Discrete Event Dyn Syst (2008) 18:163–179
DOI 10.1007/s10626-007-0029-9

Approximate Simulation Relations for Hybrid Systems

Antoine Girard · A. Agung Julius · George J. Pappas

Received: 27 September 2006 / Accepted: 18 September 2007 /
Published online: 11 October 2007

Abstract Approximate simulation relations have recently been introduced as a powerful tool for the approximation of discrete and continuous systems. In this paper, we extend this abstraction framework to hybrid systems. Using the notion of simulation functions, we develop a characterization of approximate simulation relations which can be used for hybrid systems approximation. For several classes of hybrid systems, this characterization leads to effective algorithms for the computation of approximate simulation relations. An application in the context of reachability analysis is shown.

Keywords Hybrid systems · Abstractions · Approximation · Approximate simulation relation

1 Introduction

Approximation of purely discrete systems has traditionally been based on language inclusion and equivalence with notions such as simulation or bisimulation

This research is partially supported by the NSF Presidential Early CAREER (PECASE) Grant 0132716.

A. Girard (✉)
Laboratoire Jean Kuntzmann, Université Joseph Fourier, B.P. 53,
38041 Grenoble Cedex 9, France
e-mail: Antoine.Girard@imag.fr

A. A. Julius · G. J. Pappas
Department of Electrical and Systems Engineering, University of Pennsylvania,
Philadelphia, PA 19104, USA

A. A. Julius
e-mail: agung@seas.upenn.edu

G. J. Pappas
e-mail: pappasg@seas.upenn.edu

relations (Clarke et al. 2000; Milner 1989). These concepts have been very useful for simplifying complex problems such as safety verification or controller synthesis. More recently, they have been extended to the framework of continuous and hybrid systems (Haghverdi et al. 2005; Pappas 2003; Pola et al. 2004; van der Schaft 2004) allowing to consider the approximation of systems in a unified (discrete/continuous) manner. Applications of simulation and bisimulation relations to verification or control problems can be found for instance in Alur et al. (1995, 2000), Belta et al. (2005) and Tabuada (2007)

When dealing with continuous and hybrid systems, typically observed over the real numbers with possibly noisy observations, the usual notions based on *exact* language inclusion are quite restrictive and not robust. The notion of distance between languages is much more adequate in this context. In Girard and Pappas (2007a), we proposed a framework for system approximation based on approximate versions of simulation relations. Instead of requiring that the observations of a system and its approximation are equal, we require that the distance between them remains bounded by some parameter called precision of the approximate simulation. This approach not only defines more robust relations between systems but also allows more significant complexity reductions in the approximation process. This framework has been applied to nonlinear autonomous systems (Girard and Pappas 2005) and constrained linear systems (Girard and Pappas 2007b). Computational methods have been developed to quantify the distance between the observed trajectories of two systems. In Julius (2006); Julius et al. (2006), the theoretical and computational frameworks have been extended to handle stochastic dynamical and hybrid systems with purely stochastic (i.e. Markovian) jumps. Related work on approximate versions of simulation and bisimulation relations has been done for quantitative transition systems (de Alfaro et al. 2004) or labeled Markov processes (Desharnais et al. 2004).

In this paper, we apply our approximation framework to hybrid systems. Using the notion of simulation functions (Girard and Pappas 2007a), we develop a characterization of approximate simulation relations which can be used for hybrid systems approximation. For several classes of hybrid systems, this characterization leads to effective algorithms for the computation of approximate simulation relations. An application in the context of reachability analysis is shown.

2 Approximate simulation relations for transition systems

The notion of approximate simulation relation has been developed in the framework of labelled transition systems in Girard and Pappas (2007a). In this section, the main results are reviewed.

2.1 Labelled transition systems

Labelled transition systems allow us to model, in a unified setting, discrete, continuous and hybrid systems. Labelled transition systems can be seen as automata, possibly with an infinite number of states or transitions.

Definition 1 A labelled transition system with observations is a tuple $T=(Q, \Sigma, \rightarrow, Q^0, \Pi, \langle\langle . \rangle\rangle)$ that consists of:

- A set Q of states,
- A set Σ of labels,
- A transition relation $\rightarrow \subseteq Q \times \Sigma \times Q$,
- A set $Q^0 \subseteq Q$ of initial states,
- A set Π of observations, and
- An observation map $\langle\langle . \rangle\rangle : Q \rightarrow \Pi$.

A state trajectory of T is a sequence of transitions,

$$q^0 \xrightarrow{\sigma^0} q^1 \xrightarrow{\sigma^1} q^2 \xrightarrow{\sigma^2} \dots, \text{ where } \mathrm{q}^0 \in \mathrm{Q}^0.$$

For a given initial state and sequence of labels, there may exist several state trajectories of T. Thus, the systems we consider are possibly nondeterministic (but not stochastic). The associated external trajectory

$$\pi^0 \xrightarrow{\sigma^0} \pi^1 \xrightarrow{\sigma^1} \pi^2 \xrightarrow{\sigma^2} \dots, \text{ where } \pi^{\mathrm{i}} = \langle\langle \mathrm{q}^{\mathrm{i}} \rangle\rangle$$

describes the evolution of the observations under the dynamics of the labelled transition system. The set of external trajectories of the labelled transition system T is called the language of T and is denoted $L(T)$. The subset of Π reachable by the external trajectories of T is noted $\mathrm{Reach}(T)$:

$$\mathrm{Reach}(T) = \left\{ \pi \in \Pi \;\middle|\; \exists \pi^0 \xrightarrow{\sigma^0} \pi^1 \xrightarrow{\sigma^1} \pi^2 \xrightarrow{\sigma^2} \dots \in L(T),\ \exists j \in \mathbb{N},\ \pi^j = \pi \right\}.$$

An important problem for transition systems is the safety verification problem which consists in checking whether the reachable set $\mathrm{Reach}(T)$ intersects a set of observations Π_U associated with unsafe states.

