

Assume-guarantee reasoning for linear dynamical systems

Florian Kerber, Arjan van der Schaft

University of Groningen

Institute for Mathematics and Computing Science

Postbus 407

9700 AV Groningen

Phone: +31(0)50 363 3972

email: {F.J.Kerber, A.J.van.der.Schaft}@rug.nl

Abstract— The notion of simulation relation has been adopted from theoretical computing science to control theory to reduce the complexity arising in modeling physical processes. Simulations can serve as an abstraction of a given system behavior whilst preserving the input-output structure. We intend to apply simulation relations to develop a framework for compositional and assume-guarantee reasoning for linear dynamical systems. The underlying idea is to use information about the relation of components or subsystems to abstract the behavior of interconnected systems. The interconnection structure is hereby defined by two types of negative feedback.

I. INTRODUCTION

Models of engineering systems become increasingly complex and therefore difficult to analyze. The complexity arises from the interaction of different components or subsystems which are embedded in the model of the whole process. In the theory of concurrent processes, abstraction concepts have been developed to deal with large scale models. An important method in this context is the notion of simulation relations (or, as a two sided version, bisimulation relations) introduced by [5]. The idea of abstracting a given system by a lower dimensional and therefore less complex one has since been applied successfully in the area of systems and control by several authors, see [1], [7] and [9]. Simulation relations between linear systems can be analyzed with tools from geometric control theory. This resulted in linear algebraic existence conditions and efficient algorithms to compute maximal simulation relations.

The assume guarantee reasoning (AGR) paradigm also originates from theoretical computer science, see e. g. [6] and [8]. More recently, applications in automata theory ([4]) and special classes of hybrid systems with dominating discrete dynamics, e.g. [2] and [3] have proven the significance of this concept. The basic principle is to make assumptions on the behavior of individual components of an interconnection as to how the components interact with their environment in order to prove properties of the structure as a whole. In the AGR literature, one distinguishes between circular and non-circular proof rules. Here, circularity means that assumptions of one antecedent are based on to be proven properties or guarantees of another antecedent. To insure correctness of circular rules, additional conditions are usually required. In contrast, non-circular rules are usually sound without imposing further conditions, but generally have to

assume universal properties of individual components which might not be easy to verify in practice.

In this paper, we want to combine the above analysis techniques to develop a theory of compositional and assume guarantee reasoning for linear feedback control systems based on simulation relations. First, we summarize the theory of simulation relations for linear continuous-time systems and define the notions of interconnection used in the following. Based on this theoretical framework, we show that modularity is a key property in the compositional analysis of linear feedback systems. In the last part, AGR proof rules, both circular and non circular, are investigated for linear feedback systems.

II. THEORETICAL BACKGROUND

Consider linear continuous-time systems of the form

$$\begin{aligned}\Sigma_i : \quad \dot{x}_i &= A_i x_i + B_i u_i + G_i d_i, \\ y_i &= C_i x_i,\end{aligned}\tag{1}$$

where u_i represents a control input, d_i a disturbance input and $x_i \in \mathcal{X}_i, u_i \in \mathcal{U}_i, d_i \in \mathcal{D}_i, y_i \in \mathcal{Y}_i$ are all taken from vector spaces of appropriate dimensions. External disturbance inputs are introduced in analogy to both the theory of concurrent processes and the concept of abstractions of dynamical systems as developed in [7]. We call systems on which external disturbances act *non-deterministic* systems in contrast to *deterministic* systems where $d_i \equiv 0$.

Due to the complexity of physical processes it is common practice to subdivide a given structure into sub-models which – when connected in the correct manner – represent a model of the process as a whole. Similarly, from a control perspective, combining models of the plant and the controller yields a model of the controlled system. Assuming all these subsystems are of the class of systems (1), we are therefore interested in interconnections of linear dynamical systems, denoted by $\Sigma_1 \parallel \Sigma_2$. More precisely, we restrict ourselves to two different kinds of negative feedback interconnection. On the one hand, direct interconnection of the form $u_1 = -y_2$,

