APPROXIMATE SIMULATION RELATIONS FOR HYBRID SYSTEMS [1]

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

* *Department of Electrical and Systems Engineering*
University of Pennsylvania
Philadelphia, PA 19104
{agirard,agung,pappasg}@seas.upenn.edu

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 notion to hybrid systems. Using the so-called simulation functions, we develop a computationally effective characterization of approximate simulation relations which can be used for hybrid systems approximation. An example of application in the context of safety verification is shown.

Keywords: Approximation of hybrid systems, 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 relations (Clarke *et al.*, 2000). These concepts have been useful for simplifying problems such as safety verification or controller synthesis. More recently, they have been extended to the framework of continuous and hybrid systems (Pappas, 2003; Haghverdi *et al.*, 2005) allowing the approximation of systems in a unified (discrete/continuous) manner.

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 is quite restrictive and not robust. The notion of language approximation is much more adequate in this context. In (Girard and Pappas, 2005*c*), 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 and remain equal, we require that they are and remain arbitrarily close. This approach not only defines more robust relations between systems but also allows more significant complexity reduction in the approximation process. In (Girard and Pappas, 2005*a*; Girard and Pappas, 2005*b*), this framework has been applied to constrained linear systems and nonlinear autonomous systems. Computational methods have been developed to quantify the distance between two systems. In (Julius *et al.*, 2006; Julius, 2006), the theoretical and computational frameworks have been extended to handle stochastic dynamical and hybrid systems (with purely stochastic 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 so-called simulation functions (Girard and Pappas, 2005*c*), we

[1] This research is partially supported by the Région Rhône-Alpes (Projet CalCel) and the NSF Presidential Early CAREER (PECASE) Grant 0132716.

develop a computationally effective characterization of approximate simulation relations which can be used for hybrid systems approximation. An example of application in the context of safety verification is shown.

2. APPROXIMATION OF TRANSITION SYSTEMS

In this section, we summarize the notion of approximate simulation relations for labeled transition systems as developed in (Girard and Pappas, 2005*c*). Labeled transition systems allow to model in a unified framework, discrete, continuous and hybrid systems. They can be seen as graphs, possibly with an infinite number of states or transitions.

Definition 2.1. A labeled 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,

$$q^0 \overset{\sigma^0}{\rightarrow} q^1 \overset{\sigma^1}{\rightarrow} q^2 \overset{\sigma^2}{\rightarrow} \ldots, \text{ where } \mathrm{q}^0 \in \mathrm{Q}^0.$$

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. The associated external trajectory

$$\pi^0 \overset{\sigma^0}{\rightarrow} \pi^1 \overset{\sigma^1}{\rightarrow} \pi^2 \overset{\sigma^2}{\rightarrow} \ldots, \text{ where } \pi^{\mathrm{i}} = \langle\langle \mathrm{q}^{\mathrm{i}} \rangle\rangle$$

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

Exact simulation relations between two labeled transition systems require that their observations are (and remain) identical (Clarke *et al.*, 2000). Approximate simulation relations are less rigid since they only require that the observations of both systems are (and remain) arbitrarily close. 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 labeled 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 2.2. 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) $\forall q_1 \overset{\sigma}{\rightarrow}_1 q_1', \exists q_2 \overset{\sigma}{\rightarrow}_2 q_2'$ such that $(q_1', q_2') \in \mathcal{S}_\delta$.

Note that for $\delta = 0$, we have the usual notion of *exact* simulation relation (Clarke *et al.*, 2000).

