

# Compositional and Assume-Guarantee Reasoning for Switching Linear Systems

Florian Kerber\* Arjan J. van der Schaft\*

\* University of Groningen, Institute of Mathematics and Computing Science, P.O. Box 407, 9700AV Groningen, The Netherlands, Phone: +31(0)50 363 3972, email:{F.J.Kerber,A.J.van.der.Schaft}@rug.nl

**Abstract:** Modular modeling techniques play an important role in the analysis of engineering processes as well as in control applications. While individual components of aggregated models can be relatively simple, complexity increases significantly when interconnections are considered. To address the problem of complexity explosion, simulation relations can be employed to abstract system behaviors by lower order models. As an application to formal verification, simulation relations allow to check system properties such as safety requirements. In a compositional framework, they can be used to approximate interconnections of systems based on approximations of the individual components. While results with regard to compositional analysis have been presented for discrete and recently also for continuous-time systems, it is our aim to develop compositional and assume-guarantee reasoning for a specific class of hybrid systems, namely switching linear systems.

*Keywords:* Switching Linear Systems, Simulation Relations, Compositional Reasoning, Assume-Guarantee Reasoning

## 1. INTRODUCTION

Engineering systems can usually be viewed as the interconnection of interacting subsystems. Therefore, modular techniques to derive mathematical models of processes are widely used in different branches of engineering. While beneficial with regard to standardization, the complexity of such models increases rapidly with the number of subsystems. This problem is well known in the theory of concurrent processes, see e.g. Clarke et al. (1999). As a result, methods have been developed to tackle the complexity issue, amongst which the concept of simulation (or, as a bilateral version, bisimulation), c.f. Milner (1989). Simulation relations can be used to abstract systems by lower dimensional models that approximate the original input-/output behavior. In recent years, the concept of simulations has been adapted to be applicable for continuous-time systems, see Pappas et al. (2000) and van der Schaft (2004a) as examples. Formal verification is another field where simulation relations have proved to be useful. For that purpose, system properties such as safety requirements are formulated in the formalism of a temporal logic which can then be checked using simulation relations, see Clarke et al. (1999) for a detailed treatment. Our focus lies on the compositional analysis of switching linear systems, as a first class of hybrid systems. The key idea is to infer properties of interconnections from known properties of component systems using simulations. The first property to be considered is *invariance under composition*. If the component systems  $\Sigma_{P_1}$  and  $\Sigma_{Q_1}$  are approximated by  $\Sigma_{P_2}$  and  $\Sigma_{Q_2}$  on a possibly coarser level of abstraction, invariance under composition ensures that also the interconnection of the abstractions  $\Sigma_{Q_1} \parallel \Sigma_{Q_2}$  can

serve as an abstraction of the interconnection of the original systems  $\Sigma_{P_1} \parallel \Sigma_{P_2}$ ,

$$\text{rule 1: } \frac{\Sigma_{P_1} \preceq \Sigma_{Q_1}, \Sigma_{P_2} \preceq \Sigma_{Q_2}}{\Sigma_{P_1} \parallel \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel \Sigma_{Q_2}}$$

Invariance under composition is the basic property for compositional analysis albeit possibly restrictive. Indeed, a component system might not be simulated by any other systems in general but only in a restricted environment, i.e. when interconnected with other components. This principle is used in assume-guarantee reasoning (AGR) thus offering an alternative method to abstract interconnected systems, see also Misra and Chandy (1981) and Henzinger et al. (2001). There are two basic types: In *non-circular* assume-guarantee reasoning, the to be proven implications of a rule, the so-called guarantees, are derived from independent assumptions. Therefore, non-circular rules directly result from compositionality properties which ensure their validity. In the terminology of assume-guarantee reasoning, such a rule is *sound*. For the purpose of this paper, the following non-circular rule will be investigated:

$$\text{rule 2: } \frac{\begin{array}{l} \text{(A1)} \\ \text{(B1)} \\ \text{(C1)} \end{array} \quad \frac{\Sigma_{P_1} \preceq \Sigma_{Q_1}}{\Sigma_{Q_1} \parallel \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel \Sigma_{Q_2}}}{\Sigma_{P_1} \parallel \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel \Sigma_{Q_2}}$$

It should be pointed out that the symmetric counterpart of rule 1, i.e. replacing statement (A1) by  $\Sigma_{P_2} \preceq \Sigma_{Q_2}$  and (B1) by  $\Sigma_{P_1} \parallel \Sigma_{Q_2} \preceq \Sigma_{Q_1} \parallel \Sigma_{Q_2}$ , is an equally valid non-circular rule based on only one unconditional assumption. On the contrary, *circular* assume-guarantee reasoning involves dependencies of assumptions on to be proven guar-

antees in the course of reasoning. As an example, consider the following

$$\text{rule 3: } \frac{\begin{array}{l} \text{(A2)} \quad \Sigma_{P_1} \parallel \Sigma_{Q_2} \preceq \Sigma_{Q_1} \parallel \Sigma_{Q_2} \\ \text{(B2)} \quad \Sigma_{Q_1} \parallel \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel \Sigma_{Q_2} \\ \text{(C2)} \quad \Sigma_{P_1} \parallel \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel \Sigma_{Q_2} \end{array}}{\quad}$$

It is known from the assume-guarantee literature that proof obligations like rule 3 are usually not sound, i.e. they are only valid under some additional conditions.

Due to its origin in computing science, compositional analysis techniques have been applied extensively to discrete-event systems. Frehse (2005) presented results for labeled transition systems with regard to the above mentioned rules 1–3. Recently, compositional and assume-guarantee reasoning was investigated for linear time-invariant dynamical systems, see Kerber and van der Schaft (2008) using tools from geometric control theory. Combining techniques for discrete and continuous-time processes facilitates the study of hybrid systems which have become increasingly popular in modeling physical systems. In computing science, one usually describes the continuous evolution of hybrid systems by means of valuations of the continuous variables, see e.g. Alur et al. (2000) and Henzinger et al. (2001). Compositional and assume-guarantee reasoning for such types of hybrid systems therefore prioritizes the discrete over the continuous dynamics, see as an example Frehse (2005). On the contrary, the standard approach in control theory is to describe the continuous evolution of hybrid systems by differential equations. This approach is advantageous since it does not rely on the computation of actual system trajectories (which is often not possible). Furthermore, it turns out that simulation relations can be computed effectively on the basis of differential equations. For linear systems, this computation relies on linear algebra. This allows us to focus on a particular class of hybrid systems, namely switching linear systems (SLS) as described e.g. in Pola et al. (2006). The particular structure of SLS's makes it possible to define a structural notion of hybrid simulation.