$y_1 = u_2$, denoted by $\|_c$, yields the combined system

$$\begin{aligned} \Sigma_1 \|_c \Sigma_2 : \begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} &= \begin{bmatrix} A_1 & -B_1 C_2 \\ B_2 C_1 & A_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \end{bmatrix} \\ \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} &= \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \\ u_1 &= -y_2, \quad u_2 = y_1 \\ &\text{("closed feedback interconnection")} \end{aligned} \quad (2)$$

On the other hand, the feedback interconnection might involve external signals such as measurement noise or reference signals which act as new inputs on the closed loop system. Such an interconnection will be denoted by $\|_o$ and results in the following dynamics

$$\begin{aligned} \Sigma_1 \|_o \Sigma_2 : \begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} &= \begin{bmatrix} A_1 & -B_1 C_2 \\ B_2 C_1 & A_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} B_1 & 0 \\ 0 & B_2 \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \end{bmatrix} + \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \end{bmatrix} \\ \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} &= \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \\ u_1 &= -y_2 + e_1, \quad u_2 = y_1 + e_2 \\ &\text{("open feedback interconnection")} \end{aligned} \quad (3)$$

Despite being so closely related, distinguishing between these two types of feedback interconnection will indeed make a difference for compositional reasoning as will be shown in the remainder. Whenever $\|$ is used unspecified it represents both open and closed feedback interconnection.

The relation \preccurlyeq denotes simulation as defined in [9, Definition 5.1].

Definition 1: Given two systems $\Sigma_i, i = 1, 2$ as in (1). A simulation relation S of Σ_1 by Σ_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 $(x_{10}, x_{20}) \in S$, any joint input function $u_1(\cdot) = u_2(\cdot)$ and any disturbance function $d_1(\cdot)$ there should exist a disturbance function $d_2(\cdot)$ such that the resulting state trajectories $x_i(\cdot), i = 1, 2$ with $x_i(0) = x_{i0}$ satisfy

$$\begin{aligned} (i) : \quad &(x_1(t), x_2(t)) \in S \quad \forall t \geq 0 \\ (ii) : \quad &C_1 x_1(t) = C_2 x_2(t) \quad \forall t \geq 0 \end{aligned} \quad (4)$$

Furthermore, Σ_1 is **simulated** by Σ_2 , denoted $\Sigma_1 \preccurlyeq \Sigma_2$, if there exists a simulation relation $S \subset \mathcal{X}_1 \times \mathcal{X}_2$ fulfilling $\Pi_{\mathcal{X}_1} S = \mathcal{X}_1$ with $\Pi_{\mathcal{X}_1} : \mathcal{X}_1 \times \mathcal{X}_2 \rightarrow \mathcal{X}_1$ the canonical projection from $\mathcal{X}_1 \times \mathcal{X}_2$ to \mathcal{X}_1 . In this case, S is called a **full simulation relation**.

Remark 1: In this definition as for the remainder, we shall denote an element of the cartesian product space $\mathcal{X}_1 \times \mathcal{X}_2$ both by (x_1, x_2) and $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, x_1 \in \mathcal{X}_1, x_2 \in \mathcal{X}_2$.

Due to the similarity with the disturbance decoupling problem, the subspace properties of a simulation relation S can be described as follows:

Theorem 1 (c. f. Proposition 5.2 in [9]): A linear subspace $S \subset \mathcal{X}_1 \times \mathcal{X}_2$ is a simulation relation of Σ_1 by Σ_2 if and only if

$$(i) : \quad S + \text{im} \begin{bmatrix} G_1 \\ 0 \end{bmatrix} \subset S + \text{im} \begin{bmatrix} 0 \\ G_2 \end{bmatrix} \quad (5)$$

$$(ii) : \quad \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix} S \subset S + \text{im} \begin{bmatrix} 0 \\ G_2 \end{bmatrix}$$

$$(iii) : \quad \text{im} \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} \subset S + \text{im} \begin{bmatrix} 0 \\ G_2 \end{bmatrix}$$

$$(iv) : \quad S \subset \ker \begin{bmatrix} C_1 & -C_2 \end{bmatrix}$$

Analogously to [9, Proposition 2.9] an alternative characterization for a subspace to be a simulation relation can be given.