Definition 2.3. 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 $q_1 \in \mathcal{Q}_1^0$, there exists $q_2 \in \mathcal{Q}_2^0$ 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 2.4. (Girard and Pappas, 2005*c*) If $T_1 \preceq_\delta T_2$, then for all external trajectories of T_1,

$$\pi_1^0 \overset{\sigma^0}{\rightarrow} \pi_1^1 \overset{\sigma^1}{\rightarrow} \pi_1^2 \overset{\sigma^2}{\rightarrow} \ldots,$$

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

$$\pi_2^0 \overset{\sigma^0}{\rightarrow} \pi_2^1 \overset{\sigma^1}{\rightarrow} \pi_2^2 \overset{\sigma^2}{\rightarrow} \ldots$$

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

Approximation of transition systems based on approximate simulation relations is useful for solving the safety verification problem. Indeed, from Theorem 2.4, it is straightforward that if T_2 approximately simulates T_1 with the precision δ and $\mathrm{Reach}(T_2) \cap \mathcal{N}_\Pi(\Pi_U, \delta) = \emptyset$ (where $\mathcal{N}_\Pi(., \delta)$ denotes the δ-neighborhood for the metric d_Π), then $\mathrm{Reach}(T_1) \cap \Pi_U = \emptyset$. 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 show that hybrid systems can be formulated as transition systems. A hybrid system is defined as 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, $L = \{1, \ldots, |L|\}$.
- $n : L \rightarrow \mathbb{N}$, where for every $l \in L$, 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 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 in 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 accounting for disturbances and modelling uncertainties. While the discrete part of the state is l, the continuous part evolves 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 in 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 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 is not defined here. In the spirit of (Alur *et al.*, 1995), we can derive from H a 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 than in H. The set of labels is $\Sigma = \mathbb{R}^+ \cup \{\tau\}$. The observation map is given by

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

The transition relation $\to$ is given by:

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

$$\dot{z}(s) = f_l(z(s), u(s))$$

with $u(s) \in U_l$ 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 observation Π of a hybrid system is equipped with the following metric d_Π:

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

In the following, we show that our approximation framework based on approximate simulation relations can be applied 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 $T_i = (Q_i, \Sigma_i, \to_i, Q_i^0, \Pi_i, \langle\langle . \rangle\rangle_i)$, $(i = 1, 2)$ be the associated 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.* $L_1 = L_2 = L$, $p_1 = p_2 = p$). [2] We will further assume that the discrete dynamics of both systems are the same (*i.e.* $E_1 = E_2 = E$). The goal of the approximation process presented here is then essentially to simplify the continuous dynamics of the hybrid system H_1. In this section, we establish sufficient conditions so that H_2 approximately simulates H_1 and provide a method to evaluate the precision of the approximate simulation relation.

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:

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

In (Girard and Pappas, 2005*c*), we showed that approximate simulation relations could be characterized efficiently using the notion of simulation

[2] The approximation of a hybrid systems by another hybrid systems with a smaller number of locations has been considered for systems with purely stochastic jumps (Julius, 2006). We will also consider this type of approximation for hybrid systems with non stochastic jumps in the future.

function. In our context, this can be instantiated as follows.

Definition 4.1. $V_l : \mathbb{R}^{n_{1,l}} \times \mathbb{R}^{n_{2,l}} \to \mathbb{R}^+$ is a simulation function of $F_{1,l}$ by $F_{2,l}$ if for all $x \in \mathbb{R}^{n_{1,l}} \times \mathbb{R}^{n_{2,l}}$,

$$V_l(x) \geq g_l(x)^T g_l(x), \quad (1)$$

$$\max_{u_1 \in U_{1,l}} \min_{u_2 \in U_{2,l}} \nabla V_l(x)^T f_l(x, u_1, u_2) \leq 0. \quad (2)$$

Remark 4.2. The concept of simulation function is related to robust control Lyapunov functions (Freeman and Kokotovic, 1996; Liberzon *et al.*, 2002), though they slightly differ in spirit. Indeed, considering the input u_1 as a disturbance and the input u_2 as a control variable, the interpretation of equation (2) is that for all disturbances there exists a control such that the simulation function decreases during the evolution of the system. In this context, u_2 may have full knowledge (and be a function) of u_1. In comparison, a robust control Lyapunov function would require that there exists a control u_2 such that for all possible (and unknown) disturbances u_1 the function decreases during the evolution of the system. Therefore, robust control Lyapunov functions require stronger conditions than simulation functions.

Methods for the computation of simulation functions have been proposed for the class of constrained linear systems (Girard and Pappas, 2005*a*) and autonomous nonlinear systems (Girard and Pappas, 2005*b*). These methods are based on linear matrix inequalities, sum of squares programs and static games and are thus computationally effective. The computation of simulation functions for constrained linear systems has been implemented in the Matlab toolbox MATISSE [3].