The paper is organized as follows: In Section 2, switching linear systems and their time evolution are defined. Interconnections of SLS's are investigated in Section 3 restating the main results for compositional reasoning for the discrete and continuous layer. A formal definition as well as a structural notion of hybrid simulation relations are introduced in Section 4. The main results for compositional and assume-guarantee reasoning for SLS's are given in Section 5. In the concluding remarks of Section 6 we sketch possible extensions of the above methodology.

## 2. PRELIMINARIES AND BASIC DEFINITIONS

In our definition of switching linear systems, we will incorporate the structure of labeled transition systems with transition labels on the level of the discrete dynamics and linear continuous-time systems on the level of the continuous dynamics following the definitions in Pola et al. (2006).

*Definition 1.* (Switching linear system)

A switching linear system  $S$  is a tuple  $S = (\Xi, U, Y, V, \Sigma, E, M)$  with

- $\Xi = \bigcup_{q \in Q} \{q\} \times X(q)$  the hybrid state space where  $Q = \{q_1, \dots, q_N\}$ ,  $N \in \mathbb{N}$  is the discrete state

space with associated continuous state space  $X(q) \subset \mathbb{R}^{\dim(q)}$ ,  $\dim : Q \rightarrow \mathbb{N}$ ,

- $U = \mathbb{R}^m$  and  $Y = \mathbb{R}^p$  the linear continuous input and output spaces, respectively,
- $V$  the set of discrete transition labels,
- $\Sigma$  a function associating to every discrete state  $q$  the deterministic linear continuous-time system

$$\Sigma(q) : \begin{cases} \dot{x}(t) = A(q)x(t) + B(q)u(t), \\ y(t) = C(q)x(t) \end{cases}$$

- $E \subset Q \times V \times Q$  the transition relation
- $M$  a reset function associating to every  $e = (q, v, q') \in E$  a reset matrix  $M(e) \in \mathbb{R}^{\dim(q) \times \dim(q')}$ .

The evolution of a SLS is influenced by uncontrollable discrete events  $v \in V$  causing the system to switch from one discrete state to another. The associated continuous dynamics, which are governed by linear systems  $\Sigma(q)$  in every discrete state, are reset with every transition  $e_i$  such that  $x(t_i^+) = M(e_i)x(t_i^-)$  where  $t_i^-$  and  $t_i^+$  represent the continuous time instants just before and after the occurrence of the  $i$ -th event, respectively. For a more detailed discussion of the semantics of hybrid systems we refer to van der Schaft and Schumacher (2001).

*Definition 2.* (Associated labeled transition system)

Given a SLS  $S = (\Xi, U, Y, V, \Sigma, E, M)$ , the associated labeled transition system (LTS)  $D_S$  is given by the triple  $D_S = (Q, V, E)$  where

- $Q$  represents the set of discrete states,
- $V$  the set of transition labels,
- and  $E \subset Q \times V \times Q$  the transition relation.

The trajectories of a SLS will be specified with respect to a hybrid time basis  $T$  (Lygeros et al. (1999)).

*Definition 3.* (Execution of a SLS)

An execution of a SLS  $S$  is a collection  $(\xi^0, T, u, y, v, \xi)$  where

- $\xi_0 = (q_0, x_0) \in \Xi$ ,  $q_0 = q(0) \in Q$ ,  $x_0 = x(t_0, 0) \in X(q(0))$  is the initial hybrid state;
- $T$  denotes the hybrid time basis which we define as follows:

$$T = \bigcup_{j=0}^J I_j \times \{j\}, J \in \mathbb{N} \cup \infty, \quad (1)$$

$$I_j = \{t \in \mathbb{R}_0^+ \mid t_j \leq t \leq t_{j+1}\}$$

- $u \in \mathcal{C}^0(\mathbb{R}_0^+, U)$ ;
- $y \in \mathcal{C}(\mathbb{R}_0^+, Y)$ ;
- $v \in \mathcal{C}(\mathbb{N}, V)$ ;
- $\xi = (q, x)$  where  $q \in \mathcal{C}(\mathbb{N}, Q)$  and  $x \in \mathcal{C}(\mathbb{R}_0^+ \times \mathbb{N}, X(\cdot))$  and  $\xi(t, j) = (q(j), x(t, j))$  for  $(t, j) \in T$ .

## 3. COMPOSITION OF SLS'S

Since there is only unidirectional interference, i.e. the discrete dynamics influences the continuous evolution by means of switches caused by discrete events but not vice versa, the two dynamics can be considered separately. Thus, one can define interconnections of SLS's by first determining the parallel composition of the associated LTS's and then interconnecting the respective continuous systems for every discrete state of the interconnection LTS whilst obeying the reset rules.

### 3.1 Interconnections and Simulations of Labeled Transition Systems

The interconnection of the discrete layer of two SLS's  $S_i, i = 1, 2$ , involves the labeled transition systems  $D_{S_i}$  associated to  $S_i, i = 1, 2$ . The treatment of these LTS's follows the standard definitions found in the computing science literature, in particular Milner (1989) and Frehse (2005).

*Definition 4.* (Parallel composition of LTS)

Consider two LTS  $D_i = (Q_i, V_i, E_i)$ . The parallel composition  $D_S = D_{S_1} \parallel_{pc} D_{S_2}$  is again a LTS  $D_S = (Q, V, E_{12})$  with

- $Q = Q_1 \times Q_2$
- $V = V_1 \cup V_2$
- $E_{12} = \begin{cases} ((q_1, q_2), v, (q'_1, q'_2)), v \in V_1 \cap V_2, \\ \quad (q_i, v, q'_i) \in E_i, i = 1, 2 \\ ((q_1, q_2), v, (q'_1, q'_2)), v \in V_1 \setminus V_2, \\ \quad (q_1, v, q'_1) \in E_1 \\ ((q_1, q_2), v, (q_1, q'_2)), v \in V_2 \setminus V_1, \\ \quad (q_2, v, q'_2) \in E_2 \end{cases}$

The notion of simulations is instrumental for compositional analysis since it provides a tool to relate LTS's with the same transition structure.

