Symbolic models for unstable nonlinear control systems

Majid Zamani, Giordano Pola and Paulo Tabuada

***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 subject to a schedulability constraint.**

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 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 or expansion metric characterizations [ZPJT10]. 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 alternatingly 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 control system also guarantees the existence of a controller for the symbolic model.

Our technical results are illustrated on an inverted pendulum that does not satisfy the stability assumptions required in [Tab08], [PGT08], [PT09], [Gir07]. We show how the novel abstractions in this paper can be used to synthesize a controller stabilizing the pendulum in the up-right position despite the schedulability constraints imposed by executing the controller on a microprocessor executing other tasks.

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

M. Zamani and P. Tabuada are with the Department of Electrical Engineering, University of California, Los Angeles, CA 90095, USA. Email: {zamani,tabuada}@ee.ucla.edu, URL: http://www.ee.ucla.edu/∼{zamani,tabuada}.

G. Pola is with the Department of Electrical and Information Engineering, Center of Excellence DEWS, University of L'Aquila, Poggio di Roio, 67040 L'Aquila, Italy. Email: giordano.pola@univaq.it, URL: http://www.diel.univaq.it/people/pola.

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 $\imath_A : A \hookrightarrow B$ or simply by $\imath$ the natural inclusion map taking any $a \in A$ to $\imath(a) = a \in B$. 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 $\|x\| = \max\{|x_1|, |x_2|, ..., |x_n|\}$, where $|x_i|$ denotes the absolute value of x_i. Given a measurable function $f : \mathbb{R}_0^+ \to \mathbb{R}^n$, the (essential) supremum of f is denoted by $\|f\|_\infty$; f is essentially bounded if $\|f\|_\infty < \infty$. The closed ball centered at $x \in \mathbb{R}^n$ with radius ε 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 $[A]_\mu = \{a_i \in A \mid a_i = k_i\mu, k_i \in \mathbb{Z}, i \in \mathbb{N}\}$. The set $[A]_\mu$ will be used as an approximation of the set A with precision μ. Geometrically, for any $\mu \in \mathbb{R}^+$ and $\lambda \geq \frac{\mu}{2}$ 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 $\lambda < \frac{\mu}{2}$, $\mathbb{R}^n \not\subseteq \bigcup_{q\in[\mathbb{R}^n]_\mu} \mathcal{B}_\lambda(q)$. A continuous function $\gamma : \mathbb{R}_0^+ \to \mathbb{R}_0^+$, is said to belong to class $\mathcal{K}$ if it is strictly increasing and $\gamma(0) = 0$; γ is said to belong to class $\mathcal{K}_\infty$ if $\gamma \in \mathcal{K}$ and $\gamma(r) \to \infty$ as $r \to \infty$. A continuous function $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$ 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 $\beta(r, s) \to 0$ as $s \to \infty$. We identify a relation $R \subseteq A \times B$ with the map $R : A \to 2^B$ 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:

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

where:

- $\mathbb{R}^n$ is the state space;
- $\mathsf{U} \subseteq \mathbb{R}^m$ 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 $a < 0$, $b > 0$, and satisfying the following Lipschitz assumption: there exists a positive constant K such that $\|\upsilon(t) - \upsilon(t')\| \leq K|t - t'|$ for all $\upsilon \in \mathcal{U}$ and for all $t, t' \in]a, b[$;
- $f : \mathbb{R}^n \times \mathsf{U} \to \mathbb{R}^n$ is a continuous map satisfying the following Lipschitz assumption: for every compact set $Q \subset \mathbb{R}^n$, there exists a constant $Z \in \mathbb{R}^+$ such that $\|f(x, u) - f(y, u)\| \leq Z\|x - y\|$ for all $x, y \in Q$ and all $u \in \mathsf{U}$.