Simulation functions satisfy the following property which will be useful in characterizing approximate simulation relations for hybrid systems.

Proposition 4.3. For all $(x_1, x_2) \in \mathbb{R}^{n_{1,l}} \times \mathbb{R}^{n_{2,l}}$, for all inputs $u_1(.)$, there exists an input $u_2(.)$ such that

$$\forall t \in \mathbb{R}^+, V_l(z_1(t), z_2(t)) \leq V_l(x_1, x_2) \quad (3)$$

where

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

Proof: Let us remark that

$$\dot{V}_l(z(t)) = \nabla V_l(z(t))^T f_l(z(t), u_1(t), u_2(t))$$

where $z(t) = [z_1(t)\ z_2(t)]^T$. Then, from equation (2), it is clear that for all inputs $u_1(.)$, there exists an input $u_2(.)$ such that $\dot{V}_l(z(t)) \leq 0$. ■

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

4.2 Approximate simulation relations

In this section, we give a characterization of approximate simulation relations for hybrid systems. 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, for all $x_1 \in \mathbb{R}^{n_{1,l}}$, $\beta \geq 0$,

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

Theorem 4.4. Let $\beta_1, \ldots, \beta_{|L|}$ be positive numbers such that

(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 $l \in L$,

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

(d) for all $e = (l, l') \in E$,

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

Let $\delta = \max(\sqrt{\beta_1}, \ldots, \sqrt{\beta_{|L|}})$. 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 equation (1), we have that $\|g_{l,1}(x_1) - g_{l,2}(x_2)\| \leq \sqrt{\beta_l} \leq \delta$. Hence, the first property of Definition 2.2 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 4.3, 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 4.4 insures 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 4.4 ensures that $x_2 \in G_{2,e}$. From assumption (d) of Theorem 4.4, 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 (c) of Theorem 4.4, 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 $T_1 \preceq_\delta T_2$. ■

Assumption (d) can be interpreted as a condition of non-propagation of the approximation error through the reset maps. It is clear that the scalars $\beta_1, \ldots, \beta_{|L|}$ cannot be chosen independently. Thus, it is not necessarily the case that such numbers exist. There are two cases where we can guarantee easily the existence of these numbers. First, if we consider memoryless resets (*i.e.* $R_{1,e}(x_1) = R_{1,e}$ and $R_{2,e}(x_2) = R_{2,e}$ for all $e \in E$), then we can see that $\beta_1, \ldots, \beta_l$ can be chosen independently. Second, if the graph (L, E) does not contain any cycle, then there is no circular dependency between $\beta_1, \ldots, \beta_{|L|}$ and thus it is easy to compute numbers such that the fourth assumption holds.

4.3 Approximation of hybrid systems

Based on Theorem 4.4, we can define a procedure to approximate a hybrid systems 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.

First, in each location $l \in L$, we approximate the continuous dynamics $F_{1,l}$ by a *simpler* continuous dynamics $F_{2,l}$. If $F_{1,l}$ is a large linear system, then $F_{2,l}$ may be chosen as a smaller linear system (Girard and Pappas, 2005*a*). If $F_{1,l}$ is a nonlinear system, then $F_{2,l}$ may be chosen as a linear system (Girard and Pappas, 2005*b*). The goal of this approximation is to reduce the complexity of analysis tasks such as reachability computation. Then, we compute a simulation function V_l of the continuous dynamics $F_{1,l}$ by $F_{2,l}$. Note that such a function always exists if $F_{1,l}$ and $F_{2,l}$ are asymptotically stable. In the case of nonstable systems, a simulation function exists if the unstable subsystem of $F_{2,l}$ exactly simulates the unstable subsystem of $F_{1,l}$ (Girard and Pappas, 2005*a*).