2.2 Approximate simulation relations

Exact simulation relations between two labelled transition systems require that their observations are (and remain) identical (Clarke et al. 2000; Milner 1989). Approximate simulation relations are less rigid since they only require that the distance between the observations of both systems is (and remains) bounded by some parameter called precision. Let $T_1 = (Q_1, \Sigma_1, \rightarrow_1, Q_1^0, \Pi_1, \langle\langle . \rangle\rangle_1)$ and $T_2 = (Q_2, \Sigma_2, \rightarrow_2, Q_2^0, \Pi_2, \langle\langle . \rangle\rangle_2)$ be two labelled transition systems with the same set of labels ($\Sigma_1 = \Sigma_2 = \Sigma$) and the same set of observations ($\Pi_1 = \Pi_2 = \Pi$). Let us assume that the set of observations Π is a metric space; d_Π denotes the metric on Π.

Definition 2 A relation $\mathcal{S}_\delta \subseteq Q_1 \times Q_2$ is a δ-approximate simulation relation of T_1 by T_2 if for all $(q_1, q_2) \in \mathcal{S}_\delta$:

1. $d_\Pi\left(\langle\langle q_1 \rangle\rangle_1, \langle\langle q_2 \rangle\rangle_2\right) \leq \delta$,
2. For all $q_1 \xrightarrow{\sigma}_1 q_1'$, there exists $q_2 \xrightarrow{\sigma}_2 q_2'$ such that $(q_1', q_2') \in \mathcal{S}_\delta$.

The parameter δ is called the precision of the approximate simulation relation. Note that for precision $\delta = 0$, we recover the usual notion of *exact* simulation relation.

Definition 3 T_2 approximately simulates T_1 with the precision δ (noted $T_1 \preceq_\delta T_2$), if there exists $\mathcal{S}_\delta$, a δ-approximate simulation relation of T_1 by T_2 such that for all $q_1 \in Q_1^0$, there exists $q_2 \in Q_2^0$ such that $(q_1, q_2) \in \mathcal{S}_\delta$.

If T_2 approximately simulates T_1 with the precision δ then the language of T_1 is approximated with precision δ by the language of T_2.

Theorem 1 *If $T_1 \preceq_\delta T_2$, then for all external trajectories of T_1,*

$$\pi_1^0 \xrightarrow{\sigma^0} \pi_1^1 \xrightarrow{\sigma^1} \pi_1^2 \xrightarrow{\sigma^2} \dots,$$

there exists an external trajectory of T_2 with the same sequence of labels

$$\pi_2^0 \xrightarrow{\sigma^0} \pi_2^1 \xrightarrow{\sigma^1} \pi_2^2 \xrightarrow{\sigma^2} \dots$$

such that for all $i \in \mathbb{N}$, $d_\Pi(\pi_1^i, \pi_2^i) \leq \delta$.

Proof There exists a state trajectory of T_1, $q_1^0 \xrightarrow{\sigma^0} q_1^1 \xrightarrow{\sigma^1} q_1^2 \xrightarrow{\sigma^2} \dots$, such that for all $i \in \mathbb{N}$, $\langle\langle q_1^i \rangle\rangle_1 = \pi_1^i$. $q_1^0 \in Q_1^0$, then there exists $q_2^0 \in Q_2^0$ such that (q_1^0, q_2^0) is in the δ-approximate simulation relation $\mathcal{S}_\delta$. Using the second property of Definition 2, it can be shown by induction that there exists a state trajectory of T_2,

$$q_2^0 \xrightarrow{\sigma^0} q_2^1 \xrightarrow{\sigma^1} q_2^2 \xrightarrow{\sigma^2} \dots \text{ such that } \forall i \in \mathbb{N},\ (q_1^i, q_2^i) \in \mathcal{S}_\delta.$$

Let $\pi_2^0 \xrightarrow{\sigma^0} \pi_2^1 \xrightarrow{\sigma^1} \pi_2^2 \xrightarrow{\sigma^2} \dots$ be the associated external trajectory of T_2 (for all $i \in \mathbb{N}$, $\langle\langle q_2^i \rangle\rangle_2 = \pi_2^i$). Then, we have for all $i \in \mathbb{N}$,

$$d_\Pi(\pi_1^i, \pi_2^i) = d_\Pi(\langle\langle q_1^i \rangle\rangle_1, \langle\langle q_2^i \rangle\rangle_2) \leq \delta. \qquad \square$$

Approximation of labelled transition systems based on approximate simulation relations is useful for solving problems involving reachability analysis such as the safety verification problem. Indeed, from Theorem 1, it is straightforward that if T_2 approximately simulates T_1 with the precision δ then $\mathrm{Reach}(T_1) \subseteq \mathcal{N}_\Pi(\mathrm{Reach}(T_2), \delta)$ where $\mathcal{N}_\Pi(., \delta)$ denotes the δ-neighborhood for the metric d_Π. Thus, given an unsafe set Π_U, if $\mathrm{Reach}(T_2) \cap \mathcal{N}_\Pi(\Pi_U, \delta) = \emptyset$, it follows that $\mathrm{Reach}(T_1) \cap \Pi_U = \emptyset$. Therefore, the safety of T_1 can be verified using the approximate system T_2.

3 Hybrid systems as transition systems

In this section, we introduce the rather general class of hybrid systems that we consider and show that these can be seen as transition systems.

Definition 4 A hybrid system is a tuple $H = (L, n, p, E, F, Inv, G, R, Q^0)$ where

- L is a finite set of locations or discrete states. $|L|$ denotes the number of elements of L. Without loss of generality, we assume that $L = \{1, \ldots, |L|\}$.
- $n : L \to \mathbb{N}$, where for every $l \in L$, $n_l = n(l)$ is the dimension of the continuous state space in the location l. The set of states of the hybrid system is

$$Q = \bigcup_{l \in L} \{l\} \times \mathbb{R}^{n_l}.$$

- $p : L \to \mathbb{N}$, where for every $l \in L$, $p_l = p(l)$ is the dimension of the continuous observation of the hybrid system in the location l. The set of observations of the hybrid system is

$$\Pi = \bigcup_{l \in L} \{l\} \times \mathbb{R}^{p_l}.$$

- $E \subseteq L \times L$ is the set of events or discrete transitions.
- $F = \{F_l |\ l \in L\}$ defines the continuous dynamics for each location. For each $l \in L$, F_l is a triple (f_l, g_l, U_l) where $f_l : \mathbb{R}^{n_l} \times U_l \to \mathbb{R}^{n_l}$, $g_l : \mathbb{R}^{n_l} \to \mathbb{R}^{p_l}$ and $U_l \subseteq \mathbb{R}^{m_l}$ is a compact set of internal inputs which can be seen as disturbances and modelling uncertainties rather than control inputs. While the discrete part of the state is l, the continuous variables (i.e. the continuous part x of the state and the continuous part y of the observation) evolve according to

$$\begin{cases} \dot{x}(t) = f_l(x(t), u(t)), \ u(t) \in U_l \\ y(t) = g_l(x(t)). \end{cases}$$

