) \subseteq K$. Moreover, $K \backslash J_B = \{x \in X_T | x_1 > 0 \text{ or } x_1 = 0 \text{ and } x_2 > 0\}$. For x such that $x_1 > 0$, $F_B(x) \subseteq T_K(x) = X_B$. For x such that $x_1 = 0$ and $x_2 > 0$, $F_B(x) \subseteq \{v \in X | v_1 > 0\} = T_K(x)$. Therefore, K is viable by Theorem 1 and invariant by Theorem 3.

For the second part, R leaves x_1 unchanged and maps x_2 to αx_2. Therefore $R(L) \subseteq L$ since $\alpha \in [0, 1]$. Moreover

$$\begin{aligned} L \backslash J = &\{x \in X_T | x_1 > 0 \text{ or } x_2 > 0\} \\ &\cap \left\{x \in X_T | gx_1 + x_2^2/2 \leq C\right\}. \end{aligned}$$

For $x \in L\backslash J$ such that $gx_1 + x_2^2/2 < C$, $F_B(x) \subseteq T_K(x) = X_B$. For $x \in L\backslash J$ such that $gx_1 + x_2^2/2 = C$

$$\begin{aligned} T_K(x) &= \{v \in X_B | v_1 g + v_2 x_2 \leq 0\} \\ &\supseteq \{v \in X_B | v_1 g + v_2 x_2 = 0\} \supseteq F_B(x). \end{aligned}$$

The claim follows by Theorem 3. ∎

VI. Concluding Remarks

Impulse differential inclusions were introduced as a promising framework for modeling hybrid phenomena. We discussed how important problems in the hybrid systems literature, such as existence of runs, verification and controller synthesis for safety specifications can be reduced to viability and invariance questions for impulse differential inclusions. Motivated by this we developed conditions for determining whether a set of states is viable or invariant. In cases where these conditions are violated, we developed characterizations for the viability and invariance kernels of the set, and proposed conceptual algorithms for approximating them.

The results presented in this paper form the foundation for a more extensive study of hybrid control through the framework of viability theory. Problems we are currently working on include optimal control of impulse differential inclusions (value functions and their characterizations in terms of quasivariational inequalities or viability kernels), stability (Lyapunov functions and their characterization as viability kernels) and a study of the initialization map, which can be used to convert a hybrid system to a discrete time system by abstracting away the continuous dynamics. In the future we plan to address the more challenging problem of hybrid differential gaming, in terms of discriminating kernels. This will allow us to address more general control problems, such as controller synthesis in the presence of disturbances and nondeterminism.

Appendix
Additional Proofs

Proof of Proposition 2

We shall prove the first statement inductively. If $t = \tau_0$ the statement is true. If $\tau_0 = \tau_0'$, $x(\tau_0') = x(\tau_0)$. Otherwise, if $\tau_0 < \tau_0'$, $x(t)$ is a solution of the differential inclusion $\dot{x} \in F(x)$ over $[\tau_0, \tau_0']$ starting at $x(\tau_0)$. Therefore

$$x(t) \in \{x(\tau_0)\} + \int_{\tau_0}^{t} F(x(t'))\, dt', \quad \text{for all } t \in [\tau_0, \tau_0'].$$

In either case, equation (1) holds for all $t \in [\tau_0, \tau_0']$.

Assume that (τ, x) satisfies equation (1) for all $t \in [\tau_0, \tau_0'], \ldots, [\tau_n, \tau_n']$. Observe that $x(\tau_{n+1}) \in R(x(\tau_n'))$, and

$$\begin{aligned} R(x(\tau_n')) &= \{x(\tau_n')\} + S(x(\tau_n')) \\ &= \{x(\tau_0)\} + \sum_{\{i | \tau_i' \prec \tau_{n+1}\}} S(x(\tau_i')) \\ &\quad + \int_0^{\tau_{n+1}} F(x(t'))\, dt'. \end{aligned}$$

If $\tau_{n+1} = \tau_{n+1}'$

$$\begin{aligned} x(\tau_{n+1}') &= x(\tau_{n+1}) \\ &\in \{x(\tau_0)\} + \sum_{\{i | \tau_i' \prec \tau_{n+1}'\}} S(x(\tau_i')) \\ &\quad + \int_0^{\tau_{n+1}'} F(x(t'))\, dt'. \end{aligned}$$

Otherwise, if $\tau_{n+1} < \tau_{n+1}'$, $x(t)$ is a solution of the differential inclusion $\dot{x} \in F(x)$ over $[\tau_{n+1}, \tau_{n+1}']$ starting at $x(\tau_{n+1})$. Therefore, for all $t \in [\tau_{n+1}, \tau_{n+1}']$

$$\begin{aligned} x(t) &\in \{x(\tau_{n+1})\} + \int_{\tau_{n+1}}^{t} F(x(t'))\, dt' \\ &= \{x(\tau_0)\} + \sum_{\{i | \tau_i' \prec t\}} S(x(\tau_i')) + \int_0^t F(x(t'))\, dt'. \end{aligned}$$

Summarizing, if (τ, x) satisfies equation (1) for all $t \in [\tau_0, \tau_0'], \ldots, [\tau_n, \tau_n']$, then it also satisfies (1) for all $t \in [\tau_{n+1}, \tau_{n+1}']$. The first statement of the proposition follows by induction.

To prove the second statement, observe that a pair (τ, x) such that for all $t \in \tau$

$$x(t) \in \{x(\tau_0)\} + \sum_{\{i | \tau_i' \prec t\}} S(x(\tau_i')) + \int_0^t F(x(t'))\, dt'$$

satisfies $x(\tau_{i+1}) \in \{x(\tau_i')\} + S(x(\tau_i')) = R(x(\tau_i))$. Moreover, if $\tau_i < \tau_i'$, $x(t)$ is a solution to $\dot{x} \in F(x)$ over $[\tau_i, \tau_i']$ starting at $x(\tau_i)$. Therefore, according to Definition 3, if $J = \emptyset$ then (τ, x) is a run of (X, F, R, J). ∎

Proof of Lemma 1

Necessity: Consider $x_0 \in K\backslash C$ and $x(\cdot)$ a trajectory starting from x_0 which stays in K on some interval $[0, \sigma]$ (and which does not reach C in this time interval). By application of [30, Prop. 3.4.1], we obtain

$$F(x_0) \cap T_K(x_0) \neq \emptyset.$$

Sufficiency: Let $x_0 \in K\backslash C$. Because C is closed, some $r > 0$ exists such that $B(x_0, r) \cap C \neq \emptyset$. In the set $B_K(x_0, r) := K \cap B(x_0, r)$, one can imitate the proof of [30, Prop. 3.4.2] and obtain the existence of $T > 0$ and of a solution to $\dot{x} \in F(x)$ starting at x_0 which remains in $B_K(x_0, r)$ on $[0, T]$.

Using an argument (Zorn's Lemma) classical in differential equation theory, it is possible to extend $x(\cdot)$ to a maximal trajectory—again denoted $x(\cdot)$—on some $[0, \hat{T}]$ viable in K and such that $C \cap [0, \hat{T}) = \emptyset$. Either $\hat{T} = +\infty$ and the proof is complete, or $\hat{T} < +\infty$ and then $x(\hat{T}) \in C$ [if not one could extend a little the trajectory to a viable one, this would be a contradiction with the maximality of $x(\cdot)$]. ∎

Proof of Theorem 1

Notice that, since R is upper semicontinuous with closed domain and K is closed, $R^{-1}(K)$ is also closed.

Necessity: Assume that K is viable under (X, F, R, J) and consider an arbitrary $x_0 \in K$. To show the first condition is necessary assume $x_0 \in K \cap J$. Then continuous evolution is impossible at x_0. Assume, for the sake of contradiction, that $x_0 \notin R^{-1}(K)$. Then either $R(x) = \emptyset$ (in which case the system blocks and no infinite runs start at x_0) or all runs starting at x_0 leave K through a discrete transition to some $x_1 \in R(x_0)$. In either case, the assumption that K is viable is contradicted. To show the second condition is necessary, assume $x_0 \in K \backslash R^{-1}(K)$. Since an infinite run viable in K starts at x_0, there exists a solution to the differential inclusion $\dot{x} \in F(x)$ starting at x_0 which is either

1) defined on $[0, \infty[$ with $x(t) \in K \backslash J$ for all $t \geq 0$;
2) defined on $[0, t']$ with $x(t') \in R^{-1}(K)$ and $x(t) \in K \backslash J$ for all $t \in [0, t'[$.

This implies, in particular, that there is a solution to the differential inclusion $\dot{x} \in F(x)$ starting at x_0 which is either

1) defined on $[0, \infty[$ with $x(t) \in K$ for all $t \geq 0$;
2) defined on $[0, t']$ with $x(t') \in R^{-1}(K)$ and $x(t) \in K$ for all $t \in [0, t']$.

By the necessary part of Lemma 1, this implies that for all $x_0 \in K \backslash R^{-1}(K)$, $F(x) \cap T_K(x) \neq \emptyset$.

