

# Symbolic models for nonlinear control systems without stability assumptions

Majid Zamani<sup>1</sup>, Giordano Pola<sup>2</sup> and Paulo Tabuada<sup>1</sup>

<sup>1</sup>Department of Electrical Engineering  
University of California at Los Angeles  
Los Angeles, CA 90095

E-mail: {zamani, tabuada}@ee.ucla.edu

<sup>2</sup>Department of Electrical and Information Engineering  
Center of Excellence DEWS, University of LAquila  
Poggio di Roio, 67040 LAquila, Italy  
E-mail: giordano.pola@ing.univaq.it

**Abstract**—In this paper we take an important step in our quest to synthesize correct-by-design embedded control software for nonlinear systems. We have shown in previous work that by relying on diverse stability and stabilizability assumptions it is possible to construct finite-state models describing the dynamics of nonlinear control systems. Such finite-state models enable the use of algorithmic techniques to automatically synthesize controllers enforcing control and software requirements. In the present paper, we show that similar results can still be obtained by replacing the stability or stabilizability assumptions by the much weaker assumption of incremental forward completeness. We illustrate the new results by synthesizing a controller for an inverted pendulum.

## I. INTRODUCTION

Symbolic models are abstract descriptions of control systems in which several states are represented by a symbol. Each symbol can thus be seen as an abstract representation for a collection of states that share similar dynamical properties. Past research has shown that symbolic models exist for several classes of systems such as timed automata [AD90], rectangular hybrid automata [HKPV98], o-minimal hybrid systems [LPS00], [BM05], multi-affine control systems [HCS06], some classes of polynomial systems [RCT05], etc. These references also showed that when the symbolic models have finitely many states, problems of verification or controller synthesis can be algorithmically solved.

Among the many different technical approaches employed to compute symbolic models, the present paper

This work has been partially supported by the National Science Foundation award 0717188, 0820061 and the Center of Excellence for Research DEWS, University of LAquila, Italy.

follows the use of approximate simulations and bisimulations. This concept, introduced in [GP07] and in [Tab08] using set-valued output maps, was successfully applied to incrementally input-to-state stable systems with and without disturbances in [PGT08], [PT09] and to incrementally stable switched systems in [GPT09]. All of these results relied on suitable stability assumptions to establish the existence of symbolic models. In this paper we show that symbolic models still exist even if we no longer make any stability assumptions. Instead, we rely on the notion of incremental forward completeness which is the incremental version of forward completeness. This is a much milder assumption that can be given by simple Lyapunov characterizations in the spirit of [AS99]. The main contribution of this paper is to show that for every nonlinear control system satisfying the incremental forward completeness assumption we can construct a symbolic model that:

- is approximately and alternately simulated by the control system;
- approximately simulates the control system.

Such relationships are weaker than the approximate bisimulation relationships established in [PGT08], [PT09], [Gir07], [GPT09] but they apply to a much wider class of control systems as they no longer require stability. Moreover, the relationships established in this paper are still sufficient to guarantee that any controller synthesized for the symbolic model enforces the desired specifications on the original control system. However, we can no longer guarantee, as in [PGT08], [PT09], [Gir07], that existence of a controller for the original con-

trol system also guarantees the existence of a controller for the symbolic model.

Our technical results are illustrated on an inverted pendulum that fails to satisfy the stability assumptions of the previous works and for which a controller can be found using the new results in this paper.

## II. CONTROL SYSTEMS AND INCREMENTAL FORWARD COMPLETENESS

### A. Notation

The identity map on a set  $A$  is denoted by  $1_A$ . If  $A$  is a subset of  $B$  we denote by  $\iota_A : A \hookrightarrow B$  or simply by  $\iota$  the natural inclusion map taking any  $a \in A$  to  $\iota(a) = a \in B$ . The symbols  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{R}$ ,  $\mathbb{R}^+$  and  $\mathbb{R}_0^+$  denote the set of natural, integer, real, positive, and nonnegative real numbers, respectively. Given a vector  $x \in \mathbb{R}^n$  we denote by  $x_i$  the  $i$ -th element of  $x$  and by  $\|x\|$  the infinity norm of  $x$ ; we recall that  $\|x\| = \max\{|x_1|, |x_2|, \dots, |x_n|\}$ , where  $|x_i|$  denotes the absolute value of  $x_i$ . A function  $f : [a, b] \rightarrow \mathbb{R}^n$  is said to be absolutely continuous on  $[a, b]$  if for any  $\varepsilon \in \mathbb{R}^+$  there exists  $\delta \in \mathbb{R}^+$  so that for every  $k \in \mathbb{N}$  and for every sequence of points  $a \leq a_1 < b_1 < a_2 < b_2 < \dots < a_k < b_k \leq b$ , if  $\sum_{i=1}^k (b_i - a_i) < \delta$  then  $\sum_{i=1}^k |f(b_i) - f(a_i)| < \varepsilon$ . A function  $f : ]a, b[ \rightarrow \mathbb{R}^n$  is said to be locally absolutely continuous if the restriction of  $f$  to any compact subset of  $]a, b[$  is absolutely continuous. Given a measurable function  $f : \mathbb{R}_0^+ \rightarrow \mathbb{R}^n$ , the (essential) supremum of  $f$  is denoted by  $\|f\|_\infty$  where  $\|f\|_\infty := \sup\{\|f(t)\|, t \geq 0\}$ ;  $f$  is essentially bounded if  $\|f\|_\infty < \infty$ . For a given time  $\tau \in \mathbb{R}^+$ , define  $f_\tau$  so that  $f_\tau(t) = f(t)$ , for any  $t \in [0, \tau]$ , and  $f_\tau(t) = 0$  elsewhere;  $f$  is said to be locally essentially bounded if for any  $\tau \in \mathbb{R}^+$ ,  $f_\tau$  is essentially bounded. The closed ball centered at  $x \in \mathbb{R}^n$  with radius  $\varepsilon$  is defined by  $\mathcal{B}_\varepsilon(x) = \{y \in \mathbb{R}^n \mid \|x - y\| \leq \varepsilon\}$ . For any  $A \subseteq \mathbb{R}^n$  and  $\mu \in \mathbb{R}^+$  set  $[A]_\mu = \{a \in A \mid a_i = k_i \mu, k_i \in \mathbb{Z}, i = 1, \dots, n\}$ . The set  $[A]_\mu$  will be used as an approximation of the set  $A$  with precision  $\mu$ . Geometrically, for any  $\mu \in \mathbb{R}^+$  and  $\lambda \geq \mu/2$  the collection of sets  $\{\mathcal{B}_\lambda(q)\}_{q \in [\mathbb{R}^n]_\mu}$  is a covering of  $\mathbb{R}^n$ , i.e.  $\mathbb{R}^n \subseteq \bigcup_{q \in [\mathbb{R}^n]_\mu} \mathcal{B}_\lambda(q)$ . Moreover, for any  $\lambda < \mu/2$ ,  $\mathbb{R}^n \not\subseteq \bigcup_{q \in [\mathbb{R}^n]_\mu} \mathcal{B}_\lambda(q)$ . A continuous function  $\gamma : \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+$ , is said to belong to class  $\mathcal{K}$  if it is strictly increasing and  $\gamma(0) = 0$ ;  $\gamma$  is said to belong to class  $\mathcal{K}_\infty$  if  $\gamma \in \mathcal{K}$  and  $\gamma(r) \rightarrow \infty$  as  $r \rightarrow \infty$ . A continuous function  $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+$  is said to belong to class  $\mathcal{KL}$  if, for each fixed  $s$ , the map  $\beta(r, s)$  belongs to class  $\mathcal{K}_\infty$  with respect to  $r$  and, for each fixed  $r$ , the map  $\beta(r, s)$  is decreasing with respect to  $s$  and  $\beta(r, s) \rightarrow 0$  as