- $Inv = \{Inv_l |\ l \in L\}$ defines an invariant set for each location. For each $l \in L$, $Inv_l \subseteq \mathbb{R}^{n_l}$ constrains the value of the continuous part of the state while the discrete part is l.
- $G = \{G_e |\ e \in E\}$ defines the guard for each discrete transition. For each $e = (l, l') \in E$, $G_e \subseteq Inv_l$. The discrete transition e is enabled when the continuous part of the state is in G_e.
- $R = \{R_e |\ e \in E\}$ defines the reset map for each discrete transition. For each $e = (l, l') \in E$, $R_e : G_e \to 2^{Inv_{l'}}$. When the event e occurs, the continuous part of the state is reset using the map R_e.
- $Q^0 \subseteq Q$ is the set of initial states:

$$Q^0 = \bigcup_{l \in L} \{l\} \times I_l^0, \text{ with } I_l^0 \subseteq Inv_l.$$

The semantics of a hybrid system is well established (see for instance Alur et al. 2000) and will become clear with the definition of the labelled transition system associated to H. In the spirit of Alur et al. (1995), we can derive from H the nondeterministic transition system $T = (Q, \Sigma, \to, Q^0, \Pi, \langle\langle . \rangle\rangle)$ where the set of states Q, the set of observations Π, and the set initial states Q^0 are the same as in the hybrid system H. The set of labels is $\Sigma = \mathbb{R}^+ \cup \{\tau\}$ where the labels in $\mathbb{R}^+$ represent the durations labelling the continuous transitions while the symbol τ is used to label discrete transitions occurring instantaneously. The observation map is defined naturally by

$$\langle\langle (l, x) \rangle\rangle = (l, g_l(x)).$$

The transition relation $\rightarrow$ is given by:

1. *Continuous transitions*: For $t \in \mathbb{R}^+$, $(l, x) \xrightarrow{t} (l, x')$ iff there exists a measurable function $u(.)$ and an absolutely continuous function $z(.)$ such that $z(0) = x$, $z(t) = x'$ and for all $s \in [0, t]$,

$$\dot{z}(s) = f_l(z(s), u(s)), \text{ with } u(s) \in U_l \text{ and } z(s) \in Inv_l\ .$$

2. *Discrete transitions*: $(l, x) \xrightarrow{\tau} (l', x')$ iff $(l, l') = e \in E$, $x \in G_e$ and $x' \in R_e(x)$.

The set of observations Π of the hybrid system H is equipped with the following metric d_Π:

$$d_\Pi\left((l_1, y_1), (l_2, y_2)\right) = \begin{cases} \|y_1 - y_2\|, & \text{if } l_1 = l_2 \\ +\infty, & \text{if } l_1 \neq l_2 \end{cases}$$

where $\|.\|$ is the usual Euclidean norm.

In the following, we give a characterization of approximate simulation relations, suitable for hybrid systems; thus showing that the approximation framework presented in Section 2 can be applied in an effective way to hybrid systems.

4 Approximate simulation relations for hybrid systems

Let $H_i = (L_i, n_i, p_i, E_i, F_i, Inv_i, G_i, R_i, Q_i^0)$, $(i = 1, 2)$ be two hybrid systems and $T_i = (Q_i, \Sigma_i, \rightarrow_i, Q_i^0, \Pi_i, \langle\langle . \rangle\rangle_i)$, $(i = 1, 2)$ be the associated labelled transition systems. We assume that T_1 and T_2 have the same set of observations $\Pi_1 = \Pi_2 = \Pi$. Particularly, this implies that the set of locations and the dimensions of the continuous observations are the same for both systems (i.e. $L_1 = L_2 = L$, $p_1 = p_2 = p$).

We will further assume that the discrete dynamics of both systems are the same (i.e. $E_1 = E_2 = E$). The approximation of the discrete dynamics of a hybrid system has been considered for systems with purely stochastic jumps (Julius 2006). In this paper, we choose to concentrate on the approximation of the continuous dynamics and reserve the approximation of the discrete dynamics for future research. In this section, we provide a characterization of approximate simulation relations thus establishing sufficient conditions so that H_2 approximately simulates H_1.

4.1 Simulation functions

Let $l \in L$, let $n_{1,l}$, $n_{2,l}$ be the dimensions of the continuous part of the state of H_1 and H_2 in the location l. Let $F_{1,l} = (f_{1,l}, g_{1,l}, U_{1,l})$ and $F_{2,l} = (f_{2,l}, g_{2,l}, U_{2,l})$ be the continuous dynamics of H_1 and H_2 associated to the location l. We define the following notations:

$$x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \quad f_l(x, u_1, u_2) = \begin{bmatrix} f_{1,l}(x_1, u_1) \\ f_{2,l}(x_2, u_2) \end{bmatrix},$$

$$g_l(x) = g_{1,l}(x_1) - g_{2,l}(x_2).$$

In Girard and Pappas (2007a), we showed that approximate simulation relations could be characterized efficiently using the notion of simulation functions. Intuitively, a simulation function is a function bounding the distance between the observations and non-increasing under the simultaneous execution of the two continuous dynamics.

Definition 5 A differentiable function $V_l : \mathbb{R}^{n_{1,l}} \times \mathbb{R}^{n_{2,l}} \to \mathbb{R}^+$ is a simulation function of $F_{1,l}$ by $F_{2,l}$ if for all $x \in \mathbb{R}^{n_{1,l}} \times \mathbb{R}^{n_{2,l}}$, the following equations hold

$$V_l(x) \geq \|g_l(x)\|, \tag{1}$$

$$\sup_{u_1 \in U_{1,l}} \inf_{u_2 \in U_{2,l}} \nabla V_l(x)^T f_l(x, u_1, u_2) \leq 0. \tag{2}$$

Remark 1 There are similarities between the notions of simulation function and of robust control Lyapunov function (Freeman and Kokotovic 1996; Liberzon et al. 2002) for output stabilization of the composite system given by vector field f_l and observation map g_l. Let us consider the input $u_1(.)$ as a disturbance and the input $u_2(.)$ as a control variable in Eq. 2. Then, the interpretation of this inequality is that for all disturbances there exists a control input such that the simulation function decreases. This means that the choice of $u_2(.)$ can be made with the knowledge of $u_1(.)$. In comparison, a robust control Lyapunov function requires that there exists a control $u_2(.)$ such that for all disturbances $u_1(.)$, the function decreases. Thus, it appears that robust control Lyapunov functions require stronger conditions than simulation functions.