*Definition 5.* For any two LTS's  $D_1, D_2$  with the same set of labels  $V$ , a relation  $R \subset Q_1 \times Q_2$  is a simulation relation of  $D_1$  by  $D_2$  if and only if for all  $(q_1, q_2) \in R, v \in V$  and  $q'_1 \in Q_1$  the following holds:

$$(q_1, v, q_2) \in E_1 \implies \exists q'_2 \in Q_2 : (q_2, v, q'_2) \in E_2, (q'_1, q'_2) \in R$$

If there exists a simulation relation  $R$  of  $D_1$  by  $D_2$  such that  $\Pi_1 R = Q_1$ , then  $D_2$  **simulates**  $D_1$ , denoted by  $D_1 \preceq D_2$  and  $R$  is called a **full simulation relation**.

To prepare for the analysis of SLS's later, we restate the most important results for compositional and assume-guarantee reasoning. The following results are taken from Frehse (2005).

*Theorem 6.* (Invariance under composition for LTS)

Given LTS's  $D_i, i \in \{P_1, P_2, Q_1, Q_2\}$  such that  $V_{P_1} = V_{Q_1}, V_{P_2} = V_{Q_2}$  and define parallel composition  $\parallel_{pc}$  of LTS's as in Definition 4. Simulation of LTS's as defined in Definition 5 fulfils rule 1.

*Theorem 7.* (Soundness of AGR for LTS (Frehse (2005)))

Given LTS's  $D_i, i \in \{P_1, P_2, Q_1, Q_2\}$  such that  $V_{P_1} = V_{Q_1}, V_{P_2} = V_{Q_2}$  and define parallel composition  $\parallel_{pc}$  of LTS as in Definition 4. Then the non-circular AGR rule 1 is sound.

Moreover, the circular rule 2 is sound if and only if  $\forall ((p_1, p_2), (q_1, q_2)) \in R, v \in V_{P_1} \cap V_{P_2}$  the following *AGR condition* holds:

$$((p_1, p_2), v, (p'_1, p'_2)) \in E_{P_1 P_2} \implies$$

$$\exists q'_1 : (q_1, v, q'_1) \in E_{Q_1} \quad \vee \quad \exists q'_2 : (q_2, v, q'_2) \in E_{Q_2}$$

Intuitively, the AGR condition (2) ensures that the evolution of the approximation  $D_{Q_1} \parallel_{pc} D_{Q_2}$  will not be halted due to inactive transitions that are executable in  $D_{P_1} \parallel_{pc} D_{P_2}$ .

### 3.2 Interconnections and simulations of continuous-time dynamical systems

On the continuous layer, we are dealing with interconnections of linear time-invariant dynamical systems (LTI). In Kerber and van der Schaft (2008), we analyzed two different types of negative feedback interconnections for LTI systems.

*Definition 8.* (Interconnections of LTI systems)

Given two LTI systems

$$\Sigma_i : \begin{cases} \dot{\mathbf{x}}_i(t) = A_i \mathbf{x}_i(t) + B_i \mathbf{u}_i(t), & i = 1, 2 \\ \mathbf{y}_i(t) = C_i \mathbf{x}_i(t) \end{cases} \quad (3)$$

such that  $\dim \mathbf{u}_i = \dim \mathbf{y}_j, (i, j) \in \{(1, 2), (2, 1)\}$ .

Then we define the **open interconnection**  $\Sigma_1 \parallel_o \Sigma_2$  by

$$\begin{bmatrix} \mathbf{u}_1 \\ \mathbf{u}_2 \end{bmatrix} = \begin{bmatrix} 0 & -I \\ I & 0 \end{bmatrix} \begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \end{bmatrix} + \begin{bmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \end{bmatrix} \quad (4)$$

to obtain

$$\begin{bmatrix} \dot{\mathbf{x}}_1(t) \\ \dot{\mathbf{x}}_2(t) \end{bmatrix} = \begin{bmatrix} A_1 & -B_1 C_2 \\ B_2 C_1 & A_2 \end{bmatrix} \begin{bmatrix} \mathbf{x}_1(t) \\ \mathbf{x}_2(t) \end{bmatrix} + \begin{bmatrix} B_1 & 0 \\ 0 & B_2 \end{bmatrix} \begin{bmatrix} \mathbf{u}_1(t) \\ \mathbf{u}_2(t) \end{bmatrix}$$

$$\begin{bmatrix} y_1(t) \\ y_2(t) \end{bmatrix} = \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix}$$

The **closed interconnection**  $\Sigma_1 \parallel_{cl} \Sigma_2$  is accordingly defined by

$$\begin{bmatrix} \mathbf{u}_1 \\ \mathbf{u}_2 \end{bmatrix} = \begin{bmatrix} 0 & -I \\ I & 0 \end{bmatrix} \begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \end{bmatrix} \quad (5)$$

so that the closed loop interconnected system becomes

$$\begin{bmatrix} \dot{\mathbf{x}}_1(t) \\ \dot{\mathbf{x}}_2(t) \end{bmatrix} = \begin{bmatrix} A_1 & -B_1 C_2 \\ B_2 C_1 & A_2 \end{bmatrix} \begin{bmatrix} \mathbf{x}_1(t) \\ \mathbf{x}_2(t) \end{bmatrix}$$

$$\begin{bmatrix} \mathbf{y}_1(t) \\ \mathbf{y}_2(t) \end{bmatrix} = \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix} \begin{bmatrix} \mathbf{x}_1(t) \\ \mathbf{x}_2(t) \end{bmatrix}$$

Corresponding to Definition 5, simulations on the continuous-time level relate LTI systems with the same input-output behavior.