$s \rightarrow \infty$ . We identify a relation  $R \subseteq A \times B$  with the map  $R : A \rightarrow 2^B$  defined by  $b \in R(a)$  iff  $(a, b) \in R$ . Given a relation  $R \subseteq A \times B$ ,  $R^{-1}$  denotes the inverse relation defined by  $R^{-1} = \{(b, a) \in B \times A : (a, b) \in R\}$ .

### B. Control Systems

The class of control systems that we consider in this paper is formalized in the following definition.

*Definition 2.1:* A control system is a quadruple:

$$\Sigma = (\mathbb{R}^n, U, \mathcal{U}, f),$$

where:

- $\mathbb{R}^n$  is the state space;
- $U \subseteq \mathbb{R}^m$  is the input space;
- $\mathcal{U}$  is a subset of the set of all functions of time from intervals of the form  $]a, b[ \subseteq \mathbb{R}$  to  $U$  with  $a < 0$  and  $b > 0$  satisfying the following Lipschitz assumption: there exists a positive constant  $M$  such that  $\|v(t) - v(t')\| \leq M|t - t'|$  for all  $v \in \mathcal{U}$  and for all  $t, t' \in ]a, b[$ .
- $f : \mathbb{R}^n \times U \rightarrow \mathbb{R}^n$  is a continuous map satisfying the following Lipschitz assumption: for every compact set  $K \subset \mathbb{R}^n$ , there exists a constant  $L > 0$  such that  $\|f(x, u) - f(y, u)\| \leq L\|x - y\|$  for all  $x, y \in K$  and all  $u \in U$ .

A locally absolutely continuous curve  $\xi : ]a, b[ \rightarrow \mathbb{R}^n$  is said to be a *trajectory* of  $\Sigma$  if there exists  $v \in \mathcal{U}$  satisfying:

$$\dot{\xi}(t) = f(\xi(t), v(t)), \quad (\text{II.1})$$

for almost all  $t \in ]a, b[$ . Although we have defined trajectories over open domains, we shall refer to trajectories  $\xi : [0, \tau] \rightarrow \mathbb{R}^n$  defined on closed domains  $[0, \tau]$ ,  $\tau \in \mathbb{R}^+$  with the understanding of the existence of a trajectory  $\xi' : ]a, b[ \rightarrow \mathbb{R}^n$  such that  $\xi = \xi'|_{[0, \tau]}$ . We also write  $\xi_{xv}(\tau)$  to denote the point reached at time  $\tau$  under the input  $v$  from initial condition  $x$ ; this point is uniquely determined, since the assumptions on  $f$  ensure existence and uniqueness of trajectories [Son98]. A control system  $\Sigma$  is said to be forward complete if every trajectory is defined on an interval of the form  $]a, \infty[$ . Sufficient and necessary conditions for a system to be forward complete can be found in [AS99].

The following technical lemma will be used later in the definition of symbolic model.

*Lemma 2.2:* Let  $\Sigma = (\mathbb{R}^n, U, \mathcal{U}, f)$  be a control system and consider a parameter  $\mu \in \mathbb{R}^+$ . For any

input  $\mathcal{U} \ni v : [0, \tau] \rightarrow U$  there exists a constant input  $v_{const} : [0, \tau] \rightarrow [U]_\mu$  such that:

$$\|v - v_{const}\|_\infty \leq \frac{\mu + M\tau}{2}. \quad (\text{II.2})$$

*Proof:* We first approximate the input  $v$  by the constant input  $\hat{v} : [0, \tau] \rightarrow U$  where  $\hat{v}(t) = \frac{v(0)+v(\tau)}{2}$  for all  $t \in [0, \tau]$ . We then approximate the constant input  $\hat{v}$  by a constant input  $v_{const} : [0, \tau] \rightarrow [U]_\mu$  so that  $\|\hat{v} - v_{const}\| \leq \mu/2$ . Note that  $v_{const}$  exists since  $\bigcup_{q \in [U]_\mu} \mathcal{B}_{\mu/2}(q)$  is a covering of  $U$ . Since  $\hat{v}$  and  $v_{const}$  are constant functions, then  $\|\hat{v} - v_{const}\|_\infty = \|\hat{v} - v_{const}\|$ . Using the Lipschitz assumption for  $v$ , the resulting approximation error is given by:

$$\begin{aligned} \|v - v_{const}\|_\infty &= \|v - \hat{v} + \hat{v} - v_{const}\|_\infty \quad (\text{II.3}) \\ &\leq \|v - \hat{v}\|_\infty + \|\hat{v} - v_{const}\|_\infty \\ &= \|v - \hat{v}\|_\infty + \|\hat{v} - v_{const}\| \\ &\leq M\tau/2 + \mu/2. \end{aligned}$$

■

For later use we also define the function  $\Psi : U \rightarrow [U]_\mu$  associating to any  $v \in \mathcal{U}$  the corresponding input  $v_{const}$  as defined in the proof of Lemma 2.2.