Simulation functions satisfy the following property which will be useful in characterizing approximate simulation relations for hybrid systems. A detailed proof of this result can be found in Girard and Pappas (2007b).

Proposition 1 *Let V_l be a simulation function of $F_{1,l}$ by $F_{2,l}$. Then, for all $(x_1, x_2) \in \mathbb{R}^{n_{1,l}} \times \mathbb{R}^{n_{2,l}}$, for all $t \in \mathbb{R}^+$, for all measurable inputs $u_1(.)$, there exists a measurable input $u_2(.)$ such that*

$$\forall s \in [0, t],\ \ V_l(z_1(s), z_2(s)) \leq V_l(x_1, x_2) \tag{3}$$

where

$$\dot{z}_i(s) = f_{i,l}(z_i(s), u_i(s)),\ \ u_i(s) \in U_{i,l},\ \ z_i(0) = x_i,\ \ i = 1, 2.$$

4.2 Approximate simulation relations

In this section, we give a characterization of approximate simulation relations for hybrid systems using the notion of simulation function. Let us assume that for each location $l \in L$, there exists a simulation function V_l of the continuous dynamics $F_{1,l}$ by $F_{2,l}$. We define the following sets which can be thought as some kind of neighborhoods associated with the simulation functions. For all $x_1 \in \mathbb{R}^{n_{1,l}}$, $\beta \geq 0$,

$$\mathcal{N}_l(x_1, \beta) = \{x_2 \in \mathbb{R}^{n_{2,l}} |\ V_l(x_1, x_2) \leq \beta\}.$$

We can now state the main result of the paper.

Theorem 2 *For all $l \in L$, let V_l be a simulation function of $F_{1,l}$ by $F_{2,l}$. Let $\beta_1, \dots, \beta_{|L|}$ be positive numbers such that the following conditions hold:*

(a) *For all $l \in L$, $\mathcal{N}_l(Inv_{1,l}, \beta_l) \subseteq Inv_{2,l}$,*
(b) *For all $e = (l, l') \in E$, $\mathcal{N}_l(G_{1,e}, \beta_l) \subseteq G_{2,e}$,*
(c) *For all $e = (l, l') \in E$,*

$$\beta_{l'} \geq \max_{\substack{x_1 \in G_{1,e} \\ V_l(x_1, x_2) \leq \beta_l}} \left(\max_{x_1' \in R_{1,e}(x_1)} \min_{x_2' \in R_{2,e}(x_2)} V_{l'}(x_1', x_2') \right).$$

(d) *For all $l \in L$,*

$$\beta_l \geq \max_{x_1 \in I_{1,l}^0} \min_{x_2 \in I_{2,l}^0} V_l(x_1, x_2),$$

Let $\delta = \max(\beta_1, \dots, \beta_{|L|})$. Then, the relation $\mathcal{S}_\delta \subseteq Q_1 \times Q_2$ defined by

$$\mathcal{S}_\delta = \{(l_1, x_1, l_2, x_2) |\ l_1 = l_2 = l,\ V_l(x_1, x_2) \leq \beta_l\}$$

is a δ-approximate simulation relation of T_1 by T_2 and $T_1 \preceq_\delta T_2$.

Proof Let $(l_1, x_1, l_2, x_2) \in \mathcal{S}_\delta$, then $l_1 = l_2 = l$ and $V_l(x_1, x_2) \leq \beta_l$. From Eq. 1, we have that $\|g_{l,1}(x_1) - g_{l,2}(x_2)\| \leq \beta_l \leq \delta$. Hence, the first property of Definition 2 holds.

Let $(l_1, x_1) \xrightarrow{t} (l_1, x_1')$, then there exists an input $u_1(.)$ and a function $z_1(.)$ such that $z_1(0) = x_1$, $z_1(t) = x'$ and for all $s \in [0, t]$, $u_1(s) \in U_{1,l}$, $z_1(s) \in Inv_{1,l}$ and

$$\dot{z}_1(s) = f_{l,1}(z_1(s), u_1(s)).$$

From Proposition 1, we know that there exists an input $u_2(.)$ and a function $z_2(.)$ such that $z_2(0) = x_2$, and for all $s \in [0, t]$, $u_2(s) \in U_{2,l}$,

$$\dot{z}_2(s) = f_{l,2}(z_2(s), u_2(s))$$

and $V(z_1(s), z_2(s)) \leq V(x_1, x_2) \leq \beta_l$. Then, assumption (a) of Theorem 2 ensures that for all $s \in [0, t]$, $z_2(s) \in Inv_{l,2}$. Let $x_2' = z_2(t)$, we have $(l_2, x_2) \xrightarrow{t} (l_2, x_2')$ and since $V_l(x_1', x_2') \leq \beta_l$, $(l_1, x_1', l_2, x_2') \in \mathcal{S}_\delta$.

Let $(l_1, x_1) \xrightarrow{\tau} (l_1', x_1')$, then there exists $e = (l_1, l_1')$ such that $x_1 \in G_{1,e}$ and $x_1' \in R_{1,e}(x_1)$. Assumption (b) of Theorem 2 ensures that $x_2 \in G_{2,e}$. From assumption (c) of 2, we have that there exists $x_2' \in R_{2,e}(x_2)$, such that $V_{l'}(x_1', x_2') \leq \beta_{l'}$ where $l' = l_1'$. Then, $(l_2, x_2) \xrightarrow{\tau} (l_2', x_2')$ with $l_2' = l'$ and $(l_1', x_1', l_2', x_2') \in \mathcal{S}_\delta$. Therefore, $\mathcal{S}_\delta$ is a δ-approximate simulation relation of T_1 by T_2.