*Definition 9.* Given two systems  $\Sigma_i, i = 1, 2$  as in (3). A simulation relation  $S$  of  $\Sigma_1$  by  $\Sigma_2$  is a linear subspace of the product state space  $S \subset \mathcal{X}_1 \times \mathcal{X}_2$  with the following properties:

For any  $(x_{10}, x_{20}) \in S$  and any joint input function  $u_1(\cdot) = u_2(\cdot)$ , the resulting state trajectories  $x_i(\cdot), i = 1, 2$  with  $x_i(0) = x_{i0}$  should satisfy

$$(i) : \quad (x_1(t), x_2(t)) \in S \quad \forall t \geq 0 \quad (6)$$

$$(ii) : \quad C_1 x_1(t) = C_2 x_2(t) \quad \forall t \geq 0$$

Furthermore,  $\Sigma_1$  is **simulated** by  $\Sigma_2$ , denoted  $\Sigma_1 \preceq \Sigma_2$ , if there exists a simulation relation  $S \subset \mathcal{X}_1 \times \mathcal{X}_2$  fulfilling  $\Pi_{X_1} S = \mathcal{X}_1$ . In this case,  $S$  is called a **full simulation relation**.

*Remark 10.* In Kerber and van der Schaft (2008) we showed that there is an important difference between open and closed interconnections: For the open type, there is no need for assume-guarantee reasoning since proof obligations for open interconnections are as hard as obligations for individual components. Assume we are

given any four LTI systems  $\Sigma_i, i \in \{P_1, P_2, Q_1, Q_2\}$ . Considering open interconnections, one can show that

$$\Sigma_{P_1} \preceq \Sigma_{Q_1}, \Sigma_{P_2} \preceq \Sigma_{Q_2} \iff \Sigma_{P_1} \parallel_o \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel_o \Sigma_{Q_2} \quad (7)$$

which means one can always replace a simulation between interconnected systems by the respective simulation relations of the components involved. Thus, the AGR rules 2 and 3 are sound for open interconnections. On the contrary, AGR can indeed simplify proof obligations when closed interconnections are considered. In the remainder of this paper, we will therefore only treat closed interconnections of LTI systems.

Based on Kerber and van der Schaft (2008), the following theorems for LTI systems are available:

*Theorem 11.* (Invariance Under Composition for LTI systems)

Given LTI systems  $\Sigma_i, i \in \{P_1, P_2, Q_1, Q_2\}$ . Then simulation is invariant under composition with respect to closed interconnection (5).

*Theorem 12.* (AGR for LTI systems)

Given LTI systems  $\Sigma_i, i \in \{P_1, P_2, Q_1, Q_2\}$  and define closed composition  $\parallel_{cl}$  of LTI as in Definition 5. Then both the non-circular and the circular AGR rule 2 respectively 3 are sound.

It should be pointed out that the results for compositional and assume-guarantee reasoning are not restricted to the case of negative feedback alone but could be extended to other types of interconnections as well.

### 3.3 Interconnections of SLS's

The purpose of this paper is to study switching linear systems. The preparatory work of the previous sections allows us to finally define interconnections of SLS's.

*Definition 13.* (Interconnection of SLS)

Consider two SLS's  $S_i = (\Xi_i, U_i, Y_i, V_i, \Sigma_i, E_i, M_i), i = 1, 2$ . The interconnection  $S_1 \parallel_{SLS} S_2$  is a SLS  $S = (\Xi, U, Y, V, \Sigma, E_{12}, M)$  with

- $\Xi = \bigcup_{(q_1, q_2) \in Q} \{(q_1, q_2)\} \times X(q_1, q_2)$  where  $Q = Q_1 \times Q_2$  is the discrete state space resulting from the parallel composition of the LTS's  $D_i$  associated to  $S_i$ ,  $D_1 \parallel D_2$ , and  $X(q_1, q_2) = X(q_1) \times X(q_2)$  is determined by the closed interconnection of the respective continuous-time systems at every location  $(q_1, q_2) \in Q$ ,  $\Sigma_1(q_1) \parallel_{cl} \Sigma_2(q_2)$ .
- $U = \{0, 0\}$  due to the closed interconnection  $\Sigma_1(q_1) \parallel_{cl} \Sigma_2(q_2)$  in every  $(q_1, q_2) \in Q$ ,
- $Y = Y_1 \times Y_2$ ,
- $V$  and  $E_{12}$  as determined by the parallel composition of the respective LTS and
- $M(e) = \text{diag}\{\bar{M}_1, \bar{M}_2\}$  with

$$\bar{M}_i(e_i) = \begin{cases} M_i(e_i), & \text{if } q'_i \neq q_i, e_i = (q_i, v, q'_i) \in E_i \\ I, & \text{if } q_i = q'_i \end{cases}$$

## 4. SIMULATION RELATIONS FOR SLS'S

We want to use simulation relations to abstract system behaviors. Therefore, hybrid simulation for SLS's is defined so that the evolution is synchronized with respect to

discrete transitions.

*Definition 14.* (Hybrid simulation relation)

Given two SLS's  $S_i = (\Xi_i, U, Y, V_i, \Sigma_i, E_i, M_i), i = 1, 2$ , with the same continuous input and output spaces  $U = U_1 = U_2, Y = Y_1 = Y_2$  and the same set of discrete labels  $V = V_1 = V_2$ . A hybrid simulation relation of  $S_1$  by  $S_2$  is a subset  $\mathcal{S} \subset \Xi_1 \times \Xi_2$  with the following properties. Take any initial hybrid state  $(\xi_1^0, \xi_2^0) \in R$  and any input function  $u = u_1 = u_2$ .