Sufficiency: Assume the conditions of the theorem are satisfied and consider an arbitrary $x_0 \in K$. We construct an infinite run of (X, F, R, J) starting at x_0 and viable in K by induction. We distinguish two cases, $x_0 \in K \backslash R^{-1}(K)$ and $x_0 \in K \cap R^{-1}(K)$. In the first case, by the sufficient part of Lemma 1, there exists a solution to the differential inclusion $\dot{x} \in F(x)$ starting at x_0 which is either

1) defined on $[0, \infty[$ with $x(t) \in K$ for all $t \geq 0$;
2) defined on $[0, t']$ with $x(t') \in R^{-1}(K)$ and $x(t) \in K$ for all $t \in [0, t']$.

Notice that, since by the first assumption of the theorem, $K \cap J \subseteq R^{-1}(K)$ there must also be a solution to the differential inclusion $\dot{x} \in F(x)$ starting at x_0 which is either

1) defined on $[0, \infty[$ with $x(t) \in K \backslash J$ for all $t \geq 0$;
2) defined on $[0, t']$ with $x(t') \in R^{-1}(K)$ and $x(t) \in K \backslash J$ for all $t \in [0, t'[$

[i.e., either the solution stays in K forever and never reaches J, or the solution stays in K and reaches $R^{-1}(K)$ by the time it reaches J]. In the former, consider the infinite run $([0, \infty[, x)$; this is clearly a run of (X, F, R, J), viable in K. In the latter case, let $\tau_0 = 0$, $\tau_0' = t'$, and $\tau_1 = \tau_0'$. Since $x(\tau_0') \in R^{-1}(K)$, $x(\tau_1)$ can be chosen such that $x(\tau_1) \in K$. Notice that this argument also covers the case where $x_0 \in K \cap R^{-1}(K)$, with $x(\tau_0')$ playing the role of x_0. An infinite run viable in K can now be constructed inductively, by substituting x_0 by $x(\tau_1)$ and repeating the process. ■

Proof of Theorem 2

As discussed in the proof of Theorem 1, $R^{-1}(K)$ is closed.

Necessity: The first condition was shown to be necessary in the proof of Theorem 1. To show the second condition is necessary, assume that K is viable under (X, F, R, J) an consider an arbitrary $x_0 \in K$. If $x_0 \in K \backslash J = K \cap I$, since an infinite run viable in K starts at x_0, there exists a solution to the differential inclusion $\dot{x} \in F(x)$ starting at x_0 which is either:

1) defined on $[0, \infty[$ with $x(t) \in K \cap I$ for all $t \geq 0$;
2) defined on $[0, t']$ with $x(t') \in R^{-1}(K)$ and $x(t) \in K \cap I$ for all $t \in [0, t']$.

By the necessary part of Lemma 1, this implies that for all $x_0 \in K \cap I \backslash R^{-1}(K)$, $F(x) \cap T_{K \cap I}(x) \neq \emptyset$.

Sufficiency: Assume the conditions of the theorem hold and consider an arbitrary $x_0 \in K$. We construct a run of (X, F, R, J) starting at x_0 and viable in K by induction. We distinguish two cases, $x_0 \in (K \cap I) \backslash R^{-1}(K)$ and $x_0 \in K \cap R^{-1}(K)$. Notice that, since by the first condition of the theorem $K \cap J = K \backslash I \subseteq R^{-1}(K)$, these two cases cover K. By the sufficient part of Lemma 1, there exists a solution to the differential inclusion $\dot{x} \in F(x)$ starting at x_0 which is either

1) defined on $[0, \infty[$ with $x(t) \in K \cap I$ for all $t \geq 0$;
2) defined on $[0, t']$ with $x(t') \in R^{-1}(K)$ and $x(t) \in K \cap I$ for all $t \in [0, t']$.

In the former case, consider the infinite run given by $([0, \infty[, x)$; this is clearly a run of (X, F, R, J), viable in K. In the latter case, let $\tau_0 = 0$, $\tau_0' = t'$, and $\tau_1 = \tau_0'$. Since $x(\tau_0') \in R^{-1}(K)$, $x(\tau_1)$ can be chosen such that $x(\tau_1) \in K$. Notice that this argument also covers the case where $x_0 \in K \cap R^{-1}(K)$, with $x(\tau_0')$ playing the role of x_0. An infinite run viable in K can now be constructed inductively, by substituting x_0 by $x(\tau_1)$ and repeating the process. ■

Proof of Proposition 3

Let

$$D = \inf_{x \in R(X),\, y \in R^{-1}(X)} \|x - y\|.$$

Since $R(X) \cap R^{-1}(X) = \emptyset$, $R^{-1}(X)$ is closed and $R(X)$ is compact (by the assumptions of the proposition), $D > 0$. Consider an arbitrary solution, x, of the differential inclusion $\dot{x} \in F(x)$, over an interval $[0, t]$ with $x(0) \in R(X)$ and $x(t) \in R^{-1}(X)$. Clearly, $\|x(t) - x(0)\| \geq D$. Let M be a bound on $F(x)$, over the set $B(R(X), D)$, i.e.,

$$\sup_{x \in B(R(X), D),\, y \in F(x)} \|y\| \leq M.$$

Such a bound exists since F is Marchaud and $R(X)$ is compact. Then

$$\|x(t) - x(0)\| \leq \int_0^t F(x(\sigma))\, d\sigma \leq Mt.$$

Therefore, $t \geq D/M$, or, in other words, between any two discrete transitions the system must flow along the differential inclusion for at least D/M time units.

Consider an arbitrary $x_0 \in X$, and a run (τ, x) with $x(\tau_0) = x_0$. If $\tau_0' = \infty$, then the run is trivially non-Zeno. Otherwise, $\tau_0 \leq \tau_0' < \infty$ and the system takes a discrete transition at τ_0'. Therefore, $x(\tau_0') \in R^{-1}(X)$ and $x(\tau_1) \in R(x(\tau_0'))$. If $\tau_1' = \infty$, the run is non-Zeno. If $\tau_1 \leq \tau_1' < \infty$, a discrete transition takes place at τ_1'. Therefore, $x(\tau_1') \in R^{-1}(X)$, and, by the above discussion, $\tau_1' - \tau_1 \geq T$.

The process can now be repeated by replacing τ_1 by τ_2, etc. Between any two consecutive discrete transitions at least time $T > 0$ elapses, therefore, the $\sum_i (\tau_i' - \tau_i)$ diverges. ■

Proof of Lemma 2

Necessity: Assume that all solutions starting in K stay in K until they reach C. Consider $x_0 \in K\backslash C$ and $v_0 \in F(x_0)$. Then (see for example [30, Corollary 5.3.2]) there exists a trajectory $x(\cdot)$ of $\dot{x} \in F(x)$ starting at x_0 such that $(d/dt)\,x(0) = v_0$. Since x is a solution to $\dot{x} \in F(x)$ it remains in K until it reaches C. But $x_0 \in K\backslash C$ and C is closed, therefore, there exists $\alpha > 0$ such that $x(t) \in K$ for all $t \in [0, \alpha]$. Since x is absolutely continuous, for all $t \in [0, \alpha[$ where $(d/dt)\,x(t)$ is defined, $(d/dt)\,x(t) \in T_K(x(t))$ (see for example [30]). In particular, for $t = 0$, $v_0 = (d/dt)\,x(0) \in T_K(x_0)$. Hence, for all $x_0 \in K\backslash C$ and for all $v_0 \in F(x_0)$, $v_0 \in T_K(x_0)$, or, in other words, $F(x_0) \subseteq T_K(x_0)$.