Finally, let $(l_1, x_1) \in Q_1^0$, then $x_1 \in I_{1,l}^0$ where $l = l_1$. From assumption (d) of Theorem 2, there exists $x_2 \in I_{2,l}^0$, such that $V_l(x_1, x_2) \leq \beta_l$. Then, $(l_2, x_2) \in Q_2^0$ with $l_2 = l$ and $(l_1, x_1, l_2, x_2) \in \mathcal{S}_\delta$. Then $T_1 \preceq_\delta T_2$. □

It is clear that the scalars $\beta_1, \dots, \beta_{|L|}$ cannot be chosen independently as they are linked by assumption (c) which can be interpreted as a condition of limitation of the expansion of the approximation error propagating through reset maps. Thus, it is not necessarily the case that numbers such that assumptions of the Theorem hold, exist. However, for several classes of hybrid systems we can guarantee their existence and derive procedures to compute them.

4.2.1 Acyclic hybrid systems

Let us consider hybrid systems H_1 and H_2 such that their common graph (L, E) does not contain any cycle. Without loss of generality, we can assume that the discrete states are numbered in a way such that:

$$(l, l') \in E \implies l < l'.$$

Then, the scalars $\beta_1, \ldots, \beta_{|L|}$ can be computed in an inductive way. Start by computing β_1 by solving:

$$\beta_1 = \max_{x_1 \in I^0_{1,1}} \min_{x_2 \in I^0_{2,1}} V_1(x_1, x_2).$$

Then, for $l' \in \{2, \ldots, |L|\}$, we can compute $\beta_{l'}$ from $\beta_1, \ldots, \beta_{l'-1}$ by choosing $\beta_{l'} = \max(\gamma_{1,l'}, \ldots, \gamma_{l',l'})$ where

$$\gamma_{l',l'} = \max_{x_1 \in I^0_{1,l'}} \min_{x_2 \in I^0_{2,l'}} V_{l'}(x_1, x_2)$$

and for $l < l'$, $\gamma_{l,l'} = 0$ if $e = (l, l') \notin E$ or if $e = (l, l') \in E$,

$$\gamma_{l,l'} = \max_{\substack{x_1 \in G_{1,e} \\ V_l(x_1, x_2) \le \beta_l}} \left(\max_{x'_1 \in R_{1,e}(x_1)} \min_{x'_2 \in R_{2,e}(x_2)} V_{l'}(x'_1, x'_2) \right).$$

Then, it is clear that with these $\beta_1, \ldots, \beta_{|L|}$, assumptions (c) and (d) of Theorem 2 hold.

4.2.2 Hybrid systems with memoryless resets

We now consider hybrid systems with memoryless resets (i.e. $R_{i,e}(x_i) = R_{i,e}$ for all $e \in E, i = 1, 2$), then assumption (c) becomes for all $e = (l, l') \in E$

$$\beta_{l'} \ge \max_{x'_1 \in R_{1,e}} \min_{x'_2 \in R_{2,e}} V_{l'}(x'_1, x'_2).$$

Then, the numbers $\beta_1, \ldots, \beta_{|L|}$ are not linked anymore and can be computed independently.

4.2.3 Hybrid systems with contracting resets

Let us assume that the hybrid systems have reset maps that are contracting with respect to the simulation functions: for all $e = (l, l') \in E$, for all $x_1 \in G_{1,e}$ and $x_2 \in G_{2,e}$,

$$\max_{x'_1 \in R_{1,e}(x_1)} \min_{x'_2 \in R_{2,e}(x_2)} V_{l'}(x'_1, x'_2) \le V_l(x_1, x_2).$$

Then, it follows that for all $e = (l, l') \in E$

$$\max_{\substack{x_1 \in G_{1,e} \\ V_l(x_1, x_2) \le \beta_l}} \left(\max_{x'_1 \in R_{1,e}(x_1)} \min_{x'_2 \in R_{2,e}(x_2)} V_{l'}(x'_1, x'_2) \right) \le \max_{\substack{x_1 \in G_{1,e} \\ V_l(x_1, x_2) \le \beta_l}} V_l(x_1, x_2) \le \beta_l.$$

Then, a sufficient condition for assumption (c) to hold is that for all $e = (l, l') \in E$, $\beta_{l'} \ge \beta_l$. Setting $\beta_1 = \cdots = \beta_{|L|} = \beta$, it follows that the assumption (c) holds. The common value β must be chosen such that assumption (d) holds. The computation of β can thus be done in an effective way:

$$\beta = \max_{l \in L} \left(\max_{x_1 \in I_{1,l}^0} \min_{x_2 \in I_{2,l}^0} V_l(x_1, x_2) \right).$$

An interesting subclass of hybrid systems with contracting resets are those with identity resets (i.e. $R_{i,e}(x_i) = x_i$ for all $e \in E$, $i = 1, 2$) and where we can compute a common simulation function: $V_1 = \cdots = V_{|L|} = V$.

4.3 Approximation of hybrid systems

It is well known that the computational cost of some analysis tasks such as reachability analysis of hybrid systems increases drastically with the complexity of the continuous dynamics. When analyzing a hybrid system with complex (high order and/or nonlinear) continuous dynamics, it is interesting to use an approximation of the system. Based on Theorem 2, we can sketch a procedure to approximate a hybrid system H_1 by another hybrid system H_2 with simpler continuous dynamics and to compute the precision of the approximate simulation relation of T_1 by T_2.

Firstly, for each location $l \in L$, we approximate the continuous dynamics $F_{1,l}$ by a *simpler* continuous dynamics $F_{2,l}$. The goal of this approximation is to reduce the complexity of analysis tasks (e.g. reachability computations). This approximation can be done using projections (for high order dynamics Girard and Pappas 2007b) and linearizations (for nonlinear dynamics Girard and Pappas 2005). A human user can also guide this process using his knowledge on the system. The initial sets $I_{2,l}^0$ and the reset maps $R_{2,e}$ are then chosen according to the transformation applied to the continuous dynamics (linearization, projection).

Then, we need to compute the associated simulation functions. Computational methods have been developed for the class of autonomous nonlinear systems (Girard and Pappas 2005) and constrained linear systems (Girard and Pappas 2007b). In Girard and Pappas (2005), for continuous dynamics of the form

$$\begin{cases} \dot{x}(t) = f_{i,l}(x(t)) \\ y(t) = g_{i,l}(x(t)) \end{cases} \quad i = 1, 2 \tag{4}$$

where $f_{l,i}$, $g_{l,i}$ are polynomials, it is shown that the simulation function V_l can be sought as the square root of a positive polynomial. Then, from relaxations of the inequalities 1 and 2, the simulation function V_l can be computed by solving a sum of squares program which can be done using the Matlab toolbox SOSTOOLS (Prajna et al. 2005).