The second part of the procedure consists in choosing the initial sets $I_{2,l}^0$ and the reset maps $R_{2,e}$ and computing scalars $\beta_1, \ldots, \beta_{|L|}$ satisfying the assumptions (c) and (d) of Theorem 4.4. Then, we set the invariants $Inv_{2,l} = \mathcal{N}_l(Inv_{1,l}, \beta_l)$ and the guards $G_{2,e} = \mathcal{N}_l(G_{1,e}, \beta_l)$ where $e = (l, l')$. From Theorem 4.4, we know that $T_1 \preceq_\delta T_2$ with $\delta = \max(\sqrt{\beta_1}, \ldots, \sqrt{\beta_{|L|}})$.

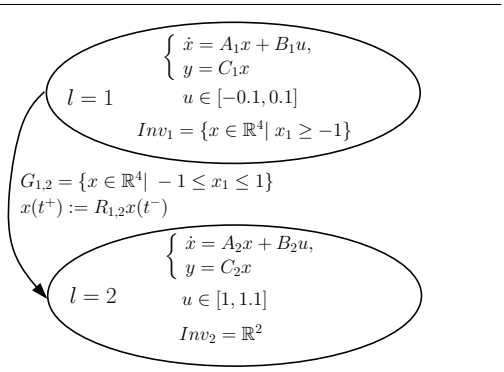

Fig. 1. Example of hybrid system

5. EXAMPLE

In this section, we illustrate our approximation framework in the context of a safety verification problem. Let us consider the hybrid system described in Figure 1. In each location, the continuous linear dynamics are given by the following matrices:

$$A_1 = \begin{bmatrix} -0.5 & 3 & 0 & 0 \\ -3 & -0.5 & 1 & 0 \\ 0 & 0 & -0.7 & 8 \\ 0 & 0 & -8 & -0.7 \end{bmatrix}, B_1 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, C_1^T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$A_2 = \begin{bmatrix} -0.5 & 1 \\ 0 & -1 \end{bmatrix}, B_2 = \begin{bmatrix} -10 \\ 5 \end{bmatrix}, C_2^T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

The linear reset map is given by $R_{1,2} = \left[\begin{smallmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right]$. The set of initial states is

$$Q^0 = \{1\} \times ([4, 5] \times [4, 5] \times [0.9, 1.1] \times \{0\}).$$

Let us consider the safety verification problem where the set of unsafe sets is

$$\Pi_U = \{2\} \times \left\{ y \in \mathbb{R}^2 |\ (y_1 + 10)^2 + (y_2 + 1)^2 \leq 1 \right\}.$$

In order to solve the safety verification problem, we will use a two dimensional approximation of the continuous dynamics in location 1, given by the following matrices:

$$A_1' = \begin{bmatrix} -0.5 & 3 \\ -3 & -0.5 \end{bmatrix}, B_1' = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, C_1' = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

The two dimensional dynamics in location 2 will be kept unchanged. The reset map of the approximate hybrid system is given by the matrix $R_{1,2}' = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$. The initial set is

$$Q'^0 = \{1\} \times ([4, 5] \times [4, 5]).$$

Simulation functions between the continuous dynamics are computed using the toolbox MATISSE. This essentially consists in solving a set of linear matrix inequalities and quadratic programs. Then, we compute β_1 and β_2 such that assumptions (c) and (d) of Theorem 4.4 hold. The invariant of location 1 and the guard of the transition $(1, 2)$ are bloated according to these numbers. The precision of the approximate simulation relation between the original hybrid system and its approximation is $\delta = 0.3877$. We computed the reachable sets of both systems using zonotope based reachability algorithms (Girard, 2005) implemented in MATISSE. We can see on Figure 2