### C. Incremental forward completeness

The results presented in this paper will assume certain incremental forward completeness assumptions that we introduce in this section. We start by recalling the notion of incremental input-to-state stability.

*Definition 2.3:* [Ang02] A control system  $\Sigma$  is incrementally input-to-state stable ( $\delta$ -ISS) if it is forward complete and there exist a  $\mathcal{KL}$  function  $\beta$  and a  $\mathcal{K}_\infty$  function  $\gamma$  such that for any  $t \in \mathbb{R}_0^+$ , any  $x, x' \in \mathbb{R}^n$ , and any  $v, v' \in \mathcal{U}$  the following condition is satisfied:

$$\|\xi_{xv}(t) - \xi_{x'v'}(t)\| \leq \beta(\|x - x'\|, t) + \gamma(\|v - v'\|_\infty). \quad (\text{II.4})$$

We now describe a weaker concept that is satisfied even in the absence of stability.

*Definition 2.4:* A control system  $\Sigma$  is incrementally forward complete ( $\delta$ -FC) if there exist continuous functions  $\beta : \mathbb{R}^+ \times \mathbb{R}^+ \rightarrow \mathbb{R}^+$  and  $\gamma : \mathbb{R}^+ \times \mathbb{R}^+ \rightarrow \mathbb{R}^+$  such that for each fixed  $s$ , the maps  $\beta(r_1, s)$  and  $\gamma(r_2, s)$  belong to class  $\mathcal{K}_\infty$  with respect to  $r_1$  and  $r_2$ , respectively, and for any  $t \in \mathbb{R}_0^+$ , any  $x, x' \in \mathbb{R}^n$  and any  $v, v' \in \mathcal{U}$  the

following condition is satisfied:

$$\|\xi_{xv}(t) - \xi_{x'v'}(t)\| \leq \beta(\|x - x'\|, t) + \gamma(\|v - v'\|_\infty, t). \quad (\text{II.5})$$

Incremental forward completeness requires the distance between two arbitrary trajectories to be bounded by the sum of two terms capturing the mismatch between the initial conditions and the mismatch between the inputs as shown in (II.5). From (II.4) and (II.5), we can immediately see that  $\delta$ -ISS implies  $\delta$ -FC. However, the converse is not true, in general, since the function  $\beta$  in (II.5) is not required to be a decreasing function of  $t$  and the function  $\gamma$  in (II.5) is allowed to depend on  $t$  while this is not the case in (II.4). Whenever the origin is an equilibrium point for  $\Sigma$ , the choice  $x' = 0, v' = 0$ , and  $\xi_{x'v'} = 0$  results in the estimate  $\|\xi_{xv}(t)\| \leq \beta(\|x\|, t) + \gamma(\|v\|_\infty, t)$  which is shown in [AS99] to be equivalent to forward completeness of  $\Sigma$ . Hence, the systems satisfying (II.5) are termed incrementally forward complete. By straightforward generalization of the results in [AS99], it is possible to drive Lyapunov characterizations of  $\delta$ -FC control systems.

## III. SYMBOLIC MODELS AND APPROXIMATE EQUIVALENCE NOTIONS

### A. Systems and control systems

We will use systems to describe both control systems as well as their symbolic models. A more detailed exposition of the notion of system that we now introduce can be found in [Tab09].

*Definition 3.1:* [Tab09] A system  $S$  is quintuple:

$$S = (X, U, \longrightarrow, Y, H),$$

consisting of:

- A set of states  $X$ ;
- A set of inputs  $U$ ;
- A transition relation  $\longrightarrow \subseteq X \times U \times X$ ;
- An output set  $Y$ ;
- An output function  $H : X \rightarrow Y$ .

A system  $(X, U, \longrightarrow, Y, H)$  is said to be:

- *metric*, if the output set  $Y$  is equipped with a metric  $d : Y \times Y \rightarrow \mathbb{R}_0^+$ ;
- *countable*, if  $X$  is a countable set;
- *finite*, if  $X$  is a finite set.

A transition  $(x, u, x') \in \longrightarrow$  is denoted by  $x \xrightarrow{u} x'$ . Note that, for such a transition  $x \xrightarrow{u} x'$ , state

$x'$  is called a  $u$ -successor, or simply successor. Since  $\longrightarrow \subseteq X \times U \times X$  is a relation, for any state and any input  $u \in U$  there may be: no  $u$ -successors, one  $u$ -successor, or many  $u$ -successors. We denote the set of  $u$ -successors of a state  $x$  by  $\mathbf{Post}_u(x)$  and by  $U(x)$  the set of inputs  $u \in U$  for which  $\mathbf{Post}_u(x)$  is nonempty. A system is deterministic if given any state  $x \in X$  and any input  $u$ , there exists at most one  $u$ -successor (there may be none). A system is called nondeterministic if it is not deterministic. Hence, for a nondeterministic system it is possible for a state to have two (or possibly more) distinct  $u$ -successors.

Systems can be used to describe control systems. Given  $\Sigma = (\mathbb{R}^n, U, \mathcal{U}, f)$ , the system associated with  $\Sigma$  and  $\tau \in \mathbb{R}^+$  is defined by:

$$S_\tau(\Sigma) := (X_\tau, U_\tau, \xrightarrow{\tau}, Y_\tau, H_\tau),$$

where:

- $X_\tau = \mathbb{R}^n$ ;
- $U_\tau = \{v_\tau \in \mathcal{U} \mid \text{the domain of } v_\tau \text{ is } [0, \tau]\}$ ;
- $x_\tau \xrightarrow{v_\tau} x'_\tau$  if there exists a trajectory  $\xi : [0, \tau] \rightarrow \mathbb{R}^n$  of  $\Sigma$  satisfying  $\xi_{x_\tau v_\tau}(\tau) = x'_\tau$ ;
- $Y_\tau = \mathbb{R}^n$ ;
- $H_\tau = 1_{\mathbb{R}^n}$ .