In Girard and Pappas (2007b), for constrained linear dynamics of the form

$$\begin{cases} \dot{x}(t) = A_{i,l}x(t) + B_{i,l}u_i(t), \; u_i(t) \in U_{i,l} \\ y(t) = C_{i,l}x(t) \end{cases} \quad i = 1, 2 \tag{5}$$

where $U_{i,l}$ are convex polytopes, it is shown that the simulation function V_l can be sought under the form $V_l(x) = \max(\sqrt{x^T M_l x}, \alpha_l)$ where M_l is a positive semidefinite symmetric matrix and α_l is a positive number. Then, the computation of V_l involves solving a set of linear matrix inequalities and a quadratic program. The computation of simulation functions for constrained linear dynamics has been implemented in the

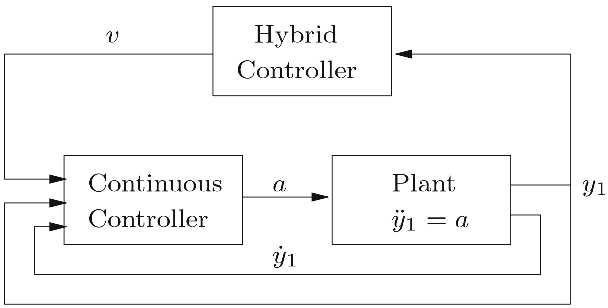

Fig. 1 Control architecture of the planar robot. The continuous controller is given by Eq. 7 and the hybrid controller is shown in Fig. 2

Matlab toolbox MATISSE.[1] More details on the approximation of the continuous dynamics can be found in Girard and Pappas (2005, 2007b).

Secondly, we compute positive numbers $\beta_1, \ldots, \beta_{|L|}$ satisfying the assumptions (c) and (d) of Theorem 2. In the previous section, for several classes of hybrid systems we provided effective procedures for the computation of such numbers. Then, we choose the invariants and the guards such that assumptions (a) and (b) of Theorem 2 hold (e.g. $Inv_{2,l} = \mathcal{N}_l(Inv_{1,l}, \beta_l)$ and $G_{2,e} = \mathcal{N}_l(G_{1,e}, \beta_l)$ where $e = (l, l')$). Then, from Theorem 2, it follows that $T_1 \preceq_\delta T_2$ with $\delta = \max(\beta_1, \ldots, \beta_{|L|})$.

5 Example

In this section, we illustrate our approximation framework in the context of reachability analysis of a simple planar robot motion. Let us consider a second order model of a robot:

$$\ddot{y}_1(t) = a(t) \tag{6}$$

where $y_1(t) \in \mathbb{R}^2$ denotes the position of the robot in a planar environment. Following Fainekos et al. (2007), the robot is equipped with a dynamic continuous controller given by

$$\begin{cases} \dot{w}(t) = v(t) \\ a(t) \ = \frac{v(t)}{2} - \frac{101}{400}(y_1(t) - w(t)) - \dot{y}_1(t) \end{cases} \tag{7}$$

Then, the robot behaves approximately like the first order system

$$\dot{y}_2(t) = v(t). \tag{8}$$

The value of the input $v(t) \in \{v_1, \ldots, v_6\}$ (with $\|v_1\| = \cdots = \|v_6\| = 0.2$) is computed by a hybrid controller on top of the continuous controller given by Eq. 7. The control architecture of the robot and the hybrid controller are shown on Figs. 1 and 2.

[1]MATISSE: Metrics for Approximate TransItion Systems Simulation and Equivalence, Available from http://www.seas.upenn.edu/~agirard/Software/MATISSE.

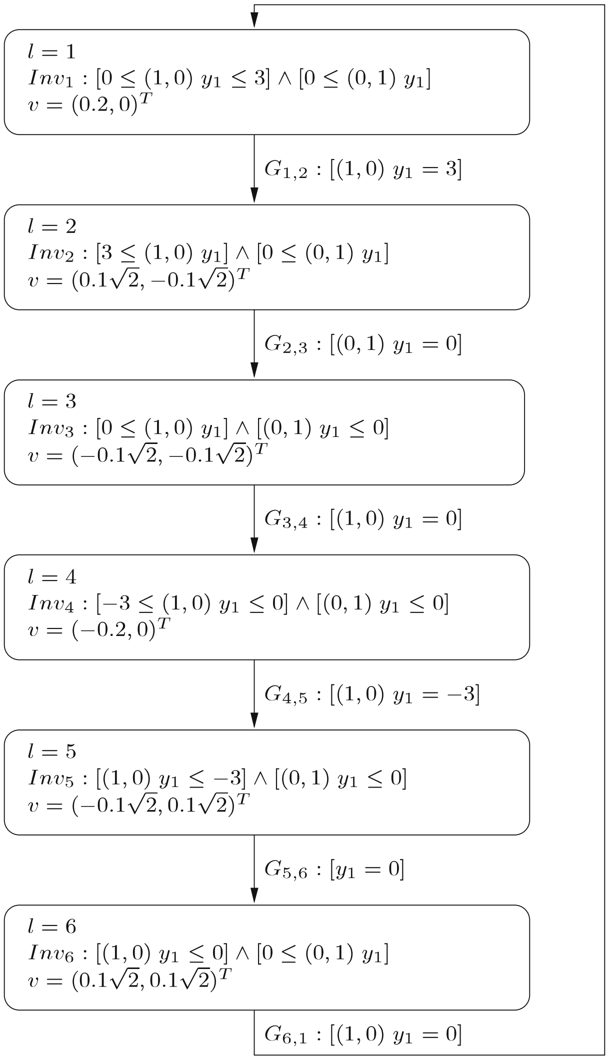

Fig. 2 Hybrid controller for the system shown in Fig. 1

We assume that the initial state of the robot is $y_1(0) \in \{0\} \times [4, 6]$ and $\dot{y}_1(0) = 0$, the initial state of the dynamic continuous controller is $w(0) = y_1(0)$ and that initially the hybrid controller is in mode 1. We want to perform a reachability analysis of the robot motion that is to compute the reachable set of the hybrid system modelling the motion of the robot. Let us remark that in each mode, the continuous dynamics is a 6-dimensional linear dynamics for which the reachability analysis is quite demanding in terms of computations.