A curve $\xi :]a, b[\to \mathbb{R}^n$ is said to be a *trajectory* of Σ if there exists $\upsilon \in \mathcal{U}$ satisfying:

$$\dot{\xi}(t) = f\left(\xi(t), \upsilon(t)\right), \tag{II.1}$$

for almost all $t \in]a, b[$. Although we have defined trajectories over open domains, we shall refer to trajectories $\xi : [0, \tau] \to \mathbb{R}^n$ defined on closed domains $[0, \tau]$, $\tau \in \mathbb{R}^+$ with the understanding of the existence of a trajectory $\xi' :]a, b[\to \mathbb{R}^n$ such that $\xi = \xi'|_{[0,\tau]}$. We also write $\xi_{x\upsilon}(\tau)$ to denote the point reached at time τ under the input υ from initial condition x; this point is uniquely determined, since the assumptions on f ensure existence and uniqueness of trajectories [Son98]. A control system Σ 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].

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 2.2: [Ang02] A control system Σ is incrementally input-to-state stable (δ-ISS) if it is forward complete and there exist a $\mathcal{KL}$ function β and a $\mathcal{K}_\infty$ function γ such that for any $t \in \mathbb{R}_0^+$, any $x, x' \in \mathbb{R}^n$, and any υ, $\upsilon' \in \mathcal{U}$ the following condition is satisfied:

$$\|\xi_{x\upsilon}(t) - \xi_{x'\upsilon'}(t)\| \leq \beta(\|x - x'\|, t) + \gamma(\|\upsilon - \upsilon'\|_\infty). \tag{II.2}$$

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

Definition 2.3: A control system Σ is incrementally forward complete (δ-FC) if there exist continuous functions $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$ and $\gamma : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$ 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 $\upsilon, \upsilon' \in \mathcal{U}$ the following condition is satisfied:

$$\|\xi_{x\upsilon}(t) - \xi_{x'\upsilon'}(t)\| \leq \beta(\|x - x'\|, t) + \gamma(\|\upsilon - \upsilon'\|_\infty, t). \tag{II.3}$$

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.3). From (II.2) and (II.3), we can immediately see that δ-ISS implies δ-FC. However, the converse is not true, in general, since the function β in (II.3) is not required to be a decreasing function of t and the function γ in (II.3) is allowed to depend on t while this is not the case in (II.2). Whenever the origin is an equilibrium point for Σ, the choice $x' = 0$, $\upsilon' = 0$, and $\xi_{x'\upsilon'} = 0$ results in the estimate $\|\xi_{x\upsilon}(t)\| \leq \beta(\|x\|, t) + \gamma(\|\upsilon\|_\infty, t)$ which is shown in [AS99] to be equivalent to forward completeness of Σ. Hence, the systems satisfying (II.3) are

termed incrementally forward complete. Descriptions of δ-FC control systems in terms of Lyapunov-like functions and expansion metrics can be found in [ZPJT10].

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 a 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 $H : X \to Y$.

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

- *metric*, if the output set Y is equipped with a metric $\mathbf{d} : Y \times Y \to \mathbb{R}_0^+$;
- *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 $\Sigma = (\mathbb{R}^n, \mathsf{U}, \mathcal{U}, f)$, the system associated with Σ and $\tau \in \mathbb{R}^+$ is defined by:

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

where:

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

The above system can be thought of as the time discretization of the control system Σ.

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 ε-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 : $x_a \xrightarrow[a]{u_a} x'_a$ in S_a implies the existence of $x_b \xrightarrow[b]{u_b} x'_b$ in S_b satisfying $(x'_a, x'_b) \in R$.

System S_a is ε-approximately simulated by S_b or S_b ε-approximately simulates S_a, denoted by $S_a \preceq^\varepsilon_\mathcal{S} S_b$, if there exists an ε-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 ε-approximate bisimulation relation between S_a and S_b, if the following two conditions are satisfied:

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

System S_a is ε-approximate bisimilar to S_b, denoted by $S_a \cong^\varepsilon_\mathcal{S} S_b$, if there exists an ε-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 ε-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 ε-approximately simulated by S_b or S_b alternatingly ε-approximately simulates S_a, denoted by $S_a \preceq^{\varepsilon}_{\mathcal{AS}} S_b$, if there exists an alternating ε-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 δ-FC Control Systems