The above system can be thought of as the time discretization of the control system  $\Sigma$ .

## B. System relations

We first consider simulation and bisimulation relations that are useful when analyzing or synthesizing controllers for deterministic systems.

*Definition 3.2:* Let  $S_a = (X_a, U_a, \xrightarrow{a}, Y_a, H_a)$  and  $S_b = (X_b, U_b, \xrightarrow{b}, Y_b, H_b)$  be metric systems with the same output sets  $Y_a = Y_b$  and metric  $\mathbf{d}$ , and consider a precision  $\varepsilon \in \mathbb{R}^+$ . A relation  $R \subseteq X_a \times X_b$  is said to be an  $\varepsilon$ -approximate simulation relation from  $S_a$  to  $S_b$ , if the following three conditions are satisfied:

- (i) for every  $x_a \in X_a$ , there exists  $x_b \in X_b$  with  $(x_a, x_b) \in R$ ;
- (ii) for every  $(x_a, x_b) \in R$  we have  $\mathbf{d}(H_a(x_a), H_b(x_b)) \leq \varepsilon$ ;
- (iii) for every  $(x_a, x_b) \in R$  we have that :

$$x_a \xrightarrow{u_a} x'_a \text{ in } S_a \text{ implies the existence of } x_b \xrightarrow{u_b} x'_b \text{ in } S_b \text{ satisfying } (x'_a, x'_b) \in R.$$

System  $S_a$  is  $\varepsilon$ -approximately simulated by  $S_b$  or  $S_b$   $\varepsilon$ -approximately simulates  $S_a$ , denoted by  $S_a \preceq_S^\varepsilon S_b$ , if there exists an  $\varepsilon$ -approximate simulation relation from  $S_a$  to  $S_b$ .

Symmetrizing the notion of simulation we arrive at bisimulation, which we report hereafter.

*Definition 3.3:* Let  $S_a$  and  $S_b$  be metric systems with the same output sets  $Y_a = Y_b$  and metric  $\mathbf{d}$ , and consider a precision  $\varepsilon \in \mathbb{R}^+$ . A relation  $R \subseteq X_a \times X_b$  is said to be an  $\varepsilon$ -approximate bisimulation relation between  $S_a$  and  $S_b$ , if the following two conditions are satisfied:

- (i)  $R$  is an  $\varepsilon$ -approximate simulation relation from  $S_a$  to  $S_b$ ;
- (ii)  $R^{-1}$  is an  $\varepsilon$ -approximate simulation relation from  $S_b$  to  $S_a$ .

System  $S_a$  is  $\varepsilon$ -approximate bisimilar to  $S_b$ , denoted by  $S_a \cong_S^\varepsilon S_b$ , if there exists an  $\varepsilon$ -approximate bisimulation relation  $R$  between  $S_a$  and  $S_b$ .

For nondeterministic systems we need to consider relationships that explicitly capture the adversarial nature of nondeterminism. We report from [PT09] the following notion of alternating approximate simulation.

*Definition 3.4:* Let  $S_a$  and  $S_b$  be metric systems with the same output sets  $Y_a = Y_b$  and metric  $\mathbf{d}$ , and let  $\varepsilon \in \mathbb{R}^+$ . A relation  $R \subseteq X_a \times X_b$  is an  $\varepsilon$ -approximate alternating simulation relation from  $S_a$  to  $S_b$  if the following conditions are satisfied:

- (i) for every  $x_a \in X_a$ , there exists  $x_b \in X_b$  with  $(x_a, x_b) \in R$ ;
- (ii) for every  $(x_a, x_b) \in R$  we have  $\mathbf{d}(H_a(x_a), H_b(x_b)) \leq \varepsilon$ ;
- (ii) for every  $(x_a, x_b) \in R$  and for every  $u_a \in U_a(x_a)$  there exists  $u_b \in U_b(x_b)$  such that for every  $x'_b \in \mathbf{Post}_{u_b}(x_b)$  there exists  $x'_a \in \mathbf{Post}_{u_a}(x_a)$  satisfying  $(x'_b, x'_a) \in R$ .

System  $S_a$  is alternatingly  $\varepsilon$ -approximately simulated by  $S_b$  or  $S_b$  alternatingly  $\varepsilon$ -approximately simulates  $S_a$ , denoted by  $S_a \preceq_{AS}^\varepsilon S_b$ , if there exists an alternating  $\varepsilon$ -approximate simulation relation from  $S_a$  to  $S_b$ . Although alternating simulation is substantially different from simulation, these two notions coincide in the special case of deterministic systems.

IV. EXISTENCE OF SYMBOLIC MODELS  
FOR  $\delta$ -FC CONTROL SYSTEMS

We now have all the ingredients to define a symbolic model that will be used to approximate a control system. Given a  $\delta$ -FC control system  $\Sigma = (\mathbb{R}^n, U, \mathcal{U}, f)$ , a desired precision  $\varepsilon$ , any time quantization  $\tau \in \mathbb{R}^+$ , state space quantization  $\eta \in \mathbb{R}^+$ , and input space quantization  $\mu \in \mathbb{R}^+$  we define the system:

$$S_{\tau\eta\mu\varepsilon}(\Sigma) := (X_{\tau\eta\mu\varepsilon}, U_{\tau\eta\mu\varepsilon}, \xrightarrow{\tau\eta\mu\varepsilon}, Y_{\tau\eta\mu\varepsilon}, H_{\tau\eta\mu\varepsilon}), \quad (\text{IV.1})$$

by:

- $X_{\tau\eta\mu\varepsilon} = [\mathbb{R}^n]_\eta$ ;
- $U_{\tau\eta\mu\varepsilon} = \Psi(U_\tau)$ ;
- $x_{\tau\eta\mu\varepsilon} \xrightarrow{\tau\eta\mu\varepsilon} x'_{\tau\eta\mu\varepsilon}$  if any of the following two conditions is satisfied:
  - a)  $\|\xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau) - x'_{\tau\eta\mu\varepsilon}\| \leq \eta/2$  and  $\beta(\varepsilon, \tau) + \gamma(\frac{\mu+M\tau}{2}, \tau) < \varepsilon/2$ ;
  - b)  $\|\xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau) - x'_{\tau\eta\mu\varepsilon}\| \leq \beta(\varepsilon, \tau) + \gamma(\frac{\mu+M\tau}{2}, \tau)$  and  $\beta(\varepsilon, \tau) + \gamma(\frac{\mu+M\tau}{2}, \tau) \geq \varepsilon/2$ ;
- $Y_{\tau\eta\mu\varepsilon} = \mathbb{R}^n$ ;
- $H_{\tau\eta\mu\varepsilon} = \iota : X_{\tau\eta\mu\varepsilon} \hookrightarrow Y_{\tau\eta\mu\varepsilon}$ .

The function  $\Psi$  in the above definition was defined at the end of Subsection II-B. Note that for a given control system  $\Sigma$  either a) or b) are satisfied. Hence, the choice between a) and b) is made only once and before the construction of any transition. We stress that while system  $S_\tau(\Sigma)$  is not countable, system  $S_{\tau\eta\mu\varepsilon}(\Sigma)$  is so and it becomes finite, when the state space of the control system  $\Sigma$  is bounded.

We can now state the main result, relating  $\delta$ -FC to the existence of symbolic models.

*Theorem 4.1:* Let  $\Sigma$  be a  $\delta$ -FC control system. For any desired precision  $\varepsilon \in \mathbb{R}^+$ , and for any  $\tau \in \mathbb{R}^+$ ,  $\mu \in \mathbb{R}^+$ , and  $\eta \in \mathbb{R}^+$  satisfying  $\eta \leq \varepsilon$ , we have:

$$S_{\tau\eta\mu\varepsilon}(\Sigma) \preceq_{\mathcal{AS}}^\varepsilon S_\tau(\Sigma) \preceq_S^\varepsilon S_{\tau\eta\mu\varepsilon}(\Sigma).$$

*Proof:* We start by proving  $S_\tau(\Sigma) \preceq_S^\varepsilon S_{\tau\eta\mu\varepsilon}(\Sigma)$ . Consider the relation  $R \subseteq X_\tau \times X_{\tau\eta\mu\varepsilon}$  defined by  $(x_\tau, x_{\tau\eta\mu\varepsilon}) \in R$  if and only if  $\|H_\tau(x_\tau) - H_{\tau\eta\mu\varepsilon}(x_{\tau\eta\mu\varepsilon})\| = \|x_\tau - x_{\tau\eta\mu\varepsilon}\| \leq \varepsilon$ . For every  $x_\tau \in X_\tau$  and since  $X_\tau \subseteq \bigcup_{q \in [\mathbb{R}^n]_\eta} \mathcal{B}_{\eta/2}(q)$ , there exists  $x_{\tau\eta\mu\varepsilon} \in X_{\tau\eta\mu\varepsilon}$  such that:

$$\|x_\tau - x_{\tau\eta\mu\varepsilon}\| \leq \eta/2 \leq \varepsilon. \quad (\text{IV.2})$$

Hence,  $(x_\tau, x_{\tau\eta\mu\varepsilon}) \in R$  and condition (i) in Definition 3.2 is satisfied. Now consider any  $(x_\tau, x_{\tau\eta\mu\varepsilon}) \in R$ . Condition (ii) in Definition 3.2 is satisfied by definition of  $R$ . Let us now show that condition (iii) in Definition 3.2 holds.

Consider any  $v_\tau \in U_\tau$  and the transition  $x_\tau \xrightarrow{v_\tau} x'_\tau = \xi_{x_\tau v_\tau}(\tau)$  in  $S_\tau(\Sigma)$ . Choose an input  $u_{\tau\eta\mu\varepsilon} \in U_{\tau\eta\mu\varepsilon}$  satisfying:

$$\|v_\tau - u_{\tau\eta\mu\varepsilon}\|_\infty \leq (\mu + M\tau)/2. \quad (\text{IV.3})$$

Note that existence of such  $u_{\tau\eta\mu\varepsilon}$  is a consequence of Lemma 2.2. It follows from the  $\delta$ -FC assumption that the distance between  $x'_\tau$  and  $\xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau)$  is bounded as:

$$\|x'_\tau - \xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau)\| \leq \beta(\varepsilon, \tau) + \gamma((\mu + M\tau)/2, \tau). \quad (\text{IV.4})$$

We now have two cases.

**Case a:**  $\beta(\varepsilon, \tau) + \gamma((\mu + M\tau)/2, \tau) < \varepsilon/2$ .

Since  $X_\tau \subseteq \bigcup_{x_{\tau\eta\mu\varepsilon} \in [\mathbb{R}^n]_\eta} \mathcal{B}_{\eta/2}(x_{\tau\eta\mu\varepsilon})$ , there exists  $x'_{\tau\eta\mu\varepsilon} \in X_{\tau\eta\mu\varepsilon}$  such that:

$$\|\xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau) - x'_{\tau\eta\mu\varepsilon}\| \leq \eta/2. \quad (\text{IV.5})$$

From (IV.5) and the definition of transition relation, we conclude the existence of  $x_{\tau\eta\mu\varepsilon} \xrightarrow{u_{\tau\eta\mu\varepsilon}} x'_{\tau\eta\mu\varepsilon}$  in  $S_{\tau\eta\mu\varepsilon}(\Sigma)$ . Using the inequalities  $\eta \leq \varepsilon$ , (IV.4), and (IV.5), we obtain the following chain of inequalities:

$$\begin{aligned} & \|x'_\tau - x'_{\tau\eta\mu\varepsilon}\| \\ &= \|x'_\tau - \xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau) + \xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau) - x'_{\tau\eta\mu\varepsilon}\| \\ &\leq \|x'_\tau - \xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau)\| + \|\xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau) - x'_{\tau\eta\mu\varepsilon}\| \\ &\leq \beta(\varepsilon, \tau) + \gamma((\mu + M\tau)/2, \tau) + \eta/2 \leq \varepsilon. \end{aligned}$$

Hence  $(x'_\tau, x'_{\tau\eta\mu\varepsilon}) \in R$  and condition (iii) in Definition 3.2 holds.