Theorem 2: A linear subspace $S \subset \mathcal{X}_1 \times \mathcal{X}_2$ is a simulation relation of Σ_1 by Σ_2 if and only if for all $(x_1, x_2) \in S$, for all $u_1 = u_2 = u$ and all d_1 there exists a d_2 such that

$$(i) : \quad \begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} A_1 x_1 + B_1 u + G_1 d_1 \\ A_2 x_2 + B_2 u + G_2 d_2 \end{bmatrix} \in S \quad (6)$$

$$(ii) : \quad C_1 x_1 = C_2 x_2$$

We also state results for deterministic systems, i.e. systems without external disturbances $d_i \equiv 0$, from [9].

Theorem 3: Given deterministic systems $\Sigma_i, i = 1, 2$. Then there exists a simulation relation of Σ_1 by Σ_2 if and only if the Markov parameters of Σ_1 and Σ_2 are equal, i.e.

$$C_1 A_1^k B_1 = C_2 A_2^k B_2, \quad k = 0, 1, 2, \dots, \quad (7)$$

or, equivalently, if and only if the transfer functions are the same, i.e. $G_1(s) = G_2(s)$.

An important statement about maximal simulation relations is given in the following theorem.

Theorem 4: Consider two deterministic systems $\Sigma_i, i = 1, 2$ with the same transfer function $G_1(s) = G_2(s)$. The maximal simulation relation S^{\max} of Σ_1 by Σ_2 is the unobservability space of the augmented system,

$$S^{\max} = \ker \begin{bmatrix} C_1 & -C_2 \\ C_1 A_1 & -C_2 A_2 \\ \vdots & \vdots \\ C_1 A_1^{n-1} & -C_2 A_2^{n-1} \end{bmatrix} \quad (8)$$

while $\text{im} \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} \subset S^{\max}$ and $n = \max\{n_1, n_2\}, n_i = \dim\{\mathcal{X}_i\}$.

In [2], it is shown that simulation relations for labeled transition systems (LTS), called Σ -simulation there, are modular with respect to the compositional operator representing parallel composition. Modularity is a desired property in compositional analysis, for instance it can be used to prove the correctness of circular assume-guarantee rules. In order to do so, we first recall some characteristics of simulation relations as given in [9].

Theorem 5: Simulation for linear continuous-time systems is a preorder, i.e., it is reflexive and transitive.

Proof: Given the systems $\Sigma_i, i = 1, 2, 3$.

Clearly, $S_{id} := \{(x_1, x_1) \mid x_1 \in \Sigma_1\}$ is a simulation relation

of Σ_1 by itself.

Moreover, given simulation relations $S_{12} \subset \mathcal{X}_1 \times \mathcal{X}_2$ and $S_{23} \subset \mathcal{X}_2 \times \mathcal{X}_3$ of Σ_1 by Σ_2 and of Σ_2 by Σ_3 , respectively, define

$$S_{13} := \{(x_1, x_3) \mid \exists x_2 \in \Sigma_2 : (x_1, x_2) \in S_{12}, (x_2, x_3) \in S_{23}\}$$

Choosing $\hat{x}_2 = A_2x_2 + B_2u + G_2d$, one indeed finds that $(\hat{x}_1, \hat{x}_2) \in S_{12}$ and $(\hat{x}_2, \hat{x}_3) \in S_{23}$ which proves the claim. ■

An important difference to Σ -simulation for LTS is expressed in the following

Proposition 1: For any two dynamical systems Σ_1 and Σ_2 (1), simulation is not commutative with respect to feedback interconnections,

$$\Sigma_1 \parallel \Sigma_2 \not\preceq \Sigma_2 \parallel \Sigma_1 \quad (9)$$

Proof: To illustrate this with an counterexample, consider the two systems

$$\begin{aligned} \Sigma_1 : \quad \dot{x}_1 &= x_1 + u_1 & \Sigma_2 : \quad \dot{x}_2 &= 2x_2 + u_2 \\ y_1 &= x_1 & y_2 &= x_2 \end{aligned} \quad (10)$$

The transfer functions of the interconnections are then given by

$$\begin{aligned} G_{\Sigma_1 \parallel \Sigma_2} &= \begin{bmatrix} g_1(s) & -g_2(s) \\ g_3(s) & g_4(s) \end{bmatrix} \\ G_{\Sigma_2 \parallel \Sigma_1} &= \begin{bmatrix} g_4(s) & -g_3(s) \\ g_2(s) & g_1(s) \end{bmatrix} \end{aligned} \quad (11)$$