We consider a δ-FC control system $\Sigma = (\mathbb{R}^n, \mathsf{U}, \mathcal{U}, f)$ with the Lipschitz constant K introduced in Definition 2.1 and a quadruple $\mathsf{q} = (\tau, \eta, \mu, \theta)$ of quantization parameters defining: time quantization $\tau \in \mathbb{R}^+$, state space quantization $\eta \in \mathbb{R}^+$, input space quantization $\mu \in \mathbb{R}^+$, and design parameter $\theta \in \mathbb{R}^+$. For Σ and q, we define the system:

$$S_{\mathsf{q}}(\Sigma) := (X_{\mathsf{q}}, U_{\mathsf{q}}, \underset{\mathsf{q}}{\longrightarrow}, Y_{\mathsf{q}}, H_{\mathsf{q}}), \tag{IV.1}$$

by:

- $X_{\mathsf{q}} = [\mathbb{R}^n]_\eta$;
- $U_{\mathsf{q}} = [\mathsf{U}]_\mu$;
- $x_{\mathsf{q}} \xrightarrow[\mathsf{q}]{u_{\mathsf{q}}} x'_{\mathsf{q}}$ if $\|\xi_{x_{\mathsf{q}}u_{\mathsf{q}}}(\tau) - x'_{\mathsf{q}}\| \leq \beta(\theta, \tau) + \gamma\left(\frac{\mu + K\tau}{2}, \tau\right) + \frac{\eta}{2}$;
- $Y_{\mathsf{q}} = \mathbb{R}^n$;
- $H_{\mathsf{q}} = \imath : X_{\mathsf{q}} \hookrightarrow Y_{\mathsf{q}}$.

The transition relation of $S_{\mathsf{q}}(\Sigma)$ is well defined in the sense that for every $x_{\mathsf{q}} \in X_{\mathsf{q}}$ and every $u_{\mathsf{q}} \in U_{\mathsf{q}}$ there always exists a $x'_{\mathsf{q}} \in X_{\mathsf{q}}$ such that $x_{\mathsf{q}} \xrightarrow[\mathsf{q}]{u_{\mathsf{q}}} x'_{\mathsf{q}}$. This can be seen by noting that by definition of X_{q}, for any $x \in \mathbb{R}^n$ there always exists a state $x'_{\mathsf{q}} \in X_{\mathsf{q}}$ such that $\|x - x'_{\mathsf{q}}\| \leq \eta/2$. Hence, for $x = \xi_{x_{\mathsf{q}}u_{\mathsf{q}}}(\tau)$ there always exists $x'_{\mathsf{q}} \in X_{\mathsf{q}}$ satisfying $\|\xi_{x_{\mathsf{q}}u_{\mathsf{q}}}(\tau) - x'_{\mathsf{q}}\| \leq \frac{\eta}{2} \leq \beta(\theta, \tau) + \gamma\left(\frac{\mu + K\tau}{2}, \tau\right) + \frac{\eta}{2}$.
We stress that while system $S_\tau(\Sigma)$ is not countable, system $S_{\mathsf{q}}(\Sigma)$ is so and it becomes finite when the state space of the control system Σ is bounded. We can now state the main result, relating δ-FC to the existence of symbolic models.

Theorem 4.1: Let Σ be a δ-FC control system. For any desired precision $\varepsilon \in \mathbb{R}^+$, and any quadruple $\mathsf{q} = (\tau, \eta, \mu, \theta)$ of quantization parameters satisfying $\eta \leq 2\varepsilon \leq 2\theta$, we have $S_{\mathsf{q}}(\Sigma) \preceq^{\varepsilon}_{\mathcal{AS}} S_\tau(\Sigma) \preceq^{\varepsilon}_{\mathcal{S}} S_{\mathsf{q}}(\Sigma)$.

The proof of Theorem 4.1 requires the following technical Lemma.

Lemma 4.2: Let $\Sigma = (\mathbb{R}^n, \mathsf{U}, \mathcal{U}, f)$ be a control system. For any $\tau, \mu \in \mathbb{R}^+$ and any input $\mathcal{U} \ni \upsilon : [0, \tau] \to \mathsf{U}$ there exists a constant input $\upsilon_{const} : [0, \tau] \to [\mathsf{U}]_\mu$ such that:

$$\|\upsilon - \upsilon_{const}\|_\infty \leq \frac{\mu + K\tau}{2}, \tag{IV.2}$$

where K is the Lipschitz constant introduced in Definition 2.1.