**Case b:**  $\beta(\varepsilon, \tau) + \gamma((\mu + M\tau)/2, \tau) \geq \varepsilon/2$ .

Combining  $\beta(\varepsilon, \tau) + \gamma((\mu + M\tau)/2, \tau) \geq \varepsilon/2$  with  $\eta \leq \varepsilon$ , we obtain  $\eta/2 \leq \beta(\varepsilon, \tau) + \gamma((\mu + M\tau)/2, \tau)$ . From this inequality and (IV.4), it can be easily proved the existence of a point  $x'_{\tau\eta\mu\varepsilon} \in \mathcal{B}_{\beta(\varepsilon, \tau) + \gamma((\mu + M\tau)/2, \tau)}(\xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau)) \cap X_{\tau\eta\mu\varepsilon}$  such that  $\|x'_{\tau\eta\mu\varepsilon} - \xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau)\| \leq \eta \leq \varepsilon$ . Hence, by definition of the transition relation, we have  $x_{\tau\eta\mu\varepsilon} \xrightarrow{u_{\tau\eta\mu\varepsilon}} x'_{\tau\eta\mu\varepsilon}$ . Therefore,  $(x'_{\tau\eta\mu\varepsilon}, x'_\tau) \in R$ . Hence, condition (iii) in Definition 3.2 is satisfied from which  $S_\tau(\Sigma) \preceq_S^\varepsilon S_{\tau\eta\mu\varepsilon}(\Sigma)$  is proved.

Now we prove  $S_{\tau\eta\mu\varepsilon}(\Sigma) \preceq_{\mathcal{AS}}^\varepsilon S_\tau(\Sigma)$ . Consider the relation  $R \subseteq X_\tau \times X_{\tau\eta\mu\varepsilon}$

defined by  $(x_\tau, x_{\tau\eta\mu\varepsilon}) \in R$  if and only if  $\|H_\tau(x_\tau) - H_{\tau\eta\mu\varepsilon}(x_{\tau\eta\mu\varepsilon})\| = \|x_\tau - x_{\tau\eta\mu\varepsilon}\| \leq \varepsilon$ .

For every  $x_{\tau\eta\mu\varepsilon} \in X_{\tau\eta\mu\varepsilon}$ , by choosing  $x_\tau = x_{\tau\eta\mu\varepsilon}$  we have  $(x_\tau, x_{\tau\eta\mu\varepsilon}) \in R$  and condition (i) in Definition 3.4 is satisfied. Now consider any  $(x_\tau, x_{\tau\eta\mu\varepsilon}) \in R$ . Condition (ii) in Definition 3.4 is satisfied by definition of  $R$ . Let us now show that condition (iii) in Definition 3.4 holds. Consider any  $u_{\tau\eta\mu\varepsilon} \in U_{\tau\eta\mu\varepsilon}$ . Choose the input  $v_\tau = u_{\tau\eta\mu\varepsilon}$  and consider the transition  $x_\tau \xrightarrow{v_\tau/\tau} x'_\tau = \xi_{x_\tau v_\tau}(\tau)$  in  $S_\tau(\Sigma)$ . From the  $\delta$ -FC assumption, the distance between  $x'_\tau$  and  $\xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau)$  is bounded as:

$$\|x'_\tau - \xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau)\| \leq \beta(\varepsilon, \tau) \quad (\text{IV.6})$$

We now have two cases.

**Case a:**  $\beta(\varepsilon, \tau) + \gamma((\mu + M\tau)/2, \tau) < \varepsilon/2$ .

Since  $X_\tau \subseteq \bigcup_{x_{\tau\eta\mu\varepsilon} \in [\mathbb{R}^n]_\eta} \mathcal{B}_{\eta/2}(x_{\tau\eta\mu\varepsilon})$ , there exists  $x'_{\tau\eta\mu\varepsilon} \in \text{Post}_{u_{\tau\eta\mu\varepsilon}}(x_{\tau\eta\mu\varepsilon})$  such that:

$$\|\xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau) - x'_{\tau\eta\mu\varepsilon}\| \leq \eta/2. \quad (\text{IV.7})$$

From (IV.7) and the definition of transition relation, we conclude the existence of  $x_{\tau\eta\mu\varepsilon} \xrightarrow{u_{\tau\eta\mu\varepsilon}/\tau\eta\mu\varepsilon} x'_{\tau\eta\mu\varepsilon}$  in  $S_{\tau\eta\mu\varepsilon}(\Sigma)$ . Using the inequalities  $\eta \leq \varepsilon$ , (IV.6), and (IV.7), we obtain the following chain of inequalities:

$$\begin{aligned} & \|x'_\tau - x'_{\tau\eta\mu\varepsilon}\| \\ &= \|x'_\tau - \xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau) + \xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau) - x'_{\tau\eta\mu\varepsilon}\| \\ &\leq \|x'_\tau - \xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau)\| + \|\xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau) - x'_{\tau\eta\mu\varepsilon}\| \\ &\leq \beta(\varepsilon, \tau) + \eta/2 \leq \varepsilon. \end{aligned}$$

Hence  $(x'_\tau, x'_{\tau\eta\mu\varepsilon}) \in R$  and condition (iii) in Definition 3.4 holds.