Even after reordering the state components, the transfer functions do not match which by Theorem 3 implies that there does not exist a simulation relation of $\Sigma_1 \parallel \Sigma_2$ by $\Sigma_2 \parallel \Sigma_1$ nor, in fact, vice versa. ■

Remark 2: Whether or not simulation relation is commutative depends heavily on the type of interconnection. Parallel composition of LTS can be thought of as restricting the dynamics of the interconnection to the intersection of the dynamics of the individual components. For linear feedback systems, the interconnection via negative feedback brakes the symmetry of the closed loop system. Choosing positive feedback instead would have preserved commutativity of the interconnection.

III. COMPOSITIONAL REASONING

Definition 2: A preorder \preceq is called **compositional** with respect to an interconnection operator \parallel if

$$\begin{aligned} \Sigma_{P_1} \preceq \Sigma_{Q_1} \quad \wedge \quad \Sigma_{P_2} \preceq \Sigma_{Q_2} \\ \implies \Sigma_{P_1} \parallel \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel \Sigma_{Q_2} \end{aligned} \quad (12)$$

and **invariant under composition** or a **precongruence** if

$$\Sigma_{P_1} \preceq \Sigma_{Q_1} \implies \Sigma_{P_1} \parallel \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel \Sigma_{P_2} \quad \text{for all } \Sigma_{P_2} \quad (13)$$

If a preorder fulfils both properties (12) and (13), it is called **modular**.

Proposition 2: Simulation is both compositional and invariant under composition with respect to feedback interconnection of linear continuous-time systems.

Proof: Given the linear dynamical systems $\Sigma_i, i \in \{P_1, P_2, Q_1, Q_2\}$.

We will prove the Proposition for open feedback interconnection \parallel_o thus implying the proof for \parallel_c where $e_i \equiv 0$.

compositionality: Assume there exists a simulation relation $S \subset \mathcal{X}_{P_1} \times \mathcal{X}_{Q_1}$ of Σ_{P_1} by Σ_{Q_1} , $\Sigma_{P_1} \preceq \Sigma_{Q_1}$. It has to be shown that there exists a simulation relation $R \subset \mathcal{X}_{P_1} \times \mathcal{X}_{P_2} \times \mathcal{X}_{Q_1} \times \mathcal{X}_{Q_2}$ of $\Sigma_{P_1} \parallel \Sigma_{P_2}$ by $\Sigma_{Q_1} \parallel \Sigma_{Q_2}$ for any system Σ_{P_2} .

Due to Theorem 2, for every $(x_{P_1}, x_{P_2}) \in S$, for any $u_1 = u_2 = u$ and any d_1 there exists a d_2 such that

$$\begin{aligned} (i) : \quad & \begin{bmatrix} A_{P_1}x_{P_1} + B_{P_1}u + G_{P_1}d_1 \\ A_{Q_1}x_{Q_1} + B_{Q_1}u + G_{Q_1}d_2 \end{bmatrix} \in S \\ (ii) : \quad & C_{P_1}x_{P_1} = C_{Q_1}x_{Q_1} \end{aligned} \quad (14)$$

Let's consider the relation $R := \{(\mathbf{x} = (x_{P_1}, x_{P_2}), (x_{Q_1}, x_{Q_2})) \mid (x_{P_1}, x_{Q_1}) \in S\}$. Take

any $\mathbf{x} \in R$, any $\mathbf{e} = \begin{bmatrix} e_1 \\ e_2 \end{bmatrix}$ and any $\mathbf{d}_1 = \begin{bmatrix} d_1^1 \\ d_1^2 \end{bmatrix}$. According to Eq. (14), for a given $(x_{P_1}, x_{Q_1}) \in S$, any $u = e_1 - C_{P_2}x_{P_2}$ and every $d_1 = d_1^1$ there exists a d_2 such that $(\hat{x}_{P_1}, \hat{x}_{Q_1}) \in S$. Thus, setting $\mathbf{d}_2 = \begin{bmatrix} d_2 \\ d_1^2 \end{bmatrix}$ yields $((\hat{x}_{P_1}, \hat{x}_{P_2}), (\hat{x}_{Q_1}, \hat{x}_{Q_2})) \in R$ since $(\hat{x}_{P_1}, \hat{x}_{Q_1}) \in S$ and $\hat{x}_{P_2} = \hat{x}'_{P_2}$.