Sufficiency: Let λ be the Lipschitz constant of F. Consider $x_0 \in K$ and a solution $x(\cdot)$ of $\dot{x} \in F(x)$ starting at x_0, and show that x remains in K until it reaches C. If $x_0 \in C$ then there is nothing to prove. If $x_0 \in K\backslash C$ consider

$$\theta = \sup\{t | \forall\, t' \in [0, t[,\, x(t') \in K\backslash C\}\,.$$

If $\theta = \infty$ or $x(\theta) \in C$ we are done. We show that $x(\theta) \in K\backslash C$ leads to a contradiction. Indeed, consider $\alpha > 0$ such that $B(x(\theta), \alpha) \cap C = \emptyset$ [which exists since $x(\theta) \notin C$ and C is closed], and $\theta' > \theta$, such that for all $t \in [\theta, \theta']$, $x(t) \in B(x(\theta), \alpha)$ (which exists since x is continuous). For $t \in [\theta, \theta']$, let $\Pi_K(x(t))$ denote a point of $B(x(\theta), \alpha) \cap K$ such that

$$d(x(t), K) = d(x(t), \Pi_K(x(t)))$$

[a projection of $x(t)$ onto K]. Then (see, for example, [30, Lemma 5.1.2]) for almost every $t \in [\theta, \theta']$

$$\begin{aligned}
&\frac{d}{dt}\, d(x(t), K) \\
&\quad \le d\left(\frac{d}{dt}\, x(t), T_K(\Pi_K(x(t)))\right) \\
&\quad \le d\left(\frac{d}{dt}\, x(t), F(\Pi_K(x(t)))\right) \\
&\quad \le d\left(\frac{d}{dt}\, x(t), F(x(t))\right) + \lambda\, d(x(t), \Pi_K(x(t))) \\
&\quad \le 0 + d(x(t), K)
\end{aligned}$$

since x is a solution to $\dot{x} \in F(x)$ and by definition of Π. By the Gronwall lemma, $d(x(t), K) = 0$ for all $t \in [\theta, \theta']$, which contradicts the definition of θ. Summarizing, if $F(x) \subseteq T_K(x)$ for all $x \in K\backslash C$, then all solutions starting in K either stay for ever in $K\backslash C$ or reach C before they leave K. ■

Proof of Theorem 3

Necessity: Assume that K is invariant under (X, F, R, J). If the first condition is violated, then there exists $x_0 \in K$ and $x_1 \in R(x_0)$ with $x_1 \notin K$. Therefore, there exists a run starting at x_0 that leaves K through a discrete transition to some x_1 and the assumption that K is invariant is contradicted. To show the second condition is necessary, notice that since all runs of (X, F, R, J) starting in K are viable in K, then all solutions to $\dot{x} \in F(x)$ starting in K are either

1) defined on $[0, \infty[$ with $x(t) \in K\backslash J$ for all $t \ge 0$;
2) defined on $[0, t']$ with $x(t') \in J$ and $x(t) \in K$ for all $t \in [0, t']$.

Otherwise, there would exist a solution of $\dot{x} \in F(x)$ which leaves K before reaching J. This solution would be a run of (X, F, R, J) that is not viable in K, which would contradict the assumption that K is invariant. By the necessary part of Lemma 2, 1 and 2 imply that for all $x_0 \in K\backslash J$, $F(x) \subseteq T_K(x)$.

Sufficiency: Assume the conditions of the theorem are satisfied and consider an arbitrary $x_0 \in K$ and an arbitrary run, (τ, x), of (X, F, R, J) starting at x_0. Notice that $x(\tau_0) = x_0 \in K$ by assumption. Assume $x(\tau_i) \in K$ and show $x(t) \in K$ until τ_{i+1}; the claim then follows by induction. If $t = \tau_i$ we are done. If $\tau_i \prec t \preceq \tau_i'$, then $x(\tau_i) \in K\backslash J$ since continuous evolution is possible from $x(\tau_i)$. By the second condition of the theorem and the sufficient part of Lemma 2, all solutions to the differential inclusion $\dot{x} \in F(x)$ starting at $x(\tau_i)$ are either

1) defined on $[0, \infty[$ with $x(t) \in K$ for all $t \ge 0$;
2) defined on $[0, t']$ with $x(t') \in J$ and $x(t) \in K$ for all $t \in [0, t']$.

In the first case, the run is viable in K and we are done. In the second case, $\tau_i' \preceq t'$ and therefore for all $t \in [\tau_i, \tau_i']$, $x(t) \in K$. If $x(\tau_i') \in R^{-1}(K)$, $x(\tau_{i+1}) \in R(x(\tau_i)) \subseteq K$ by the first condition of the theorem. If, on the other hand, $x(\tau_i') \in J$, but $R(x(\tau_i')) = \emptyset$, then the execution blocks at τ_i, and, therefore, is viable in K. ■

Proof of Lemma 3

Let $D \subseteq K$ a closed set satisfying the assumptions of Lemma 1. Clearly $D \subseteq Viab_F(K, C)$.

We claim that $Viab_F(K, C)$ is closed. Consider a sequence $x_n \in Viab_F(K, C)$ converging to some $x \in X$. Since K is closed, $x \in K$. We show that $x \in Viab_F(K, C)$. If $x \in C$, the proof is done. Else, there exists an $r > 0$ with $K \cap B(x, r) \neq \emptyset$. For n large enough $x_n \in B(x, (r/2))$. For any such n, consider $x_n(\cdot)$ a solution to the differential inclusion starting from x_n, viable in K until it reaches C. Such a solution exists, since $x_n \in Viab_F(K, C)$.

The graph of the solution map of the differential inclusion restricted to the compact set

$$\{x\} \cup \{x_n, n > 0\}$$

is compact (in [30, Th. 3.5.2]). Hence, there exists a subsequence to $x_n(\cdot)$—again denoted $x_n(\cdot)$—converging to a solution $x(\cdot)$ of the differential inclusion starting at x uniformly on compact intervals.

Let $\sigma > 0$ such that $x[0, \sigma) \cap C = \emptyset$. Such a σ exists since $x \notin C$, C is closed, and $x(\cdot)$ is continuous. Fix $0 \le t < \sigma$. For n large enough, $x_n[0, t] \cap C = \emptyset$ because C is closed and $x_n(\cdot)$

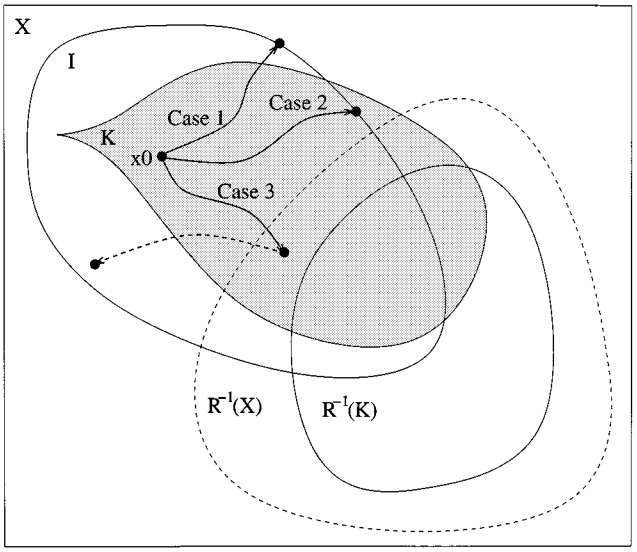

Fig. 7. Three possible evolutions for $x_0 \notin Viab_F(K \cap I,\ R^{-1}(K)) \cup (K \cap R^{-1}(K))$.

converges uniformly to $x(\cdot)$ on $[0,\ t]$. Since $x_n[0,\ t]$ is contained in K so is $x[0,\ t]$. Because σ and t are arbitrary, we can deduce that $x(\cdot)$ is viable in K until it reaches C. So $x \in Viab_F(K,\ C)$, and therefore $Viab_F(K,\ C)$ is closed.

It remains to prove that $Viab_F(K,\ C)$ satisfies the conditions of Lemma 1 (i.e., that it is itself viable with target C). Let $x_0 \in Viab_F(K,\ C)$. By the very definition of the viability kernel some trajectory $x(\cdot)$ starting from x exists which is viable in K until it reaches C. Suppose by contradiction that some $s > 0$ exists such $x(s) \notin Viab_F(K,\ C)$ and $x[0,\ s] \cap C = \emptyset$. Then any trajectory starting from $x(s)$ leaves K before reaching C. But $t \mapsto x(s+t)$ is such a trajectory which is viable in K until it reaches C, a contradiction. ■

Proof of Lemma 4

Necessity: We first show that for every closed set K viable under $H = (X, F, R, J)$, $Pre_H^{\exists}(K) = K$. $Pre_H^{\exists}(K)$ is clearly a subset of K, since $Viab_F(K \cap I,\ R^{-1}(K)) \subseteq K \cap I \subseteq K$. Conversely, consider an arbitrary $x_0 \in K$. Assume, for the sake of contradiction, that $x_0 \notin Viab_F(K \cap I,\ R^{-1}(K)) \cup (K \cap R^{-1}(K))$. Consider an arbitrary infinite run $(\tau,\ x)$ viable in K and starting at x_0. Then $x(\tau_0) \notin R^{-1}(K)$ and $x(\tau_0) \notin Viab_F(K \cap I,\ R^{-1}(K))$. If $\tau_0 = \tau_0'$, x starts by a discrete transition to some $x(\tau_1) \in R(x(\tau_0))$. Since $x(\tau_0) \notin R^{-1}(K)$, $x(\tau_1) \notin K$, which contradicts the assumption that $(\tau,\ x)$ is viable in K. If $\tau_0 < \tau_0'$, then $(\tau,\ x)$ starts by continuous evolution. Since $x_0 = x(\tau_0) \notin Viab_F(K \cap I,\ R^{-1}(K))$, the run either

1) leaves K (at time $t \prec \tau_0'$) before it reaches $R^{-1}(K)$;
2) leaves I (at time τ_0') before it reaches $R^{-1}(K)$;
3) takes a transition from some $x(\tau_0') \in K \cap I \backslash R^{-1}(K)$;

(see Fig. 7). The first case contradicts the assumption that $(\tau,\ x)$ is viable in K. In the remaining cases, $x(\tau_0') \notin R^{-1}(K)$ and since $x(\tau_1) \in R(x(\tau_0'))$, we have $x(\tau_1) \notin K$. This also contradicts the assumption that $(\tau,\ x)$ is viable in K.