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

$$\begin{aligned} \|\upsilon - \upsilon_{const}\|_\infty &= \|\upsilon - \widehat{\upsilon} + \widehat{\upsilon} - \upsilon_{const}\|_\infty \\ &\leq \|\upsilon - \widehat{\upsilon}\|_\infty + \|\widehat{\upsilon} - \upsilon_{const}\|_\infty \\ &= \|\upsilon - \widehat{\upsilon}\|_\infty + \|\widehat{\upsilon} - \upsilon_{const}\| \\ &\leq \frac{K\tau}{2} + \frac{\mu}{2}. \end{aligned} \tag{IV.3}$$

■

We now prove Theorem 4.1.

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

$$\|x_\tau - x_{\mathsf{q}}\| \leq \frac{\eta}{2} \leq \varepsilon. \tag{IV.4}$$

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

Consider any $\upsilon_\tau \in U_\tau$. Choose an input $u_{\mathsf{q}} \in U_{\mathsf{q}}$ satisfying:

$$\|\upsilon_\tau - u_{\mathsf{q}}\|_\infty \leq \frac{\mu + K\tau}{2}. \tag{IV.5}$$

Note that existence of such u_{q} is a consequence of Lemma 4.2. Consider the unique transition $x_\tau \xrightarrow[\tau]{\upsilon_\tau} x'_\tau = \xi_{x_\tau \upsilon_\tau}(\tau)$ in $S_\tau(\Sigma)$. It follows from the δ-FC assumption that the distance between x'_τ and $\xi_{x_{\mathsf{q}} u_{\mathsf{q}}}(\tau)$ is bounded as:

$$\|x'_\tau - \xi_{x_{\mathsf{q}} u_{\mathsf{q}}}(\tau)\| \leq \beta(\varepsilon,\tau) + \gamma\left(\frac{\mu + K\tau}{2}, \tau\right). \quad \text{(IV.6)}$$

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

$$\|x'_\tau - x'_{\mathsf{q}}\| \leq \frac{\eta}{2}. \quad \text{(IV.7)}$$

Using the inequalities $\varepsilon \leq \theta$, (IV.6), and (IV.7), we obtain:

$$\begin{aligned}\|\xi_{x_{\mathsf{q}} u_{\mathsf{q}}}(\tau) - x'_{\mathsf{q}}\| &= \|\xi_{x_{\mathsf{q}} u_{\mathsf{q}}}(\tau) - x'_\tau + x'_\tau - x'_{\mathsf{q}}\| \\ &\leq \|\xi_{x_{\mathsf{q}} u_{\mathsf{q}}}(\tau) - x'_\tau\| + \|x'_\tau - x'_{\mathsf{q}}\| \\ &\leq \beta(\varepsilon,\tau) + \gamma\left(\frac{\mu + K\tau}{2}, \tau\right) + \frac{\eta}{2} \\ &\leq \beta(\theta,\tau) + \gamma\left(\frac{\mu + K\tau}{2}, \tau\right) + \frac{\eta}{2},\end{aligned}$$

which implies the existence of $x_{\mathsf{q}} \xrightarrow[\mathsf{q}]{u_{\mathsf{q}}} x'_{\mathsf{q}}$ in $S_{\mathsf{q}}(\Sigma)$ by definition of $S_{\mathsf{q}}(\Sigma)$. Therefore, from inequality (IV.7) and $\frac{\eta}{2} \leq \varepsilon$, we conclude $(x'_\tau, x'_{\mathsf{q}}) \in R$ and condition (iii) in Definition 3.2 holds.