invariance under composition: Assume we are given both a simulation relation $S_1 \subset \mathcal{X}_{P_1} \times \mathcal{X}_{Q_1}$ of Σ_{P_1} by Σ_{Q_1} and $S_2 \subset \mathcal{X}_{P_2} \times \mathcal{X}_{Q_2}$ of Σ_{P_2} by Σ_{Q_2} . Define the subspace

$$S := \{(x_{P_1}, x_{P_2}, x_{Q_1}, x_{Q_2}) \mid (x_{P_1}, x_{Q_1}) \in S_1, (x_{P_2}, x_{Q_2}) \in S_2\} \quad (15)$$

Again, the proof uses Theorem 2. Take any element $\mathbf{x} = (x_{P_1}, x_{P_2}, x_{Q_1}, x_{Q_2}) \in S$, any $\mathbf{e} = \begin{bmatrix} e_1 \\ e_2 \end{bmatrix}$ and $\mathbf{d}_1 = \begin{bmatrix} d_1^1 \\ d_1^2 \end{bmatrix}$. Since $(x_{P_1}, x_{Q_1}) \in S_1$ it follows that $C_{P_1}x_{P_1} = C_{Q_1}x_{Q_1}$ and similarly from S_2 that $C_{Q_2}x_{Q_2} = C_{P_2}x_{P_2}$. Moreover, for every u_1 and d_1 there exists a d_2 such that $(A_{P_1}x_{P_1} + B_{P_1}u_1 + G_{P_1}d_1, A_{Q_1}x_{Q_1} + B_{Q_1}u_1 + G_{Q_1}d_2) \in S_1$. Similarly, for every u_2 and d_3 there exists a d_4 such that $(A_{P_2}x_{P_2} + B_{P_2}u_2 + G_{P_2}d_3, A_{Q_2}x_{Q_2} + B_{Q_2}u_2 + G_{Q_2}d_4) \in S_2$. Setting $e_1 = u_1 + B_{P_2}x_{P_2}$, $e_2 = u_2 + B_{P_1}x_{P_1}$, $d_1^1 = d_1$, $d_1^2 = d_3$, $d_2^1 = d_2$, $d_2^2 = d_4$, it follows that indeed $(\hat{x}_{P_1}, \hat{x}_{P_2}, \hat{x}_{Q_1}, \hat{x}_{Q_2}) \in S$. ■

Remark 3: Even though in this framework simulation is not commutative with respect to feedback interconnection, nevertheless the modularity properties of compositionality and invariance under composition hold. Commutativity of the simulation preorder would have simplified the proof obligation since in that case, invariance under composition is equivalent to compositionality, c.f. [2, Proposition 3.7.].

Based on assumed properties of individual system components such as $\Sigma_{P_i} \preceq \Sigma_{Q_i}$, compositionality allows to draw conclusions about interconnections of components. For the open type of interconnections of linear continuous-time systems it will be shown that also the converse is true.

Proposition 3: For linear dynamical systems (1) interconnected by open negative feedback (3), the following equivalence holds with respect to simulation relations \preceq :

$$\begin{aligned} \Sigma_{P_1} \preceq \Sigma_{Q_1} \wedge \Sigma_{P_2} \preceq \Sigma_{Q_2} & \quad (16) \\ \iff \\ \Sigma_{P_1} \parallel_o \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel_o \Sigma_{Q_2} \end{aligned}$$

Proof:

“ \implies ”: This holds because of Proposition 2.