**Case b:**  $\beta(\varepsilon, \tau) + \gamma((\mu + M\tau)/2, \tau) \geq \varepsilon/2$ .

Combining  $\beta(\varepsilon, \tau) + \gamma((\mu + M\tau)/2, \tau) \geq \varepsilon/2$  with  $\eta \leq \varepsilon$ , we obtain  $\eta/2 \leq \beta(\varepsilon, \tau) + \gamma((\mu + M\tau)/2, \tau)$ . From this inequality and (IV.4), it can be easily proved the existence of a point  $x'_{\tau\eta\mu\varepsilon} \in \mathcal{B}_{\beta(\varepsilon, \tau) + \gamma((\mu + M\tau)/2, \tau)}(\xi_{x_{\tau\eta\mu\varepsilon} u_{\tau\eta\mu\varepsilon}}(\tau)) \cap X_{\tau\eta\mu\varepsilon}$  such that  $\|x'_{\tau\eta\mu\varepsilon} - x'_\tau\| \leq \eta \leq \varepsilon$ . Hence, by definition of the transition relation,  $x'_{\tau\eta\mu\varepsilon} \in \text{Post}_{u_{\tau\eta\mu\varepsilon}}(x_{\tau\eta\mu\varepsilon})$ . Therefore,  $(x'_{\tau\eta\mu\varepsilon}, x'_\tau) \in R$ . Hence, condition (iii) in Definition 3.4 is satisfied from which  $S_{\tau\eta\mu\varepsilon}(\Sigma) \preceq_{\mathcal{AS}} S_\tau(\Sigma)$  is proved. ■

*Remark 4.2:* If we assume  $\delta$ -ISS and piecewise-constant inputs, the conclusion of Theorem 4.1 can be strengthened to  $\varepsilon$ -approximate bisimulation. For sufficiently large values of  $\tau$ , the  $\delta$ -ISS assumption guarantees  $\beta(\varepsilon, \tau) < \varepsilon/2$ ; then by choosing a sufficiently small value of  $\mu$  and combining with  $\eta \leq \varepsilon$ , we obtain

$\beta(\varepsilon, \tau) + \gamma(\mu/2) + \eta/2 < \varepsilon$ . Hence, as proved in Theorem 5.1 in [PGT08], we will have  $S_\tau(\Sigma) \cong_{\mathcal{S}}^{\varepsilon} S_{\tau\eta\mu\varepsilon}(\Sigma)$ .

## V. SYMBOLIC CONTROL DESIGN FOR AN INVERTED PENDULUM

We illustrate the results in this paper on the well known inverted pendulum. In order to make use of the software tool Pessoa<sup>1</sup> for the computation of symbolic models and synthesis of controllers, we use the following linear model for the pendulum:

$$\Sigma : \begin{cases} \dot{x}_1 = x_2, \\ \dot{x}_2 = \frac{g}{l}x_1 - \frac{k}{ml^2}x_2 + \frac{1}{ml}u. \end{cases} \quad (\text{V.1})$$

In the above model,  $x_1$  is the angular position,  $x_2$  is the velocity of the point mass,  $u$  is the applied force (control input),  $g = 9.8$  is gravity's acceleration,  $l = 0.5$  is the length of the rod,  $m = 0.5$  is the mass, and  $k = 2$  is the coefficient of rotational friction. All constants and variables are expressed in the International System. The eigenvalues of the system are  $\lambda_1 = 1.1433$  and  $\lambda_2 = -17.1433$  showing that it is unstable. We assume that  $u \in U = [-4, 4]$  and that control input is piecewise-constant. We work on the subset  $X = [-1, 1] \times [-1, 1]$  of the state space of  $\Sigma$ . In order to construct a symbolic abstraction for the preceding model, we need to find functions  $\beta$  and  $\gamma$  describing the incremental forward completeness property in (II.5). For a linear control system:

$$\dot{\xi} = A\xi + Bu, \quad \xi(t) \in \mathbb{R}^n, \quad u(t) \in U \subseteq \mathbb{R}^m,$$

the functions  $\beta$  and  $\gamma$  can be chosen as:

$$\beta(r, t) = \|e^{At}\|r; \quad \gamma(r, t) = (\|B\| \int_0^t \|e^{As}\|ds)r, \quad (\text{V.2})$$

where  $\|e^{At}\|$  denotes the infinity norm of the matrix  $e^{At}$ . For the inverted pendulum described above, the functions  $\beta$  and  $\gamma$  are given by  $\beta(r, t) = 3.6482e^{1.1433t}r$  and  $\gamma(r, t) = 12.7638(e^{1.1433t} - 1)r$ . Suppose that our objective is to design a controller forcing the trajectories to reach and stay indefinitely in the target set:  $W = [-0.06, 0.06] \times [-0.3, 0.3]$ . For a precision  $\varepsilon = 0.05$ , we choose  $\eta = 0.03$ ,  $\tau = 0.5$ , and  $\mu = 0.4$  so as to satisfy the assumptions of Theorem 4.1 and there exists a controller enforcing the states to reach and stay indefinitely in that target set. A control strategy for the mentioned target set can be obtained by using standard methods in the context of algorithmic approaches to game

<sup>1</sup>Pessoa is a software tool for the synthesis of correct-by-design embedded control systems, developed at UCLA's CyPhyLab. Pessoa is scheduled to be publicly released on November 2009.

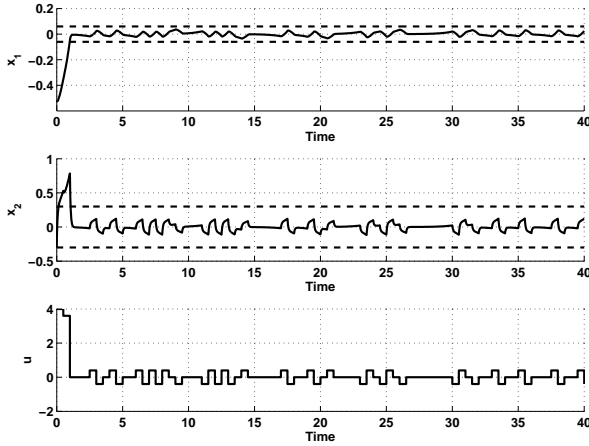


Fig. 1. Upper and medium panels: trajectory of  $(x_1, x_2)$ , with initial condition  $(-0.5196, 0.3)$ . The dashed lines define the target set bounds. Lower panel: input signal.