Then for any hybrid execution  $\xi_1 = (\xi_1^0, T_1, u, y_1, v, \xi_1)$  there should exist an execution  $\xi_2 = (\xi_2^0, T_2, u, y_2, v, \xi_2)$  such that  $T_1 = T_2 = T$  and

- (i)  $\forall j \in \{0, 1, \dots, J\} :$   
 $(q_1(j), v(j+1), q_1(j+1)) \in E_1$   
 $\implies \exists q_2(j+1) : (q_2(j), v(j+1), q_2(j+1)) \in E_2$
- (ii)  $((q_1(j), x_1(t, j)), (q_2(j), x_2(t, j))) \in \mathcal{S} \forall (t, j) \in T$

Moreover, if there exists a hybrid simulation relation  $\mathcal{S}$  of  $S_1$  by  $S_2$  such that  $\Pi|_{\Xi_i} \mathcal{S} = \Xi_i, i = 1, 2$ , then  $S_1$  **simulates**  $S_2$ , denoted by  $S_1 \preceq S_2$ . In this case,  $\mathcal{S}$  is called a **full simulation relation**.

As a consequence of this definition, hybrid simulation relations possess the same properties as their discrete and continuous counterparts.

*Proposition 15.* Hybrid simulation as defined in Definition 14 is a preorder, i.e., reflexive and transitive.

**Proof.** (Sketch) Given SLS  $S_1, S_2$  and  $S_3$ .

(reflexivity) Consider a relation  $\mathcal{S} = \{(q, x), (q, x) \mid (q, x) \in \Xi_1\}$ . It is easy to check that  $\mathcal{S}$  is a hybrid simulation relation of  $S_1$  by  $S_1$ , in fact it is the finest one.

(transitivity) Assume there exist hybrid simulation relations  $\mathcal{S}_{12}$  and  $\mathcal{S}_{23}$  of  $S_1$  by  $S_2$  and  $S_2$  by  $S_3$ , respectively. Then  $\mathcal{S}_{13} := \{((q_1, x_1), (q_3, x_3)) \mid \exists (q_2, x_2) : ((q_1, x_1), (q_2, x_2)) \in \mathcal{S}_{12}, ((q_2, x_2), (q_3, x_3)) \in \mathcal{S}_{23}\}$  is a hybrid simulation relation of  $S_1$  by  $S_3$ .

Exploiting the structure of SLS's, in particular interdependencies between the discrete and continuous layer, facilitates the construction of hybrid simulation relations.

*Proposition 16.* If  $\mathcal{S}$  is a hybrid simulation relation of  $S_1$  by  $S_2$ , there exists  $Q_{\mathcal{S}} \subset Q_1 \times Q_2$  and for any  $(q_1, q_2) \in Q_{\mathcal{S}}$  suitable sets  $\mathcal{S}(q_1, q_2) \subset X_1(q_1) \times X_2(q_2)$  such that

$$((q_1, x_1), (q_2, x_2)) \in \mathcal{S} \iff (q_1, q_2) \in Q_{\mathcal{S}}, (x_1, x_2) \in \mathcal{S}(q_1, q_2)$$

*Remark 17.* It has been shown in Pola et al. (2006) that the sets  $\mathcal{S}(q_1, q_2)$  can be assumed to be linear subspaces. In fact, given a hybrid simulation relation  $\mathcal{S}$  of  $S_1$  by  $S_2$ , its linear closure

$$\begin{aligned} \mathcal{L}(\mathcal{S}) &= \{((q_1, x_1), (q_2, x_2)) \in \Xi_1 \times \Xi_2 \mid \\ &\quad (q_1, q_2) \in Q_{\mathcal{S}}, (x_1, x_2) \in \mathcal{L}(\mathcal{S}(q_1, q_2))\} \\ \mathcal{L}(\mathcal{S}(q_1, q_2)) &= \{\alpha(x_1, x_2) + \beta(x'_1, x'_2) \mid \alpha, \beta \in \mathbb{R}, \\ &\quad (x_1, x_2), (x'_1, x'_2) \in \mathcal{S}(q_1, q_2)\} \end{aligned}$$

is also a hybrid simulation relation of  $S_1$  by  $S_2$ . Therefore, we will assume in the remainder that the subsets of the continuous variable spaces  $\mathcal{S}(q_1, q_2)$  are indeed linear subspaces.

Since the set of discrete states  $Q_S$  gives rise to a simulation relation between the associated LTS's and similarly, the linear subspaces  $\mathcal{S}(q_1, q_2)$  at every location  $(q_1, q_2) \in Q_S$  define a simulation relation of the underlying LTI systems, the only direct coupling between discrete and continuous dynamics is imposed by the reset maps  $M_i(e_i)$ . This yields a more checkable notion of hybrid simulation which is usually referred to as structural hybrid simulation relation in the literature (van der Schaft (2004b)).

*Theorem 18.* (Structural hybrid simulation relation)

Given two SLSs  $S_1$  and  $S_2$  with the same set of labels  $V = V_1 = V_2$ , a set

$$\mathcal{S} = \{((q_1, x_1), (q_2, x_2)) \in \Xi_1 \times \Xi_2 \mid (q_1, q_2) \in Q_S, (x_1, x_2) \in \mathcal{S}(q_1, q_2)\} \quad (8)$$

is a hybrid simulation relation of  $S_1$  by  $S_2$  if and only if the following properties hold:

- (i)  $Q_S$  is a simulation relation of  $D_{S_1}$  by  $D_{S_2}$  where  $D_{S_i}$  are the LTS's associated to  $S_i, i = 1, 2$ , and for every  $(q_1, q_2) \in Q_S$ ,  $\mathcal{S}(q_1, q_2)$  is a simulation relation of  $\Sigma_1(q_1)$  by  $\Sigma_2(q_2)$ ;
- (ii) for every  $(q_1, q_2) \in Q_S$  and every possible set of successor states  $(q'_1, q'_2) \in Q_S$  such that  $(q_1, v, q'_1) \in E_1$  and  $(q_2, v, q'_2) \in E_2$ ,

$$\text{diag}\{M_1(e_1), M_2(e_2)\}\mathcal{S}(q_1, q_2) \subset \mathcal{S}(q'_1, q'_2)$$

**Proof.** ( $\implies$ ):

Assume  $Q_S$  is not a simulation relation of  $D_{S_1}$  by  $D_{S_2}$  and there exists at least one pair  $(q_1, q_2) \in Q_S$  such that there does not exist a simulation relation of  $\Sigma(q_1)$  by  $\Sigma(q_2)$ . Then for some joint input function  $u_1 = u_2 = u$  and a joint hybrid time basis  $T_1 = T_2 = T$ , one can find a hybrid execution  $\xi_1 = (\xi_1^0, T_1, u, y_1, v, \xi_1)$  such that for any execution  $\xi_2 = (\xi_2^0, T, u, y_2, v, \xi_2)$  there exists a  $j \in \{0, 1, \dots, J\}$  and a  $v \in V$  for which  $(q_1(j), v(j+1), q_1(j+1)) \in E_1$  but there does not exist a  $q_2(j+1)$  such that  $(q_2(j), v(j+1), q_2(j+1)) \in E_2$ .