Sufficiency: Next, we show that every closed set K such that $K = Pre_H^{\exists}(K)$ is viable. Consider an arbitrary $x_0 \in K$; we construct by induction an infinite run, $(\tau,\ x)$ that starts at x_0 and is viable in K. By assumption, $x_0 = x(\tau_0) \in K$. Assume that we have constructed a run viable in K defined over a finite sequence $[\tau_0,\ \tau_0']$, $[\tau_1,\ \tau_1']$, $\ldots$, $[\tau_i,\ \tau_i]$. Since K is a fixed point of $Pre_H^{\exists}$, and the run is viable in K, $x(\tau_i) \in Viab_F(K \cap I,\ R^{-1}(K)) \cup (K \cap R^{-1}(K))$. If $x(\tau_i) \in K \cap R^{-1}(K)$, let $\tau_i' = \tau_i$ and chose $x(\tau_{i+1}) \in R(x(\tau_i')) \cap K$. If $x(\tau_i) \in Viab_F(K \cap I,\ R^{-1}(K))$, then there exists a solution to the differential inclusion $\dot{x} \in F(x)$ which is either:

1) defined over $[0,\ \infty[$ with $x(t) \in K \cap I$ for all $t \geq 0$;
2) defined over $[0,\ t']$ with $x(t') \in R^{-1}(K)$ and $x(t) \in K \cap I$ for all $t \in [0,\ t']$.

In the former case, set $\tau_i' = \infty$ and the construction of the infinite run is complete. In the latter case, let $\tau_i' = \tau_i + t'$ and choose $x(\tau_{i+1}) \in R(x(\tau_i')) \cap K$. The claim follows by induction. ■

Proof of Theorem 4

The proof makes use of the sequence of sets $\{K_i\}$ constructed by the Viability Kernel Approximation algorithm, that is the sequence $K_0 = K$, $K_{i+1} = Pre_H^{\exists}(K_i)$. Let

$$K_\infty = \bigcap_{i=0}^{\infty} K_i.$$

The proof proceeds in a sequence of steps. We show that

1) for every viable set $L \subseteq K$, $L \subseteq Viab_H(K)$;
2) K_∞ is closed;
3) $Viab_H(K) \subseteq K_\infty$;
4) $K_\infty \subseteq Viab_H(K)$;
5) $Viab_H(K)$ is viable.

Step 1: Every set $L \subseteq K$ which viable under $H = (X, F, R, J)$ must be contained in $Viab_H(K)$, since for all $x_0 \in L$ there exists an infinite run starting at x_0 that stays in L, and, therefore, in K.

Step 2: Since $Viab_F(K_i \cap I,\ R^{-1}(K_i)) \subseteq K_i \cap I \subseteq K_i$, $K_{i+1} \subseteq K_i$ for all i. Since K is closed, K_0 is closed. Moreover, if K_i is closed, then $R^{-1}(K_i)$ is closed (since R is upper semicontinuous with closed domain), and $Viab_F(K_i \cap I,\ R^{-1}(K_i))$ is closed [by Lemma 3, since I and $R^{-1}(K_i)$ are closed], and, therefore, K_{i+1} is closed. By induction, K_i form a sequence of nested closed sets, and, therefore, K_∞ is closed (possibly the empty set).

Step 3: Consider a point $x_0 \in Viab_H(K)$ and show that $x_0 \in K_\infty$. Assume, for the sake of contradiction, that $x_0 \notin K_\infty$. Then there exists $N \geq 0$ such that $x_0 \notin K_N$. If $N = 0$, then $x_0 \notin K_0 = K$, therefore all runs starting at x_0 that are not viable in K (trivially). This contradicts the assumption that $x_0 \in Viab_H(K)$. If $N > 0$, we show that for all infinite runs $(\tau,\ x)$ starting at x_0 [which exist since $x_0 \in Viab_H(K)$], there

exists a $t \preceq \tau_1$ such that[1] $x(t) \notin K_{N-1}$. The claim then follows by induction. Indeed, since $x_0 \notin K_N$ we must have $x_0 \notin Viab_F(K_{N-1} \cap I, R^{-1}(K_{N-1})) \cup (K_{N-1} \cap R^{-1}(K_{N-1}))$. If $\tau_0 < \tau_0'$, then (τ, x) starts by continuous evolution. Since $x_0 = x(\tau_0) \notin Viab_F(K_{N-1} \cap I, R^{-1}(K_{N-1}))$, then all solutions to $\dot{x} \in F(x)$ either

1) leave K_{N-1} (at some $t \preceq \tau_0'$) before they reach $R^{-1}(K_{N-1})$;
2) leave I (at time τ_0') before they reach $R^{-1}(K_{N-1})$;
3) take a transition from some $x(\tau_0') \in (K_{N-1} \cap I) \backslash R^{-1}(K_{N-1})$;

(refer to Fig. 7). In the first case, we are done. In the remaining cases, $x(\tau_0') \notin R^{-1}(K_{N-1})$ and since $x(\tau_1) \in R(x(\tau_0'))$, we have $x(\tau_1) \notin K_{N-1}$. The last argument also subsumes the case $\tau_0 = \tau_0'$, since $x_0 \notin K_{N-1} \cap R^{-1}(K_{N-1})$.

Step 4: Consider an arbitrary $x_0 \in K_\infty$. To show that $x_0 \in Viab_H(K)$, we construct an infinite run $(\tau, x) \in \mathcal{R}_H^\infty(x_0)$ viable in K. More specifically, since $x_0 \in K_k$ for all k, by Lemma 5, there exists a sequence of runs $(\tau^{(k)}, x^{(k)}) \in \mathcal{R}_H(x_0)$, which remain in K for at least k jumps. We will show that the sequence $(\tau^{(k)}, x^{(k)})$ has a cluster point $(\overline{\tau}, \overline{x}) \in \mathcal{R}_H^\infty(x_0)$, which is an infinite run of (X, F, R, J), starting at x_0, viable in K.

Let $[\tau_i^{(k)}, \tau_i^{(k)'}]$ [or $[\tau_i^{(k)}, \tau_i^{(k)'}[$ if i is the last interval] denote the sequence of intervals $\tau^{(k)}$. Recall that, without loss of generality, we can assume that $\tau_0^{(k)} = 0$ for all k. Let $\overline{\tau}_0 = 0$ and define

$$\overline{\tau}'_0 = \lim \inf_{k \to \infty} \tau_0^{(k)'}.$$

Then there exists a subsequence of $\tau_0^{(k)'}$, denoted by $\tau_0^{\sigma(k)'}$, such that

$$\lim_{k \to \infty} \tau_0^{\sigma(k)'} = \overline{\tau}'_0.$$

We distinguish three cases

1) $\overline{\tau}'_0 = +\infty$;
2) $\overline{\tau}'_0 \in]0, +\infty[$;
3) $\overline{\tau}'_0 = 0$.

Case 1 will lead to a run $(\overline{\tau}, \overline{x}) \in \mathcal{R}_H^\infty(x_0)$ that is viable in K and makes no jumps. Case 2 will lead to a run $(\overline{\tau}, \overline{x}) \in \mathcal{R}_H^\infty(x_0)$ that is viable in K, whose first jump comes after an interval of continuous evolution. Finally, Case 3 will lead a run $(\overline{\tau}, \overline{x}) \in \mathcal{R}_H^\infty(x_0)$ viable in K, that takes its first jump immediately.

Case 1: Consider a sequence $y^{\sigma(k)}(\cdot)$ of solutions to the differential inclusion

$$\dot{x} \in F(x), \quad x(0) = x_0 \tag{2}$$

that coincide with $x^{\sigma(k)}$ on $[0, \tau_0^{\sigma(k)'}[$. Because the set of solutions of (2) is compact (see [30, Th. 3.5.2]), there exists a subsequence $y^{\phi(k)}(\cdot)$ of the sequence $y^{\sigma(k)}(\cdot)$ that converges to a solution $\overline{y}(\cdot)$ of (2). Moreover, since $\lim_{k \to \infty} \tau_0^{\sigma(k)'} = +\infty$, the sequence $y^{\phi(k)}(\cdot)$ [and hence the sequence $x^{\phi(k)}(\cdot)$] converges to $\overline{y}(\cdot)$ uniformly over $[0, T]$, for all $T > 0$.

Now, $(\tau^{\phi(k)}, x^{\phi(k)})$ is a run of (X, F, R, J) viable in K for at least k jumps. Therefore, $x^{\phi(k)}(t) \in K \cap I$ for all $t \in [0, \tau_0^{\phi(k)'}[$, and hence, for sufficiently large k, $x^{\phi(k)}(t) \in K \cap I$ for all $t \in [0, T]$. Since $K \cap I$ is closed, $\overline{y}(t) \in K \cap I$ for all $t \in [0, T]$. Since T is arbitrary, $([0, \infty[, \overline{y})$ is an infinite run of (X, F, R, J) (with no jumps) starting at x_0 and viable in K. The proof is complete.