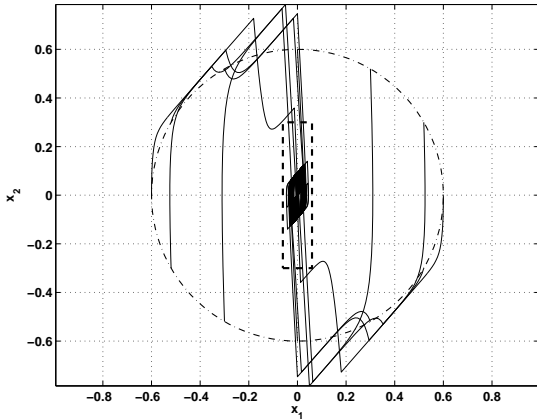


Fig. 2. Trajectories of the closed-loop system for different initial conditions on a circle with the center at the origin and radius 0.6.

theory [Tab09]. We use reachability game and safety game, both implemented in Pessoa, to reach and stay indefinitely in the target set, respectively. In Figure 1, we show the closed-loop trajectory stemming from the initial condition  $(-0.5196, 0.3)$  and the evolution of the input signal. Figure 2 shows trajectories of the system initiated with different initial conditions on the circle centered at the origin and radius 0.6. The dashed rectangle in Figure 2 is the target set. As can be seen, all the trajectories converge to the target set in finite time. Figure 3 illustrates the states of the target set for which control inputs  $u = -0.4$ ,  $u = 0$ , and  $u = 0.4$  force the system to

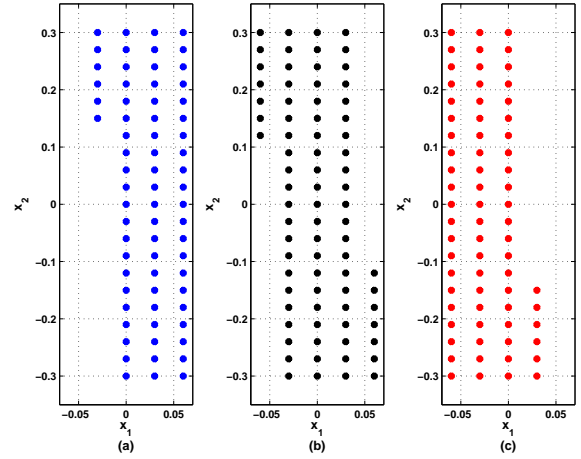


Fig. 3. Solution of the safety game for the symbolic model and target set  $[-0.06, 0.06] \times [-0.3, 0.3]$ . The states in  $W$  where  $u = -0.4$ ,  $u = 0$ , and  $u = 0.4$  force the system to stay in  $W$  are shown in figures (a), (b), and (c) respectively.

stay in  $W$ .

## VI. DISCUSSION

In this paper we showed that  $\delta$ -FC control systems admit symbolic model. The results of this paper generalize the work in [Tab08], [PGT08], [PT09], [Gir07] by not requiring stability assumptions. After constructing the symbolic models for the  $\delta$ -FC control systems, one can take the advantages of controller design for the abstraction models. However, there is a drawback in the result in Theorem 4.1 since it is only sufficient. If it is failed to find a controller forcing the desired specification on symbolic model, we cannot conclude anything regarding the existence of a controller for the original model.

## REFERENCES

- [AD90] R. Alur and D. L. Dill. *Automata, Languages and Programming*, volume 443 of *Lecture Notes in Computer Science*, chapter Automata for modeling real-time systems, pages 322–335. Springer, Berlin, April 1990.
- [Ang02] D. Angeli. A lyapunov approach to incremental stability properties. *IEEE Transactions on Automatic Control*, 47(3):410–21, 2002.
- [AS99] D. Angeli and E. D. Sontag. Forward completeness, unboundedness observability, and their lyapunov characterizations. *Systems and Control Letters*, 38:209–217, 1999.
- [BM05] T. Brihaye and C. Michaux. On the expressiveness and decidability of o-minimal hybrid systems. *Journal of Complexity*, 21(4):447–478, 2005.
- [Gir07] A. Girard. Approximately bisimilar finite abstractions of stable linear systems. In *Hybrid Systems: Computation and Control*, volume 4416 of *Lecture Notes in Computer Science*, pages 231–244. Springer, Berlin, May 2007.

- [GP07] A. Girard and G. J. Pappas. Approximation metrics for discrete and continuous systems. *IEEE Transactions on Automatic Control*, 25(5):782–798, 2007.
- [GPT09] A. Girard, G. Pola, and P. Tabuada. Approximately bisimilar symbolic models for incrementally stable switched systems. *IEEE Transactions on Automatic Control*, In press, 2009.
- [HCS06] L.C.G.J.M. Habets, P.J. Collins, and J.H. Van Schuppen. Reachability and control synthesis for piecewise-affine hybrid systems on simplices. *IEEE Transactions on Automatic Control*, 51(6):938–948, 2006.
- [HKPV98] T.A. Henzinger, P. W. Kopke, A. Puri, and P. Varaiya. What’s decidable about hybrid automata? *Journal of Computer and System Sciences*, 57:94–124, 1998.
- [LPS00] G. Lafferriere, G. J. Pappas, and S. Sastry. O-minimal hybrid systems. *Math. Control Signal Systems*, 13:1–21, 2000.
- [PGT08] G. Pola, A. Girard, and P. Tabuada. Approximately bisimilar symbolic models for nonlinear control systems. *Automatica*, 44(10):2508–2516, 2008.
- [PT09] G. Pola and P. Tabuada. Symbolic models for nonlinear control systems: alternating approximate bisimulations. *SIAM Journal on Control and Optimization*, 48(2):719–733, February 2009.
- [RCT05] E. Rodriguez-Carbonell and Ashish Tiwari. Generating polynomial invariants for hybrid systems. In *Hybrid Systems: Computation and Control*, volume 3414 of *Lecture Notes in Computer Science*, pages 590–605. Springer Berlin, February 2005.
- [Son98] E. D. Sontag. *Mathematical control theory*, volume 6. Springer-Verlag, New York, 2nd edition, 1998.
- [Tab08] P. Tabuada. An approximate simulation approach to symbolic control. *IEEE Transactions on Automatic Control*, 53(6):1406–1418, July 2008.
- [Tab09] Paulo Tabuada. *Verification and Control of Hybrid Systems*. Springer US, 2009.