( $\impliedby$ ):

Due to Theorem 18 (i), the set  $Q_S$  is a simulation relation of  $D_{S_1}$  by  $D_{S_2}$  and for every  $(q_1, q_2) \in Q_S$ ,  $\mathcal{S}(q_1, q_2)$  is a simulation relation of  $\Sigma(q_1)$  by  $\Sigma(q_2)$ . By the respective definitions of simulation relations for LTS and LTI systems, Theorem 18 (i) therefore guarantees that for any hybrid execution  $\xi_1$ , there exists a hybrid execution  $\xi_2$  ( $\xi_2$ ) such that Definition 14 (i) holds. Furthermore, Theorem 18 (ii) ensures that for every transition  $j \in J$ , the reset of the continuous state remains within the simulation subspace  $\mathcal{S}(q_1(j+1), q_2(j+1))$  associated with the new location  $(q_1(j+1), q_2(j+1))$ . Combining the two conditions, one obtains the statement (ii) of Definition 14.

## 5. COMPOSITIONAL AND ASSUME GUARANTEE REASONING

Knowing that invariance under composition holds on the level of both the discrete and continuous dynamics, we attempt to establish a similar result for SLS.

*Theorem 19.* (Invariance under composition for SLS)

For any four given SLS's  $S_i, i \in \{P_1, P_2, Q_1, Q_2\}$ , such that  $V_{P_1} = V_{Q_1}, V_{P_2} = V_{Q_2}$  and interconnections  $\|_{\text{SLS}}$ , hybrid simulation fulfils rule 1.

**Proof.** Assume we are given hybrid simulation relations  $\mathcal{R}_1$  and  $\mathcal{R}_2$  of  $S_{P_1}$  by  $S_{Q_1}$  and  $S_{P_2}$  by  $S_{Q_2}$ , respectively. Define the relation

$$\mathcal{R} := \{((\xi_{P_1}, \xi_{P_2}), (\xi_{Q_1}, \xi_{Q_2})) \mid (\xi_{P_1}, \xi_{Q_1}) \in \mathcal{R}_1, (\xi_{P_2}, \xi_{Q_2}) \in \mathcal{R}_2\} \quad (9)$$

Reordering the components, one obtains

$$\tilde{\mathcal{R}} = \{((\xi_{P_1}, \xi_{Q_1}), (\xi_{P_2}, \xi_{Q_2})) \mid ((\xi_{P_1}, \xi_{P_2}), (\xi_{Q_1}, \xi_{Q_2})) \in \mathcal{R}\} = \mathcal{R}_1 \times \mathcal{R}_2 \quad (10)$$

From Theorems 6 and 11, we know that the associated LTS's  $D_i, i \in \{P_1, P_2, Q_1, Q_2\}$ , as well as the respective LTI systems at every location  $((p_1, p_2), (q_1, q_2)) \in Q_{\mathcal{R}}$  are invariant under composition so that condition (i) in Theorem 18 is fulfilled.

Since  $\mathcal{R}_1, \mathcal{R}_2$  are hybrid simulation relations, it holds for every  $(p_1, q_1) \in Q_{\mathcal{R}_1}$  and every possible successor state  $(p'_1, q'_1) \in Q_{\mathcal{R}_1}$  that

$$\begin{bmatrix} M_{P_1}(e_{P_1}) & 0 \\ 0 & M_{Q_1}(e_{Q_1}) \end{bmatrix} \mathcal{R}_1(p_1, q_1) \subset \mathcal{R}_1(p'_1, q'_1) \quad (11)$$

with  $e_{P_1} = (p_1, v, p'_1) \in E_{P_1}$  and  $e_{Q_1} = (q_1, v, q'_1) \in E_{Q_1}$  for some  $v \in V_{P_1}$ . Similarly, for every  $(p_2, q_2) \in Q_{\mathcal{R}_2}$  and every successor state  $(p'_2, q'_2) \in Q_{\mathcal{R}_2}$  such that  $e_{P_2} = (p_2, v, p'_2) \in E_{P_2}$  and  $e_{Q_2} = (q_2, v, q'_2) \in E_{Q_2}$  for some  $v \in V_{P_2}$  the following holds:

$$\begin{bmatrix} M_{P_2}(e_{P_2}) & 0 \\ 0 & M_{Q_2}(e_{Q_2}) \end{bmatrix} \mathcal{R}_2(p_2, q_2) \subset \mathcal{R}_2(p'_2, q'_2) \quad (12)$$

Depending on the discrete transition label  $v \in V = V_{P_1} \cup V_{P_2} = V_{Q_1} \cup V_{Q_2}$ , three cases have to be distinguished:

- (1)  $v \in V_{P_1} \cap V_{P_2}$ :  $((p_1, p_2), v, (p'_1, p'_2)) \in E_{P_1 P_2}$  implies  $((q_1, q_2), v, (q'_1, q'_2)) \in E_{Q_1 Q_2}$  and therefore  $(p'_1, q'_1, p'_2, q'_2) \in Q_{\tilde{\mathcal{R}}}$ . From (11) and (12) it follows that  $\text{diag}\{M_{P_1}(e_{P_1 P_2}), M_{Q_1}(e_{Q_1 Q_2}), M_{P_2}(e_{P_1 P_2}), M_{Q_2}(e_{Q_1 Q_2})\}\tilde{\mathcal{R}}(p_1, q_1, p_2, q_2) \subset \tilde{\mathcal{R}}(p'_1, q'_1, p'_2, q'_2)$
- (2)  $v \in V_{P_1} \setminus V_{P_2}$ : Here,  $((p_1, p_2), v, (p'_1, p_2)) \in E_{P_1 P_2}$  implies  $((q_1, q_2), v, (q'_1, q_2)) \in E_{Q_1 Q_2}$  and therefore  $(p'_1, q'_1, p_2, q_2) \in Q_{\tilde{\mathcal{R}}}$ . Thus,  $\text{diag}\{M_{P_1}(e_{P_1 P_2}), M_{Q_1}(e_{Q_1 Q_2}), I, I\}\tilde{\mathcal{R}}(p_1, q_1, p_2, q_2) \subset \tilde{\mathcal{R}}(p'_1, q'_1, p_2, q_2)$
- (3)  $v \in V_{P_1} \setminus V_{P_2}$ : This case is symmetrical to (2).