Case 2: We can restrict attention to $k \geq 1$. As for case 1, define the sequence $y^{\sigma(k)}(\cdot)$ of solutions of (2) that coincide with $x^{\sigma(k)}$ on $[0, \tau_0^{\sigma(k)'}[$ and the subsequence $y^{\phi(k)}(\cdot)$ converging (uniformly over compact intervals) to a solution $\overline{y}(\cdot)$ of (2). As before, $(\tau^{\phi(k)}, x^{\phi(k)})$ is a run of (X, F, R, J) viable in K for at least $k > 0$ jumps. Therefore, $x^{\phi(k)}(t) \in K \cap I$ for all $t \in [0, \tau_0^{\phi(k)'}[$. Since $K \cap I$ is closed, $\overline{y}(t) \in K \cap I$ for all $t \in [0, \overline{\tau}'_0]$. Therefore, $([\overline{\tau}_0, \overline{\tau}'_0], \overline{y})$ is a finite run of (X, F, R, J) (with no jumps) starting at x_0 and viable in K.

Since $y^{\phi(k)}(\cdot)$ converges to $\overline{y}(\cdot)$ and $\tau_0^{\phi(k)'}$ converges to $\overline{\tau}'_0$, $x^{\phi(k)}(\tau_0^{\phi(k)'})$ converges to $\overline{y}(\overline{\tau}'_0)$. Recall that $(\tau^{\phi(k)}, x^{\phi(k)})$ is a run of (X, F, R, J) viable in K for at least $k > 0$ jumps, therefore $x^{\phi(k)}(\tau_1^{\phi(k)}) \in R(x^{\phi(k)}(\tau_0^{\phi(k)'})) \cap K$. Since R is upper semicontinuous with closed domain and compact images, there exists a subsequence of $x^{\phi(k)}(\tau_1^{\phi(k)})$ converging to some point $\overline{y}_1 \in R(\overline{y}(\overline{\tau}'_0)) \cap K$. Therefore, $([0, \overline{\tau}'_0][\overline{\tau}_1, \overline{\tau}'_1], \overline{y})$ with $\overline{\tau}_1 = \overline{\tau}'_1 = \overline{\tau}'_0$ and $\overline{y}(\overline{\tau}_1) = \overline{y}_1$ defined as above is a finite run of (X, F, R, J) (with one jump) starting at x_0 and viable in K.

Case 3: The second part of the argument for Case 2 shows that, since $x^{\phi(k)}(\tau_0^{\sigma(k)'})$ converge to x_0, there exists $\overline{y}_1 \in R(x_0) \cap K$. Therefore, $([0, \overline{\tau}'_0][\overline{\tau}_1, \overline{\tau}'_1], \overline{y})$ with $\overline{\tau}'_0 = \overline{\tau}_1 = \overline{\tau}'_1 = 0$, $\overline{y}(\tau'_0) = x_0$ and $\overline{y}(\overline{\tau}_1) = \overline{y}_1$ is a finite run of (X, F, R, J) (with one instantaneous jump) starting at x_0 and viable in K.

To complete the proof for Cases 2 and 3, we repeat the argument starting at $\overline{y}(\overline{\tau}_1)$ (discarding the initial part of the sequences accordingly). We generate $\overline{\tau}'_1 = \lim \inf_{k \to \infty} \tau_1^{(k)'}$ and construct a run of (X, F, R, J) viable in K, defined either over $[0, \overline{\tau}_0][\overline{\tau}_1, \overline{\tau}'_1[$ (if $\overline{\tau}'_1 = +\infty$, in which case the proof is complete) or over $[0, \overline{\tau}'_0][\overline{\tau}_1, \overline{\tau}'_1][\overline{\tau}_2, \overline{\tau}'_2]$ with $\overline{\tau}_2 = \overline{\tau}'_2 = \overline{\tau}'_1$ (if $\overline{\tau}'_1$ is finite). The claim follows by induction.

Step 5: Finally, we show $Viab_H(K)$ is viable by showing that it is a fixed point of $Pre_H^\exists$. Recall that $Pre_H^\exists(Viab_H(K)) \subseteq Viab_H(K)$. Consider an arbitrary $x_0 \in Viab_H(K)$ and assume, for the sake of contradiction, that $x_0 \notin Pre_H^\exists(Viab_H(K))$. Consider an arbitrary infinite run (τ, x) viable in K and starting at x_0 [which exists since $x_0 \in Viab_H(K)$]. If $\tau_0 = \tau_0'$, x starts by a discrete transition to some $x(\tau_1) \in R(x_0)$. Since $x_0 \notin R^{-1}(Viab_H(K))$, $x(\tau_1) \notin Viab_H(K)$. If $\tau_0 < \tau_0'$, then (τ, x) starts by continuous evolution. Since $x_0 \notin Viab_F(Viab_H(K) \cap I, R^{-1}(Viab_H(K)))$, the execution either

1) leaves $Viab_H(K)$ (at time $t \prec \tau_0'$) before it reaches $R^{-1}(Viab_H(K))$;
2) leaves I (at time τ_0') before it reaches $R^{-1}(Viab_H(K))$;

[1] If $\tau = [\tau_0, \infty)$, $t \preceq \tau_1$ is replaced by $t \prec \tau_0' = \infty$.

3) takes a transition from some $x(\tau_0') \in Viab_H(K) \cap I \backslash R^{-1}(Viab_H(K))$;

(see Fig. 7). In all cases, (τ, x) either blocks or leaves $Viab_H(K)$ at some $t \in \tau$ with $t \preceq \tau_1$. But if $x(t) \notin Viab_H(K)$ there is no infinite run of $H = (X, F, R, J)$ starting at $x(t)$ and viable in K. Therefore, (τ, x) either blocks or is not viable in K. This contradicts the assumption that $x_0 \in Viab_H(K)$. ■

Proof of Lemma 5

Necessity: The proof was given in Step 3 of Theorem 4 above, where it was shown that if $x_0 \notin K_N$, then all runs starting at x_0 leave K after at most N transitions.

Sufficiency: If $N = 0$ there is nothing to prove. If $N > 0$, $x_0 \in K_N$ implies that $x_0 \in Viab_F(K_{N-1} \cap I, R^{-1}(K_{N-1})) \cup (K_{N-1} \cap R^{-1}(K_{N-1}))$. If $x_0 \in Viab_F(K_{N-1} \cap I, R^{-1}(K_{N-1}))$, then there exists a solution to $\dot{x} \in F(x)$ starting at x_0 which is either

1) defined on $[0, \infty[$ with $x(t) \in K_{N-1} \cap I$ for all $t \geq 0$;
2) defined on $[0, t']$ with $x(t') \in R^{-1}(K_{N-1})$ and $x(t) \in K_{N-1} \cap I$ for all $t \in [0, t']$.

In the former case, the run $([0, \infty[, x)$ is an infinite run viable in K_{N-1} (and, hence, K), and the proof is complete. In the latter case, there exists a finite run with one transition $([\tau_0, \tau_0'][\tau_1, \tau_1'], x)$ with $\tau_0 = 0$, $\tau_0' = \tau_1 = \tau_1' = t'$, $x(t) \in K_{N-1} \cap I$ for all $t \in [\tau_0, \tau_0']$ and $x(\tau_1) \in K_{N-1}$. This also subsumes the case $x_0 \in K_{N-1} \cap R^{-1}(K_{N-1})$: there exists a finite run with one transition $([\tau_0, \tau_0'][\tau_1, \tau_1'], x)$ with $\tau_0 = \tau_0' = \tau_1 = \tau_1'$, $x(\tau_0) = x(\tau_0') = x_0 \in K_{N-1}$ and $x(\tau_1) \in K_{N-1}$.

Since $K_N \subseteq K_{N-1} \subseteq K$, the constructed run remains in K_{N-1} for at least one jump. The claim follows by induction. ■

Proof of Lemma 6

By definition, $Inv_F(K, C)$ is the set of $x_0 \in K$ such that for all solutions $x(\cdot)$ of $\dot{x} \in F(x)$ starting at x_0 either

1) $x(t) \in K$ for all $t \geq 0$;
2) there exists $t' \geq 0$ such that $x(t') \in C$ and $x(t) \in K$ for all $t \in [0, t']$.

Therefore, $Inv_F(K, C)$ satisfies the conditions of Lemma 2. Moreover, every subset $L \subseteq K$ which satisfies the conditions of Lemma 2 must be contained in $Inv_F(K, C)$, since all runs starting in L stay in L (and therefore in K) until they reach C.