Thus, we would like to perform the reachability analysis using the approximate continuous dynamics 8. Following Fainekos et al. (2007), we can check that the function

$$V(y_1, \dot{y}_1, w, y_2) = \max\left(\sqrt{\|y_1 - w\|^2 + 100\|y_1 - w + 2\dot{y}_1\|^2}, 0.4\right) + \|w - y_2\|$$

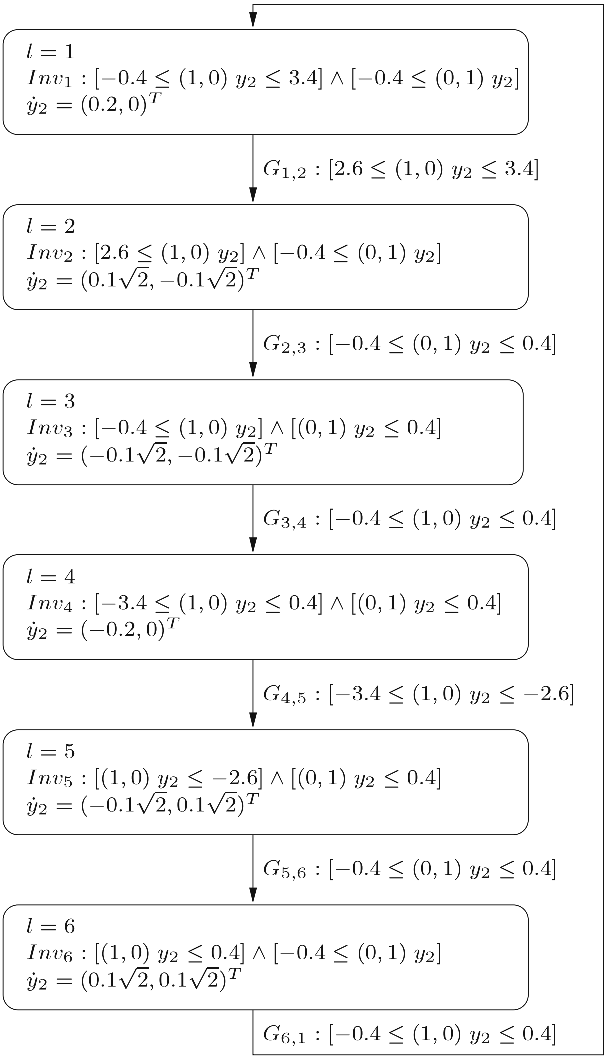

Fig. 3 Hybrid system approximating the system shown in Fig. 1

is a common simulation function for the continuous dynamics in each mode. We are in the situation described in the Section 4.2.3 and it is clear that the assumptions (c) and (d) of Theorem 2 hold with $\beta_1 = \cdots = \beta_6 = 0.4$. We then choose the invariants and the guards so that assumptions (a) and (b) hold as well. The resulting approximate hybrid system is shown in Fig. 3. It approximately simulates the system shown in Fig. 1 with precision 0.4. Let us remark that it is a planar linear hybrid automata for which reachability analysis is much simpler to perform using a tool such PHAVer (Frehse 2005).

We performed the reachability analysis for both system. For the original system, the algorithm does not terminate and we had to stop after a given number of iterations. The computed set is represented in Fig. 4. For the approximate system, we can compute exactly the reachable set. It is also represented in Fig. 4. We know

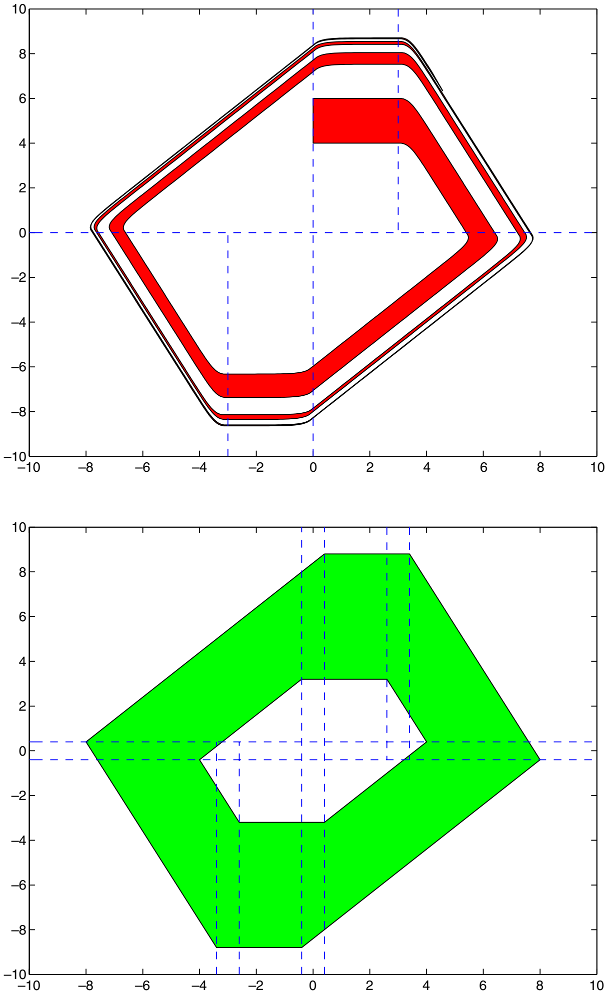

Fig. 4 Reachable sets of the original hybrid system (*top*) and of its approximation (*bottom*). The *dashed lines* represent the guards. We can see that the approximate hybrid system allows to conclude that the robot remains in an annulus centered around 0

that the reachable set of the original system is included in the 0.4-neighbourhood of the reachable set of the approximate system.[2] This allows us to guarantee that the robot will remain forever in an annulus centered around 0.

6 Conclusion

In this paper, we extended the notion of approximate simulation relations to hybrid systems. We developed a characterization of approximate simulation relations for

[2]Note that Theorem 1 states approximate inclusion and not approximate equality of the languages. This is why the precision of the over-approximation of the reachable sets on Fig. 4 is not uniform.

hybrid systems based on simulation functions for the continuous dynamics. For several classes of hybrid systems, we derived effective procedures for the computation of approximate simulation relations. We showed how our framework could be used to approximate hybrid systems and a non-trivial example in the context of reachability analysis was shown.