We can therefore conclude that for every  $(p_1, p_2, q_1, q_2) \in Q_{\tilde{\mathcal{R}}}$  and every possible successor state  $(p'_1, q'_1, p'_2, q'_2) \in Q_{\tilde{\mathcal{R}}}$

$$\text{diag}\{\bar{M}_{P_1}(e_{P_1 P_2}), \bar{M}_{Q_1}(e_{Q_1 Q_2}), \bar{M}_{P_2}(e_{P_1 P_2}), \bar{M}_{Q_2}(e_{Q_2})\} \tilde{\mathcal{R}}(p_1, q_1, p_2, q_2) \subset \tilde{\mathcal{R}}(p'_1, q'_1, p'_2, q'_2)$$

where  $e_{P_1 P_2} = ((p_1, p_2), v, (p'_1, p'_2)) \in E_{P_1 P_2}$  and  $e_{Q_1 Q_2} = ((q_1, q_2), v, (q'_1, q'_2)) \in E_{Q_1 Q_2}$ . Reordering the components,  $\tilde{\mathcal{R}}$  as defined in (9) indeed defines a structural hybrid simulation relation of  $S_{P_1} \|_{\text{SLS}} S_{P_2}$  by  $S_{Q_1} \|_{\text{SLS}} S_{Q_2}$ .

*Theorem 20.* (Soundness of the non-circular AGR rule)  
Consider SLS's  $S_i, i \in \{P_1, P_2, Q_1, Q_2\}$  such that  $V_{P_1} = V_{Q_1}, V_{P_2} = V_{Q_2}$  and their interconnections  $\|_{\text{SLS}}$ . The non-circular AGR rule 2 is sound with respect to hybrid simulation.

**Proof.** Theorem 19 ensures that hybrid simulation is invariant under compositions  $\|_{\text{SLS}}$ . Together with the

transitivity property of hybrid simulation (cf. Proposition 15), one can easily deduce (C1).

It cannot be expected that the circular AGR rule 3 is unconditionally sound. From Theorem 7 it is known that already on the level of the discrete dynamics, an additional AGR condition is needed. Using the notion of structural simulation relations, it can be shown that (2) is necessary and sufficient for the soundness of rule 3 when considering SLS's.

*Theorem 21.* (Soundness of the circular AGR rule)

Consider any given SLS  $S_i, i \in \{P_1, P_2, Q_1, Q_2\}$ , such that  $V_{P_1} = V_{Q_1}, V_{P_2} = V_{Q_2}$  and their interconnections  $\|_{\text{SLS}}$ . Then the circular AGR rule 3 is sound if and only if the AGR-condition (2) for the associated LTS's holds.

**Proof.** Assume we are given hybrid simulation relations  $\mathcal{R}_1$  and  $\mathcal{R}_2$  of  $S_{P_1} \|_{\text{SLS}} S_{Q_2}$  and  $S_{Q_1} \|_{\text{SLS}} S_{P_2}$  by  $S_{Q_1} \|_{\text{SLS}} S_{Q_2}$ , respectively. Construct a relation

$$\mathcal{R} := \left\{ (\xi_{P_1}, \xi_{P_2}, \xi_{Q_1}, \xi_{Q_2}) \mid \exists \hat{\xi}_{Q_1}, \hat{\xi}_{Q_2} : \right. \quad (13)$$

$$\left. (\xi_{P_1}, \xi_{Q_2}, \xi_{Q_1}, \hat{\xi}_{Q_2}) \in \mathcal{R}_1, (\xi_{Q_1}, \xi_{P_2}, \hat{\xi}_{Q_1}, \xi_{Q_2}) \in \mathcal{R}_2 \right\}$$

We claim that  $\mathcal{R}$  is a hybrid simulation relation of  $S_{P_1} \|_{\text{SLS}} S_{P_2}$  by  $S_{Q_1} \|_{\text{SLS}} S_{Q_2}$ . From Theorem 7, we know that the associated LTS's fulfil the circular AGR rule (i) if and only if the AGR-condition (2) holds. Furthermore, for the respective LTI systems at every location  $(p_1, p_2, q_1, q_2) \in Q_{\mathcal{R}}$ , the circular AGR rule is also sound as stated in Theorem 12. Thus, condition (i) in Theorem 18 is readily fulfilled.

Now take for any  $(p_1, p_2, q_1, q_2) \in Q_{\mathcal{R}}$  an arbitrary element  $(x_{P_1}, x_{P_2}, x_{Q_1}, x_{Q_2}) \in Q_{\mathcal{R}}(p_1, p_2, q_1, q_2)$ . Define first for every location  $(p_1, p_2, q_1, q_2) \in Q_{\mathcal{R}}$  the subspaces

$$Q_T(q_1, q_2) := \{ (x_{Q_1}, x_{Q_2}) \mid \exists x_{P_1}, \bar{x}_{Q_2}, x_{P_2}, \bar{x}_{Q_1} :$$

$$(x_{P_1}, x_{Q_2}, x_{Q_1}, \bar{x}_{Q_2}) \in Q_{\mathcal{R}_1}(p_1, p_2, q_1, \bar{q}_2),$$

$$(x_{Q_1}, x_{P_2}, \bar{x}_{Q_1}, x_{Q_2}) \in Q_{\mathcal{R}_2}(q_1, p_2, \bar{q}_1, q_2) \}$$

$$Q_1(p_1) := \{ x_{P_1} \mid \exists x_{P_2}, x_{Q_1}, x_{Q_2} :$$

$$(x_{P_1}, x_{P_2}, x_{Q_1}, x_{Q_2}) \in Q_{\mathcal{R}}(p_1, p_2, q_1, q_2) \}$$

$$Q_2(p_2) := \{ x_{P_2} \mid \exists x_{P_1}, x_{Q_1}, x_{Q_2} :$$

$$(x_{P_1}, x_{P_2}, x_{Q_1}, x_{Q_2}) \in Q_{\mathcal{R}}(p_1, p_2, q_1, q_2) \}$$