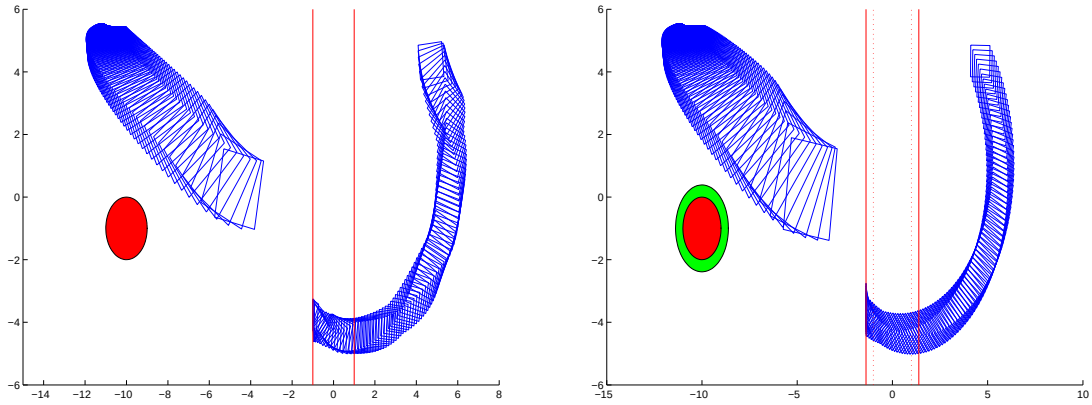

Fig. 2. Reachable sets of the original hybrid system (left) and of its approximation (right). We can see that the approximation allows to conclude that the original system is safe.

that the reachable set of the approximate hybrid system does not intersect the bloated unsafe set. Hence, this allows to conclude that the original hybrid system is safe.

6. CONCLUSION

In this paper, we extended the notion of approximate simulation relations to hybrid systems. We developed an effective characterization of approximate simulation relations based on simulation functions. We showed how our framework could be used to approximate hybrid systems and an example in the context of safety verification was shown. Future work includes developing more systematic methods to compute approximate simulation relations for hybrid systems as well as implementing these methods in MATISSE.

REFERENCES

Alur, R., T.A. Henzinger, G. Lafferriere and G.J. Pappas (2000). Discrete abstractions of hybrid systems. *Proceedings of the IEEE* **88**, 971–984.

Alur, Rajeev, Costas Courcoubetis, Nicolas Halbwachs, Thomas A. Henzinger, Pei-Hsin Ho, Xavier Nicollin, Alfredo Olivero, Joseph Sifakis and Sergio Yovine (1995). The algorithmic analysis of hybrid systems.. *Theor. Comput. Sci.* **138**(1), 3–34.

Clarke, E. M., O. Grumberg and D. A. Peled (2000). *Model Checking*. MIT Press.

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

Desharnais, J., V. Gupta, R. Jagadeesan and P. Panangaden (2004). Metrics for labelled markov processes. *Theor. Comput. Sc.* **318**(3), 323–354.

Freeman, R. A. and P. V. Kokotovic (1996). Inverse optimality in robust stabilization. *SIAM J. Control and Optimization* **34**(4), 1365–1391.

Girard, A. (2005). Reachability of uncertain linear systems using zonotopes. In: *Hybrid Systems: Computation and Control*. Vol. 3414 of *LNCS*. Springer. pp. 291–305.

Girard, A. and G. J. Pappas (2005*a*). Approximate bisimulations for constrained linear systems. In: *Proc. IEEE Conference on Decision and Control and European Control Conference*.

Girard, A. and G. J. Pappas (2005*b*). Approximate bisimulations for nonlinear dynamical systems. In: *Proc. IEEE Conference on Decision and Control and European Control Conference*.

Girard, A. and G. J. Pappas (2005*c*). Approximation metrics for discrete and continuous systems. Technical Report MS-CIS-05-10, Dept. of CIS, University of Pennsylvania.

Haghverdi, E., P. Tabuada and G. J. Pappas (2005). Bisimulation relations for dynamical, control, and hybrid systems. *Theor. Comput. Sc.* **342**(2-3), 229–262.

Julius, A.A. (2006). Approximate abstraction of stochastic hybrid automata. In: *Hybrid Systems: Computation and Control*. Vol. 3927 of *LNCS*. Springer. pp. 318–332.

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

Liberzon, D., E. D. Sontag and Y. Wang (2002). Universal construction of feedback laws achieving ISS and integral-ISS disturbance attenuation. *Systems and Control Letters* **46**, 111–127.

Pappas, G. J. (2003). Bisimilar linear systems. *Automatica* **39**(12), 2035–2047.