It remains to show that $Inv_F(K, C)$ is closed. Consider a sequence $x_n \in Inv_F(K, C)$ converging to x_0 and show that $x_0 \in Inv_F(K, C)$. Since by definition $Inv_F(K, C) \subseteq K$ and K is assumed to be closed, $x_0 \in K$. If $x_0 \in K \cap C$ there is nothing to prove, since by definition $K \cap C \subseteq Inv_F(K, C)$. If $x_0 \in K \backslash C$, let $x(\cdot)$ be any solution of $\dot{x} \in F(x)$ starting at x_0. Let

$$\theta = \sup \{t | \forall t' \in [0, t[, x(t') \in K \backslash C\}.$$

If $\theta = \infty$ or if $x(\theta) \in C$, then $x_0 \in Inv_F(K, C)$, and the proof is complete.

Let λ be the Lipschitz constant of F, and assume, for the sake of contradiction, that $\theta < \infty$ and $x(\theta) \in K \backslash C$. Then, by the definition of θ and the assumption that K and C are closed, there exists $\theta' > \theta$ such that $x(\theta') \notin K$ and for all $t \in [\theta, \theta']$, $x(t) \notin C$. Choose ϵ such that

$$d(x(\theta'), K) > \epsilon e^{\lambda \theta'} \tag{3}$$

[possible since K is closed and $x(\theta') \notin K$] and for all $t \in [0, \theta']$

$$\left\{x(t) + \epsilon B(0, 1) e^{\lambda t}\right\} \cap C = \emptyset \tag{4}$$

[possible since C is closed and for all $t \in [0, \theta']$, $x(t) \notin C$].

Since $x_n \to x_0$ there exists n large enough such that $||x_n - x_0|| < \epsilon$. By Filippovs Theorem (see, for example, [30, Theorem 5.3.1]) there exists a solution $x_n(\cdot)$ of $\dot{x} \in F(x)$ starting at x_n such that for all $t \in [0, \theta']$

$$||x_n(t) - x(t)|| \leq ||x_n - x_0|| e^{\lambda t}$$

or, in other words, for all $t \in [0, \theta']$

$$x_n(t) \in B\left(x(t), ||x_n - x_0|| e^{\lambda t}\right) \subseteq B\left(x(t), \epsilon e^{\lambda t}\right).$$

Therefore, by (4), for all $t \in [0, \theta']$, $x_n(t) \notin C$, while, by (3) $x_n(\theta') \notin K$. This contradicts the assumption that $x_n \in Inv_F(K, C)$. Hence, every converging sequence has its limit in $Inv_F(K, C)$, and therefore $Inv_F(K, C)$ is closed. ■

Proof of Lemma 7

Necessity: We first show that for every closed, invariant set K, $K = Pre_H^{\forall}(K)$. Clearly $Pre_H^{\forall}(K) \subseteq K$, since $Inv_F(K, J) \subseteq K$. Conversely, consider an arbitrary point $x_0 \in K$ and show that $x_0 \in Inv_F(K, J) \cap R^{\ominus 1}(K)$. Assume, for the sake of contradiction that this is not the case. Then, either $x_0 \notin Inv_F(K, J)$, or $x_0 \notin R^{\ominus 1}(K)$. If $x_0 \notin R^{\ominus 1}(K)$, there exists $x_1 \in R(x_0)$ such that $x_1 \notin K$; in other words, there exists a run of the impulse differential inclusion starting at x_0 that leaves K by a discrete transition. This contradicts the assumption that K is invariant. If, on the other hand, $x_0 \notin Inv_F(K, J)$ then, in particular, $x_0 \notin J \cap K$ [since $J \cap K \subseteq Inv_F(K, J)$]; but $x_0 \in K$, so we must have $x_0 \notin J$, and therefore continuous evolution starting at x_0 is possible. Since $x_0 \notin Inv_F(K, J)$, there exists a solution to $\dot{x} \in F(x)$ starting at x_0 that leaves K before reaching J. This solution is a run (X, F, R, J) that starts in K but is not viable in K. This also contradicts the assumption that K is invariant.

Sufficiency: Next, we show that every closed set K such that $K = Pre_H^{\forall}(K)$ is invariant. Consider an arbitrary run (τ, x) starting at some $x_0 \in K$. We show that (τ, x) is viable in K by induction. Assume that we have shown that $x(t) \in K$ for all $t \in [\tau_0, \tau_0'], [\tau_1, \tau_1'], \ldots, [\tau_i, \tau_i]$. Then, since $K = Pre_H^{\forall}(K)$, $x(\tau_i) \in Inv_F(K, J) \cap R^{\ominus 1}(K)$. If $\tau_i = \tau_i'$ the system takes a discrete transition to some $x(\tau_{i+1}) \in R(x(\tau_i')) \subseteq K$, since $x(\tau_i') = x(\tau_i) \in R^{\ominus 1}(K)$. If $\tau_i < \tau_i'$ the run progresses by continuous evolution. Since $x(\tau_i) \in Inv_F(K, J)$, then either

1) $\tau_i' = \infty$ and $x(t) \in K$ for all $t \geq \tau_i$;
2) $\tau_i' < \infty$, $x(\tau_i') \in J$ and $x(t) \in K$ for all $t \in [\tau_i, \tau_i']$.

Notice that $x(\tau_i') \in K = Pre_H^{\forall}(K)$, and, in particular, $x(\tau_i') \in R^{\ominus 1}(K)$. Therefore, $x(\tau_{i+1}) \in R(x(\tau_i')) \subseteq K$. The claim follows by induction.

Notice that in the last argument $R(x(\tau_i'))$ may, in fact, be empty. In this case the run "blocks," in the sense that there exist no infinite runs starting at $x(\tau_i')$. The conclusion that all runs

starting at x_0 are viable in K is still true however. To preclude this somewhat unrealistic situation, one can add Assumption 1 to the lemma and subsequent Theorem 5. ■

Proof of Theorem 5

The proof makes use of the sequence of sets constructed by the Invariance Kernel Algorithm, that is, the sets $K_0 = K$, $K_{i+1} = Pre_H^{\forall}(K_i)$. Let

$$K_\infty = \bigcap_{i=0}^{\infty} K_i.$$

The proof proceeds in a sequence of steps. We show that

1) for every invariant set $L \subseteq K$, $L \subseteq Inv_H(K)$;
2) K_∞ is closed;
3) $Inv_H(K) \subseteq K_\infty$;
4) $K_\infty = Pre_H^{\forall}(K_\infty)$.

Steps 2) and 4) and Lemma 7 imply that K_∞ is invariant. Therefore, by Step 1), $K_\infty \subseteq Inv_H(K)$, and, by Step 3), $K_\infty = Inv_H(K)$. Summarizing, $Inv_H(K)$ is the largest [(by Step 1)], closed [(by Step 2)], invariant [(by Step 4)] subset of K.

Step 1: Every set $L \subseteq K$ which invariant under (X, F, R, J) must be contained in $Inv_H(K)$, since all runs starting in L stay in L, and, therefore, in K.

Step 2: Clearly, for all i, $K_{i+1} \subseteq Inv_F(K_i, J) \subseteq K_i$. Since K is closed, K_0 is closed. Moreover, if K_i is closed, then $Inv_F(K_i, J)$ is closed (by Lemma 6, since J is closed), $R^{\ominus 1}(K_i)$ is closed (since R is lower semicontinuous), and, therefore, K_{i+1} is closed. By induction, the K_i form a sequence of nested closed sets, and, therefore, K_∞ is closed (or the empty set).

Step 3: Consider a point $x_0 \in Inv_H(K)$ and show that $x_0 \in K_\infty$. Assume, for the sake of contradiction, that $x_0 \notin K_\infty$. Then there exists $N \geq 0$ such that $x \notin K_N$. If $N = 0$, then $x_0 \notin K_0 = K$, therefore, there exists a (trivial) run starting at x_0 that is not viable in K. This contradicts the assumption that $x_0 \in Inv_H(K)$. If $N > 0$, we show that there exists a run stating at x_0 that after at most one discrete transition finds itself outside K_{N-1}. The claim then follows by induction. Indeed, since $x_0 \notin K_N$ we must either have $x_0 \notin Inv_F(K_{N-1}, J)$, or $x_0 \notin R^{\ominus 1}(K_{N-1})$. If $x_0 \notin R^{\ominus 1}(K_{N-1})$, there exists $x_1 \in R(x_0)$ such that $x_1 \notin K_{N-1}$, i.e., there exists a run starting at x_0 that transitions outside K_{N-1}. If, on the other hand, $x_0 \notin Inv_F(K_{N-1}, J)$, then $x_0 \notin J \cap K_{N-1}$. Therefore, either $x_0 \notin K_{N-1}$ (and the proof is complete), or $x_0 \notin J$ and continuous evolution is possible. In the latter case, since $x_0 \notin Inv_F(K_{N-1}, J)$, by Lemma 6 there exists a solution to $\dot{x} \in F(x)$ starting at x_0 that leaves K_{N-1} before reaching J. This solution is a run of (X, F, R, J) that leaves K_{N-1}.