Future work includes developing more systematic methods to compute approximate simulation relations for hybrid systems as well as implementing these methods in the toolbox MATISSE.

References

de Alfaro L, Faella M, Stoelinga M (2004) Linear and branching metrics for quantitative transition systems, ICALP'04, LNCS, vol 3142. Springer, pp 1150–1162

Alur R, Courcoubetis C, Halbwachs N, Henzinger TA, Ho P-H, Nicollin X, Olivero A, Sifakis J, Yovine S (1995) The algorithmic analysis of hybrid systems. Theor Comput Sci 138(1): 3–34

Alur R, Henzinger TA, Lafferriere G, Pappas GJ (2000) Discrete abstractions of hybrid systems. In: Proceedings of the IEEE, vol 88(7), pp 971–984

Belta C, Isler V, Pappas GJ (2005) Discrete abstractions for robot planning and control in polygonal environments. IEEE Trans on Robotics 21(5):864–874

Clarke EM, Grumberg O, Peled DA (2000) Model checking. MIT Press

Desharnais J, Gupta V, Jagadeesan R, Panangaden P (2004) Metrics for labelled Markov processes. Theor Comput Sci 318(3):323–354

Fainekos GE, Girard A, Pappas GJ (2007) Hierarchical synthesis of hybrid controllers from temporal logic specifications. Hybrid systems: computation and control, LNCS, vol 4416. Springer, pp 203–216

Freeman RA, Kokotovic PV (1996) Inverse optimality in robust stabilization. SIAM J Control Optim 34(4):1365–1391

Frehse G (2005) PHAVer: algorithmic verification of hybrid systems past hyTech. Hybrid systems: computation and control, LNCS, vol 3414. Springer, pp 258–273

Girard A, Pappas GJ (2007a) Approximation metrics for discrete and continuous systems. IEEE Trans Autom Control 52(5):782–798

Girard A, Pappas GJ (2007b) Approximation bisimulation relations for constrained linear systems. Automatica 43(8):1307–1317

Girard A, Pappas GJ (2005) Approximate bisimulations for nonlinear dynamical systems. In: Proc. IEEE Conference on Decision and Control and European Control Conference. IEEE, pp 684–689, December

Haghverdi E, Tabuada P, Pappas GJ (2005) Bisimulation relations for dynamical, control, and hybrid systems. Theor Comput Sci 342(2–3):229–262

Julius AA (2006) Approximate abstraction of stochastic hybrid automata. Hybrid systems: computation and control, LNCS, vol 3927. Springer, pp 318–332

Julius AA, Girard A, Pappas GJ (2006) Approximate bisimulation for a class of stochastic hybrid systems. In: Proc American Control Conference

Liberzon D, Sontag ED, Wang Y (2002) Universal construction of feedback laws achieving ISS and integral-ISS disturbance attenuation. Syst Control Lett 46:111–127

Milner R (1989) Communication and concurrency. Prentice-Hall

Pappas GJ (2003) Bisimilar linear systems. Automatica 39(12):2035–2047

Pola G, van der Schaft AJ, Di Benedetto MD (2004) Bisimulation theory for switching linear systems. In: Proc of the 43rd IEEE Conference on Decision and Control

Prajna S, Papachristodoulou A, Seiler P, Parrilo PA (2005) SOSTOOLS and its control applications. Positive Polynomials in Control. Springer

Tabuada P (2007) Symbolic models for control systems. Acta Informatica 43(7):477–500

van der Schaft A (2004) Equivalence of dynamical systems by bisimulation. IEEE Trans Autom Control 49(12):2160–2172

Antoine Girard received the Dip.Ing. from the Ecole Nationale Supérieure d'Informatique et de Mathématiques Appliquées de Grenoble, Grenoble, France, the M.S. degree in applied mathematics from the Université Joseph Fourier, Grenoble, France, both in 2001 and the Ph.D. degree in applied mathematics from the Institut National Polytechnique de Grenoble, France, in September 2004.

From October 2004 to December 2005, he was a postdoctoral researcher at the Department of Electrical and Systems Engineering of the University of Pennsylvania, Philadelphia and from January to August 2006, he was a postdoctoral researcher at the Verimag laboratory, Grenoble, France. Since September 2006, he has been an Assistant Professor at the Université Joseph Fourier, Grenoble, France.

His research interests include algorithmic analysis and approximation theory of discrete, continuous and hybrid systems as well as hierarchical and multiscale approaches to control.

Anak Agung Julius received the ST (Bachelor of Engineering) degree from Institut Teknologi Bandung, Indonesia, in 1998, the MSc and PhD degrees in Applied Mathematics from Universiteit Twente, The Netherlands, in 2001 and 2005, respectively.

He is a postdoctoral researcher at the GRASP Laboratory, School of Engineering and Applied Sciences, University of Pennsylvania. His research interests include hybrid systems, systems biology, and systems and control theory.

George J. Pappas (S'91-M'98-SM'04) received the Ph.D. degree in electrical engineering and computer sciences from the University of California, Berkeley, in 1998. He is currently a Professor in the Department of Electrical and Systems Engineering, and the Director of the GRASP Laboratory. He also holds secondary appointments in the Departments of Computer and Information Sciences, and Mechanical Engineering and Applied Mechanics.

He has published extensively in the areas of hybrid systems, hierarchical control systems, distributed control systems, nonlinear control systems, and geometric control theory, with applications to robotics, unmanned aerial vehicles, and biomolecular networks. He coedited Hybrid Systems: Computation and Control (New York: Springer-Verlag, 2004, ser. Lecture Notes in Computer Science).

Dr. Pappas was the recipient of a National Science Foundation (NSF) Career Award in 2002, as well as the 2002 NSF Presidential Early Career Award for Scientists and Engineers (PECASE). He received the 1999 Eliahu Jury Award for Excellence in Systems Research from the Department of Electrical Engineering and Computer Sciences, University of California at Berkeley. His and his students' papers were finalists for the Best Student Paper Award at the IEEE Conference on Decision and Control (1998, 2001, 2004, 2006), the American Control Conference (2001 and 2004), and the IEEE Conference on Robotics and Automation (2007). He is currently serving as an Associate Editor for the IEEE Transactions on Automatic Control.