Since  $\mathcal{R}_1$  and  $\mathcal{R}_2$  are simulation relations, they fulfil condition (ii) in Theorem 18 so that for every  $(p_1, p_2, q_1, \hat{q}_2) \in Q_{\mathcal{R}_1}$  and every possible successor state  $(p'_1, q'_2, q'_1, \hat{q}'_2) \in Q_{\mathcal{R}_1}$

$$\text{diag}\{\bar{M}_{P_1}(e_{P_1 Q_2}), \bar{M}_{Q_2}(e_{P_1 Q_2}), \bar{M}_{Q_1}(e_{Q_1 Q_2}), \bar{M}_{Q_2}(e_{Q_1 Q_2})\}$$

$$\mathcal{R}_1(p_1, p_2, q_1, \hat{q}_2) \subset \mathcal{R}_1(p'_1, q'_2, q'_1, \hat{q}'_2)$$

and similarly for every  $(q_1, p_2, \hat{q}_1, q_2) \in Q_{\mathcal{R}_2}$  and every possible successor state  $(q'_1, p'_2, \hat{q}'_1, q'_2) \in Q_{\mathcal{R}_2}$

$$\text{diag}\{\bar{M}_{Q_1}(e_{Q_1 P_2}), \bar{M}_{P_2}(e_{Q_1 P_2}), \bar{M}_{Q_1}(e_{Q_1 Q_2}), \bar{M}_{Q_2}(e_{Q_1 Q_2})\}$$

$$\mathcal{R}_2(q_1, p_2, \hat{q}_1, q_2) \subset \mathcal{R}_2(q'_1, p'_2, \hat{q}'_1, q'_2)$$

It therefore holds for every  $(p_1, p_2, q_1, q_2) \in Q_{\mathcal{R}}$  and every possible discrete successor state  $(p'_1, p'_2, q'_1, q'_2) \in Q_{\mathcal{R}}$  that

$$\begin{bmatrix} \bar{M}_{Q_1}(e_{Q_1 Q_2}) & 0 \\ 0 & \bar{M}_{Q_2}(e_{Q_1 Q_2}) \end{bmatrix} Q_T(q_1, q_2) \subset Q_T(q'_1, q'_2)$$

and similarly

$$\bar{M}_{P_1}(e_{P_1 Q_2}) Q_1(p_1) \subset Q_1(p'_1), \bar{M}_{P_2}(e_{Q_1 P_2}) Q_2(p_2) \subset Q_2(p'_2),$$

Thus, condition (ii) is fulfilled which proves that  $\mathcal{R}$  as in (13) is indeed a hybrid simulation relation of  $S_{P_1} \|_{\text{SLS}} S_{P_2}$  by  $S_{Q_1} \|_{\text{SLS}} S_{Q_2}$ .

## 6. OUTLOOK

In this paper we started to develop a methodology of compositional and assume guarantee reasoning for switching linear systems. The key principle was to exploit the hierarchical structure of the class of systems under consideration which is expressed by the notion of structural hybrid simulation relations. Thus, we proved that SLS's are invariant under composition with respect to hybrid simulation and fulfil both the circular and non-circular AGR rules 2 and 3.

The class of hybrid systems includes a much larger variety of systems than the ones considered here. Particularly on the level of the continuous dynamics, one could think of different representations such as non-deterministic LTI systems. Furthermore, it would be of interest to study switching linear systems with invariance and guard conditions. Also the extension to nonlinear systems is within reach.

## REFERENCES

- Alur, R., Henzinger, T.A., Lafferriere, G., and Pappas, G.J. (2000). Discrete abstractions of hybrid systems. *Proceedings of the IEEE*, 88, 971–984.
- Clarke, E.M., Grumberg, O., and Peled, D.A. (1999). *Model checking*. The MIT Press, Cambridge.
- Frehse, G. (2005). *Compositional Verification of Hybrid Systems using Simulation Relations*. Ph.D. thesis, Radboud Universiteit Nijmegen.
- Henzinger, T.A., Minea, M., and Prabhu, V. (2001). Assume-guarantee reasoning for hierarchical hybrid systems. In *HSCC 2001*, 275 – 290.
- Kerber, F. and van der Schaft, A.J. (2008). Assume-guarantee reasoning for linear dynamical systems. Submitted to ECC 2009.
- Lygeros, J., Tomlin, C., and Sastry, S. (1999). Controllers for reachability specifications for hybrid systems. *Automatica*, 35, 149–370.
- Milner, R. (1989). *Communication and Concurrency*. Prentice Hall.
- Misra, J. and Chandy, K.M. (1981). Proofs of networks of processes. *IEEE Trans. Softw. Eng.*, 7(4), 417–426.
- Pappas, G.J., Lafferriere, G., and Sastry, S. (2000). Hierarchically consistent control systems. *IEEE Transactions on Automatic Control*, 45(6), 1144–1160.
- Pola, G., van der Schaft, A.J., and Benedetto, M.D.D. (2006). Equivalence of switching linear systems by bisimulation. *International Journal of Control*, 79(1), 74 – 92.
- van der Schaft, A.J. (2004a). Equivalence of dynamical systems by bisimulation. *IEEE Transactions on Automatic Control*, 49(12), 2160–2172.

- van der Schaft, A.J. (2004b). Equivalence of hybrid dynamical systems. In *Proceedings of the Mathematical Theory of Networks and Systems*.
- van der Schaft, A.J. and Schumacher, H. (2001). *An Introduction to Hybrid Dynamical Systems*. Springer-Verlag, London.