Step 4: Recall that $Pre_H^{\forall}(K_\infty) \subseteq K_\infty$. Consider an arbitrary $x_0 \in K_\infty$ and show that $x_0 \in Pre_H^{\forall}(K_\infty)$. Assume, for the sake of contradiction, that $x_0 \notin Inv_F(K_\infty, J) \cap R^{\ominus 1}(K_\infty)$. Then there exists a run (τ, x) starting at x_0 and a $t \preceq \tau_1$ such that[2] $x(t) \notin K_\infty$, or, in other words, there exists a run (τ, x), a $t \preceq \tau_1$ and a $N \geq 0$ such that $x(t) \notin K_N$.

[2]If $\tau = [\tau_0, \tau_0']$ or $\tau = [\tau_0, \tau_0'[$, $t \preceq \tau_1$ should be replaced by $t \preceq \tau_0$ or, respectively, $t \prec \tau_0$.

To see this notice that either $x(\tau_0) \notin R^{\ominus 1}(K_\infty)$ [in which case we can take $\tau_0' = \tau_0$, $x(\tau_1) \notin K_\infty$ and $t = \tau_1$] or $x(\tau_0) \notin Inv_F(K_\infty, J)$ [in which case there exists a solution to $\dot{x} \in F(x)$ that leaves K before reaching J]. The same argument, however, also shows that $x(\tau_0) = x_0 \notin K_{N+1}$, which contradicts the assumption that $x_0 \in K_\infty$. ■

Proof of Lemma 8

If $N \leq 1$ there is nothing to prove. If $N > 1$, $x_0 \in K_N$ implies that $x_0 \in Inv_F(K_{N-1}, J) \cap R^{\ominus 1}(K_{N-1})$. Consider an arbitrary run $(\tau, x) \in \mathcal{R}_H(x_0)$ (if no such run exists the proof is complete). If $\tau_0 = \tau_0'$, then $x(\tau_1) \in R(x_0) \subseteq K_{N-1}$, since $x_0 \in R^{\ominus 1}(K_{N-1})$. If $\tau_0' > \tau_0$, (τ, x) starts by continuous evolution. Since $x_0 \in Inv_F(K_{N-1}, J)$, $x(t)$ remains in K_{N-1} throughout this continuous evolution. If $\tau_0' = \infty$ the proof is complete. If $\tau_0' < \infty$, $x(\tau_0') \in K_{N-1} = Inv_F(K_{N-2}, J) \cap R^{\ominus 1}(K_{N-2})$. Therefore, $x(\tau_1) \in R(x(\tau_0')) \subseteq K_{N-2}$. Therefore, all runs starting at $x_0 \in K_N$ will end up in K_{N-2} after one transition. The claim follows by induction. ■

ACKNOWLEDGMENT

The authors would like to thank one of the anonymous reviewers for their detailed comments and suggestions. J. Lygeros and M. Quincampoix would also like to thank S. Plaskacz for helpful discussions.

REFERENCES

[1] "Special issue on hybrid control systems," *IEEE Trans. Automat. Contr.*, vol. 43, Apr. 1998.
[2] "Special issue on hybrid systems," *Automatica*, vol. 35, no. 3, Mar. 1999.
[3] "Special issue on hybrid systems," *Syst. Control Lett.*, vol. 38, no. 3, October 1999.
[4] "Special issue on hybrid systems: Theory and applications," *Proc. IEEE*, vol. 88, July 2000.
[5] R. Alur, C. Courcoubetis, N. Halbawachs, T. A. Henzinger, P. H. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine, "The algorithmic analysis of hybrid systems," *Theoret. Comp. Sci.*, vol. 138, pp. 3–34, 1995.
[6] T. Henzinger, P. Kopke, A. Puri, and P. Varaiya, "What's decidable about hybrid automata," in *Proc. 27th Annual Symp. Theory Computing, STOC'95*: ACM Press, 1995, pp. 373–382.
[7] N. Lynch, R. Segala, F. Vaandrager, and H. B. Weinberg, "Hybrid I/O automata," in *Hybrid Systems III*. New York: Springer-Verlag, 1996, number 1066 in LNCS, pp. 496–510.
[8] G. Lafferriere, G. J. Pappas, and S. Sastry, "O-minimal hybrid systems," *Math. Control, Signals, Systems*, vol. 13, no. 1, pp. 1–21, Mar. 2000.
[9] R. Alur, T. A. Henzinger, G. Lafferriere, and G. J. Pappas, "Discrete abstractions of hybrid systems," *Proc. IEEE*, vol. 88, pp. 971–984, July 2000.
[10] O. Maler, A. Pnueli, and J. Sifakis, "On the synthesis of discrete controllers for timed systems," in *Theoretical Aspects of Computer Science*. New York: Springer-Verlag, 1995, number 900 in LNCS, pp. 229–242.
[11] H. Wong-Toi, "The synthesis of controllers for linear hybrid automata," in *IEEE Conf. Decision Control*, San Diego, CA, Dec. 10–12, 1997, pp. 4607–4613.
[12] J. Lygeros, C. Tomlin, and S. Sastry, "Controllers for reachability specifications for hybrid systems," *Automatica*, pp. 349–370, Mar. 1999.
[13] C. J. Tomlin, J. Lygeros, and S. S. Sastry, "A game theoretic approach to controller design for hybrid systems," *Proc. IEEE*, vol. 88, pp. 949–969, July 2000.
[14] X. D. Koutsoukos, P. J. Antsaklis, J. A. Stiver, and M. D. Lemmon, "Supervisory control of hybrid systems," *Proc. IEEE*, vol. 88, pp. 1026–1049, July 2000.
[15] E. Asarin, O. Bournez, T. Dang, O. Maler, and A. Pnueli, "Effective synthesis of switching controllers for linear systems," *Proc. IEEE*, vol. 88, pp. 1011–1025, July 2000.

[16] R. Vidal, S. Schaffert, J. Lygeros, and S. Sastry, "Controlled invariance of discrete time systems," in *Hybrid Systems: Computation and Control*, N. Lynch and B. H. Krogh, Eds. New York: Springer-Verlag, 2000, number 1790 in LNCS, pp. 437–450.

[17] A. Puri, P. Varaiya, and V. Borkar, "ϵ-approximation of differential inclusions," in *Proc. IEEE Conf. Decision Control*, New Orleans, LA, 1995, pp. 2892–2897.

[18] A. B. Kurzhanski and P. Varaiya, "Ellipsoidal techniques for reachability analysis," in *Hybrid Systems: Computation and Control*, N. Lynch and B. H. Krogh, Eds. New York: Springer-Verlag, 2000, number 1790 in LNCS, pp. 202–214.

[19] E. Asarin, O. Bournez, T. Dang, and O. Maler, "Approximate reachability analysis of piecewise-linear dynamical systems," in *Hybrid Systems: Computation and Control*, N. Lynch and B. H. Krogh, Eds. New York: Springer-Verlag, 2000, number 1790 in LNCS.

[20] 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*, E. Brinksma, W. Cleaveland, K. Larsen, T. Margaria, and B. Steffen, Eds. New York: Springer-Verlag, 1995, number 1019 in LNCS, pp. 41–71.

[21] R. Alur and R. P. Kurshan, "Timing analysis in COSPAN," in *Hybrid Systems III*. New York: Springer-Verlag, 1996, number 1066 in LNCS, pp. 220–231.

[22] C. Daws Daws, A. Olivero, S. Trypakis, and S. Yovine, "The tool KRONOS," in *Hybrid Systems III*, R. Alur, T. Henzinger, and E. Sontag, Eds. New York: Springer-Verlag, 1996, number 1066 in LNCS, pp. 208–219.

[23] J. Bengtsson, K. G. Larsen, F. Larsson, P. Petterson, and W. Yi, "UPAAL: A tool suit for automatic verification of real-time systems," in *Hybrid Systems III*. New York: Springer-Verlag, 1996, number 1066 in LNCS, pp. 232–243.

[24] T. Dang and O. Maler, "Reachability analysis via face lifting," in *Hybrid Systems: Computation and Control*, S. Sastry and T. A. Henzinger, Eds. New York: Springer-Verlag, 1998, number 1386 in LNCS, pp. 96–109.

[25] M. R. Greenstreet and I. Mitchell, "Integrating projections," in *Hybrid Systems: Computation and Control*, S. Sastry and T. A. Henzinger, Eds. New York: Springer-Verlag, 1998, number 1386 in LNCS, pp. 159–174.

[26] A. Chutinam and B. Krogh, "Verification of polyhedral-invariant hybrid automata using polygonal flow pipe approximations," in *Hybrid Systems: Computation and Control*, F. W. Vaandrager and J. H. van Schuppen, Eds. New York: Springer-Verlag, 1999, number 1569 in LNCS, pp. 76–90.

[27] O. Botchkarev and S. Tripakis, "Verification of hybrid systems with linear differential inclusions using ellipsoidal approximations," in *Hybrid Systems: Computation and Control*, N. Lynch and B. H. Krogh, Eds. New York: Springer-Verlag, 2000, number 1790 in LNCS, pp. 73–88.