Now we prove $S_{\mathsf{q}}(\Sigma) \preceq^{\varepsilon}_{\mathcal{AS}} S_\tau(\Sigma)$. Consider the relation $R \subseteq X_\tau \times X_{\mathsf{q}}$. For every $x_{\mathsf{q}} \in X_{\mathsf{q}}$, by choosing $x_\tau = x_{\mathsf{q}}$, we have $(x_\tau, x_{\mathsf{q}}) \in R$ and condition (i) in Definition 3.4 is satisfied. Now consider any $(x_\tau, x_{\mathsf{q}}) \in R$. Condition (ii) in Definition 3.4 is satisfied by the definition of R. Let us now show that condition (iii) in Definition 3.4 holds. Consider any $u_{\mathsf{q}} \in U_{\mathsf{q}}$. Choose the input $\upsilon_\tau = u_{\mathsf{q}}$ and consider the unique $x'_\tau = \xi_{x_\tau \upsilon_\tau}(\tau) \in \mathbf{Post}_{\upsilon_\tau}(x_\tau)$ in $S_\tau(\Sigma)$. From the δ-FC assumption, the distance between x'_τ and $\xi_{x_{\mathsf{q}} u_{\mathsf{q}}}(\tau)$ is bounded as:

$$\|x'_\tau - \xi_{x_{\mathsf{q}} u_{\mathsf{q}}}(\tau)\| \leq \beta(\varepsilon,\tau). \quad \text{(IV.8)}$$

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

$$\|x'_\tau - x'_{\mathsf{q}}\| \leq \frac{\eta}{2}. \quad \text{(IV.9)}$$

Using the inequalities, $\varepsilon \leq \theta$, (IV.8), and (IV.9), we obtain:

$$\begin{aligned}&\|\xi_{x_{\mathsf{q}} u_{\mathsf{q}}}(\tau) - x'_{\mathsf{q}}\| = \|\xi_{x_{\mathsf{q}} u_{\mathsf{q}}}(\tau) - x'_\tau + x'_\tau - x'_{\mathsf{q}}\| \\ &\leq \|\xi_{x_{\mathsf{q}} u_{\mathsf{q}}}(\tau) - x'_\tau\| + \|x'_\tau - x'_{\mathsf{q}}\| \leq \beta(\varepsilon,\tau) + \frac{\eta}{2} \\ &\leq \beta(\theta,\tau) + \gamma\left(\frac{\mu + K\tau}{2}, \tau\right) + \frac{\eta}{2},\end{aligned}$$

which implies the existence of $x_{\mathsf{q}} \xrightarrow[\mathsf{q}]{u_{\mathsf{q}}} x'_{\mathsf{q}}$ in $S_{\mathsf{q}}(\Sigma)$ by definition of $S_{\mathsf{q}}(\Sigma)$. Therefore, from inequality (IV.9) and $\frac{\eta}{2} \leq \varepsilon$, we can conclude that $(x'_\tau, x'_{\mathsf{q}}) \in R$ and condition (iii) in Definition 3.2 holds. ■

V. Symbolic Control Design for an Inverted Pendulum

We illustrate the results in this paper on an inverted pendulum with the following model:

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

In (V.1) x_1 is the angular position, x_2 is the angular 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 $h = 2$ is the coefficient of rotational friction. All constants and variables are expressed in the International System. The eigenvalues of the linearized system around the equilibrium point $(0, 0)$ are $\lambda_1 = 1.1433$ and $\lambda_2 = -17.1433$ showing that the original nonlinear system is unstable at $(0, 0)$. Hence, the results in [Tab08], [PGT08], [PT09], [Gir07] do not apply to this system. We assume that $u \in \mathsf{U} = [-6,\ 6]$ and that the control inputs are piecewise constant. We work on the subset $X = [-\frac{\pi}{2},\ \frac{\pi}{2}] \times [-1,\ 1]$ of the state space of Σ. In order to construct a symbolic abstraction for the preceding model, we need to find functions β and γ satisfying the incremental forward completeness property in (II.3). As shown in [ZPJT10], the functions β and γ are given by $\beta(r,t) = 2\sqrt{3}e^t r$ and $\gamma(r,t) = 2\sqrt{5}\sqrt{e^{2t}-1}r$. Our objective is to design a controller forcing the trajectories of the system to reach the target set $W = [-0.25,\ 0.25] \times [-1,\ 1]$ and to remain indefinitely inside W. We furthermore assume that the controller is implemented on a microprocessor that is executing other tasks in addition to the control task. We consider a periodic schedule with epochs of three time slots in which the first two time slots are allocated to the control tasks and the third time slot to another task. The expression of time slot refers to a time interval of the form $[k\tau, (k+1)\tau[$ with $k \in \mathbb{N}$ and where τ is the time quantization parameter. Therefore, the microprocessor schedule is given by:

$$|\mathsf{aau}|\mathsf{aau}|\mathsf{aau}|\mathsf{aau}|\mathsf{aau}|\mathsf{aau}|\mathsf{aau}|\mathsf{aau}|\mathsf{aau}|\mathsf{aau}|\cdots$$

where a denotes a slot available for the control task and u denotes a slot allotted to a different tasks. The symbol $|$ separates each epoch of three time slots. The schedulability constraint on the microprocessor can be represented by the finite system in Figure 1. When the finite system is in state q_1 and q_2 the microprocessor computes the control input for the inverted pendulum. On the other hand, when the finite system is in the state

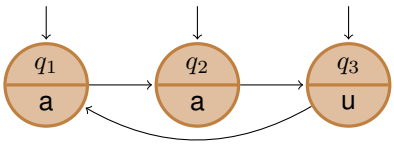

Fig. 1. Finite system describing the schedulability constraints. The lower part of the states are labeled with the outputs a and u denoting availability and unavailability of the microprocessor, respectively.

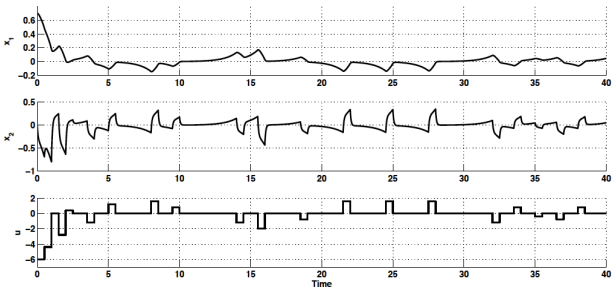

Fig. 2. Upper and central panels: evolution of ξ_1 and ξ_2 with initial condition $(0.7,\ 0)$. Lower panel: input signal.

q_3, the microprocessor computes another task. Although we can easily consider more complex schedules, the constraints described by the finite system in Figure 1 already illustrate the computational constraints imposed by implementing control laws on shared microprocessors.

For a precision $\varepsilon = 0.01$, we construct a symbolic model $S_{\mathsf{q}}(\Sigma)$ by choosing $\theta = 0.01$, $\eta = 0.02$, $\tau = 0.5$, and $\mu = 0.4$ so as to satisfy the assumptions of Theorem 4.1. The computation of the abstraction $S_{\mathsf{q}}(\Sigma)$ was performed in the tool[1] Pessoa [Pes09]. A controller enforcing the specification is found by performing simple fixed-point computations on $S_{\mathsf{q}}(\Sigma)$ using standard algorithms from game theory [Tab09]. We solve a reachability game and a safety game, both implemented in Pessoa, to reach and stay indefinitely in the target set, respectively. In Figure 2, we show the closed-loop trajectory stemming from the initial condition $(0.7,\ 0)$ and the evolution of the input signal.

VI. Discussion

In this paper we showed that δ-FC control systems admit symbolic models. The results of this paper generalize the work in [Tab08], [PGT08], [PT09], [Gir07] by not requiring stability assumptions. Although the results in this paper apply to a far greater class of control systems, the relationships between the original control system and its abstraction are weaker. The existence of a controller for the symbolic model also guarantees the existence of a controller for the original model. Otherwise, if it is failed to find a controller forcing the desired specification on the symbolic model, we cannot conclude anything regarding the existence of a controller for the original model.

[1] Pessoa can be freely downloaded from `http://www.cyphylab.ee.ucla.edu/pessoa`. All the files necessary to recreate this example are also freely available.

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*, 55(1):116–126, January 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.

[Pes09] Pessoa. It is electronically available at: http://www.cyphylab.ee.ucla.edu/pessoa. October 2009.

[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] P. Tabuada. *Verification and Control of Hybrid Systems, A symbolic approach*. Springer US, 2009.

[ZPJT10] M. Zamani, G. Pola, M. Mazo Jr., and P. Tabuada. Symbolic models for nonlinear control systems without stability assumptions. *Submitted for publication*, arXiv:1002.0822, February 2010.