[28] I. Mitchell and C. J. Tomlin, "Level set methods for computation in hybrid systems," in *Hybrid Systems: Computation and Control*, N. Lynch and B. H. Krogh, Eds. New York: Springer-Verlag, 2000, number 1790 in LNCS, pp. 310–323.

[29] Z. Manna and STeP Group, "STeP: The Stanford Temporal Prover," Computer Science Department, Stanford University, Stanford, CA, Tech. Rep. STAN-CS-TR-94-1518, July 1994.

[30] J.-P. Aubin, *Viability Theory*. Boston, MA: Birkhäuser, 1991.

[31] P. Cardaliaguet, M. Quincampoix, and P. Saint-Pierre, "Set-valued numerical analysis for optimal control and differential games," in *Stochastic and Differential Games: Theory and Numerical Methods*, M Bardi, T. E. S. Raghavan, and T. Parthasarathy, Eds. Boston, MA: Birkhäuser, 1999, number 4 in Annals of the International Society of Dynamic Games, pp. 177–247.

[32] E. Cruck, R. Moitie, and N. Seube, "Estimation of basins of attraction for uncertain systems," ENSIETA, Brest, France, Tech. Rep., 1999.

[33] P. Saint-Pierre, "Approximation of viability kernels and capture basins for hybrid systems," in *European Control Conf.*, Porto, Portugal, September 4–7, 2001, pp. 2776–2783.

[34] J.-P. Aubin and H. Frankowska, *Set Valued Analysis*. Boston, MA: Birkhäuser, 1990.

[35] R. T. Rockafellar and R. J.-B. Wets, *Variational Analysis*. New York: Springer-Verlag, 1998.

[36] J. M. Davoren and A. Nerode, "Logics for hybrid systems," *Proc. IEEE*, vol. 88, pp. 985–1010, July 2000.

[37] J. Lygeros, K. H. Johansson, S. Sastry, and M. Egerstedt, "On the existence of executions of hybrid automata," in *Proc. IEEE Conf. Decision Control*, Phoenix, AZ, Dec. 7–10, 1999, pp. 2249–2254.

[38] K. H. Johansson, M. Egerstedt, J. Lygeros, and S. Sastry, "On the regularization of Zeno hybrid automata," *Syst. Control Lett.*, vol. 38, pp. 141–150, 1999.

[39] J. Zhang, K. H. Johansson, J. Lygeros, and S. Sastry, "Zeno hybrid systems," *Int. J. Robust Nonlinear Control*, vol. 11, pp. 435–451, 2001.

[40] A. Bensoussan and J.-L. Lions, *Impulse Control of Quasi-Variational Inequalities*. Paris, France: Gauthier-Villars, 1984.

[41] J. Lygeros and S. Sastry, "Hybrid systems: Modeling, analysis and control," Electronic Research Laboratory, University of California, Berkeley, CA, Tech. Rep. UCB/ERL M99/34, EECS 291E lecture notes and class projects, 1999.

[42] M. Quincampoix and V. Veliov, "Viability with target: Theory and applications," in *Applications of Mathematics in Engineering*, B. I. Cheshankov and M. D. Todorov, Eds. Sofia, Bulgaria: Heron Press, 1998, pp. 47–54.

[43] M. Quincampoix, "Differential inclusions and target problems," *SIAM J. Control Optim.*, vol. 30, no. 2, pp. 324–335, 1992.

[44] P. Hitchcock and D. Park, "Induction rules and termination proofs," in *Automata, Languages and Programming*. Amsterdam, The Netherlands: North-Holland, 1973, pp. 225–251.

Jean-Pierre Aubin is Professor of Mathematics at the Université Paris-Dauphine. He is the author of 17 books on numerical analysis, functional analysis, convex and nonlinear analysis and optimization, set-valued analysis, morphological and mutational analysis, mathematical economics and game theory, neural networks and qualitative physics, differential inclusions, and viability theory.

John Lygeros received the B.Eng. degree in electrical and electronic engineering, the M.Sc. degree in control and systems, both from Imperial College of Science Technology and Medicine, London, U.K., and the Ph.D. degree from the Electrical Engineering and Computer Sciences Department of the University of California, Berkeley, in 1990, 1991, and 1996, respectively.

Between June 1996 and December 1999, he held Postdoctoral Research appointments with the Electrical Engineering and Computer Sciences Department, University of California, Berkeley, and the Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge. In parallel, he also held a part-time Research Engineer position at SRI International, Menlo Park, CA (May 1998 to December 1999), and a Visiting Professor position at the Mathematics Department of the Université de Bretagne Occidentale, Brest, France. He is currently a University Lecturer at the Department of Engineering, University of Cambridge, U.K. His research interests include hierarchical, hybrid and nonlinear control theory and their applications to large scale systems such as Highway Systems, Air Traffic Management, and power networks.

Marc Quincampoix He received the Ph.D. degree in 1991 at the Université Paris-Dauphine in 1991, and received his "habilitation" in 1996.

Since 1996, he has been a Professor in the Department de Mathematics of the Université de Bretagne Occidentale, Brest, France. He was Maître de Conférences at the Department de Mathematics of Université de Tours, France, from 1991 to 1994 and at the Department de Mathematics of Université Paris-Dauphine, from 1994 to 1996. His fields of interests are control theory, differential inclusions, differential games, deterministic and stochastic viability.

Shankar Sastry (S'79–M'80–SM'90–F'95) received the Ph.D. degree from the University of California, Berkeley, in 1981.

He became Chairman, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley in January, 2001. The previous year, he served as Director of the Information Technology Office at DARPA. From 1996 to 1999, he was the Director of the Electronics Research Laboratory at Berkeley, an organized research unit on the Berkeley campus conducting research in computer sciences and all aspects of electrical engineering. During his Directorship from 1996 to 1999, the laboratory grew from 29 M to 50 M in volume of extra-mural funding. He is a Professor of Electrical Engineering and Computer Sciences and a Professor of Bioengineering. He was on the faculty of the Massachusetts Institute of Technology (MIT), Cambridge, as an Assistant Professor from 1980 to 1982, and of Harvard University, Cambridge, MA, as a chaired Gordon McKay Professor in 1994. He has held visiting appointments at the Australian National University, Canberra, the University of Rome, Scuola Normale, and the University of Pisa, Italy, the CNRS laboratory LAAS in Toulouse (poste rouge), Professor Invite at Institut National Polytechnique de Grenoble (CNRS Laboratory VERIMAG), and as a Vinton Hayes Visiting Fellow at the Center for Intelligent Control Systems at MIT. His areas of research are embedded and autonomous software, computer vision, computation in novel substrates such as DNA, nonlinear and adaptive control, robotic telesurgery, control of hybrid systems, embedded systems, sensor networks, and biological motor control. His latest book is *Nonlinear Systems: Analysis, Stability and Control* (New York: Springer-Verlag, 1999). He has coauthored over 250 technical papers and six books, including *Adaptive Control: Stability, Convergence and Robustness* (Upper Saddle River, NJ: Prentice Hall, 1989) and *A Mathematical Introduction to Robotic Manipulation* (Boca Raton, FL: CRC Press, 1994). He has coedited *Hybrid Control II, Hybrid Control IV* and *Hybrid Control V* (New York: Springer Lecture Notes in Computer Science, 1995, 1997, and 1999, respectively) and coedited *Hybrid Systems: Computation and Control* (New York: Springer-Verlag Lecture Notes in Computer Science, 1998) and *Essays in Mathematical Robotics* (New York: Springer-Verlag IMA Series). Books on Embedded Software and Structure from Motion in Computer Vision are in progress.

Dr. Sastry served as Associate Editor for numerous publications, including the IEEE TRANSACTIONS ON AUTOMATIC CONTROL, IEEE CONTROL MAGAZINE, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS, *Journal of Mathematical Systems, Estimation and Control*, *IMA Journal of Control and Information*, *International Journal of Adaptive Control and Signal Processing*, *Journal of Biomimetic Systems and Materials*. He was elected into the National Academy of Engineering in 2001 "for pioneering contributions to the design of hybrid and embedded systems." He also received the President of India Gold Medal in 1977, the IBM Faculty Development award for 1983–1985, the NSF Presidential Young Investigator Award in 1985 and the Eckman Award of the of the American Automatic Control Council in 1990, an M.A. (honoris causa) from Harvard in 1994, the distinguished Alumnus Award of the Indian Institute of Technology in 1999, and the David Marr prize for the best paper at the International Conference in Computer Vision in 1999.

Nicolas Seube received the Ph.D. degree in mathematics from Paris-Dauphine University in 1991.

He has been with the Automatic Control Department of Ensieta (Ecole Nationale des ingénieurs des Etudes et Techniques d'Armement), Brest, France, since 1994, where he is currently Associate Professor. His research interest include control theory, stabilization of nonlinear systems, and viability theory.