“ \impliedby ”: Let a simulation relation S of $\Sigma_{P_1} \parallel \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel \Sigma_{Q_2}$ be given, i.e. for any $\mathbf{x} \in S$, any $\mathbf{e} = \begin{bmatrix} e_1 \\ e_2 \end{bmatrix}$ and $\mathbf{d}_1 =$

$$\begin{aligned} \begin{bmatrix} d_1^1 \\ d_1^2 \end{bmatrix} \text{ there exists a } \mathbf{d}_2 = \begin{bmatrix} d_2^1 \\ d_2^2 \end{bmatrix} \text{ such that} \\ (i) : \begin{bmatrix} A_{P_1}x_{P_1} + B_{P_1}(e_1 - C_{P_2}x_{P_2}) + G_{P_1}d_1^1 \\ A_{P_2}x_{P_2} + B_{P_2}(e_2 + C_{P_1}x_{P_1}) + G_{P_2}d_1^2 \\ A_{Q_1}x_{Q_1} + B_{Q_1}(e_1 - C_{P_2}x_{P_2}) + G_{Q_1}d_2^1 \\ A_{Q_2}x_{Q_2} + B_{Q_2}(e_2 + C_{P_1}x_{P_1}) + G_{Q_2}d_2^2 \end{bmatrix} \in S \end{aligned} \quad (17)$$

$$(ii) : C_{P_1}x_{P_1} = C_{Q_1}x_{Q_1} \quad \wedge \quad C_{P_2}x_{P_2} = C_{Q_2}x_{Q_2}$$

Define the relation $S_1 := \{(x_{P_1}, x_{Q_1}) \mid \exists x_{P_2}, x_{Q_2} : (x_{P_1}, x_{P_2}, x_{Q_1}, x_{Q_2}) \in S\}$.

It has to be shown that for any $(x_{P_1}, x_{Q_1}) \in S_1$, any u and any d_1 there exists a d_2 such that

$$(i) : \begin{bmatrix} A_{P_1}x_{P_1} + B_{P_1}u + G_{P_1}d_1 \\ A_{Q_1}x_{Q_1} + B_{Q_1}u + G_{Q_1}d_2 \end{bmatrix} \in S_1 \quad (18)$$

$$(ii) : C_{P_1}x_{P_1} = C_{Q_1}x_{Q_1}$$

Take any $(x_{P_1}, x_{Q_1}) \in S_1$ and fix u and d_1 . Since (17) holds for any \mathbf{e} and \mathbf{d}_1 , in particular it holds for $e_1 = u + C_{P_2}x_{P_2}$ and $d_1^1 = d_1$. Thus, property (18),(ii) follows directly from Eq. (17),(ii) and (18),(i) is a consequence of (17),(i) for the particular choice of \mathbf{e} and \mathbf{d}_1 . The same arguments also hold for a relation $S_2 := \{(x_{P_2}, x_{Q_2}) \mid \exists x_{P_1}, x_{Q_1} : (x_{P_1}, x_{P_2}, x_{Q_1}, x_{Q_2}) \in S\}$. ■

This means that for open interconnections, the problem of checking $\Sigma_{P_1} \parallel_o \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel_o \Sigma_{Q_2}$ can be reduced to (and, in fact, is equivalent to)

$$\begin{aligned} \Sigma_{P_1} & \preceq \Sigma_{Q_1} \\ \Sigma_{Q_1} & \preceq \Sigma_{Q_2} \end{aligned} \quad (19)$$

As a consequence, proof obligations for individual components are as hard to prove as obligations for interconnected components.

Proposition 4: For closed interconnections of linear continuous-time systems, necessity of statement (16) does in general not hold.

Proof: To construct a counterexample, define the systems

$$\Sigma_{P_2}, \Sigma_{Q_2} : \begin{aligned} \dot{x}_i &= u_i, \quad i = \{P_2, Q_2\} \\ y_i &= 0 \end{aligned} \quad (20)$$

$$\begin{aligned} \Sigma_{P_1} : \quad \dot{x}_{P_1} &= u_{P_1} & \Sigma_{Q_1} : \quad \dot{x}_{Q_1} &= \frac{1}{2}u_{Q_1} \\ y_{P_1} &= x_{P_1} & y_{Q_1} &= x_{Q_1} \end{aligned}$$

The interconnected systems are given by

$$\begin{aligned} \Sigma_{P_1} \parallel_c \Sigma_{P_2} : \quad \begin{bmatrix} \dot{x}_{P_1} \\ \dot{x}_{P_2} \\ y_{P_1} \\ y_{P_2} \end{bmatrix} &= \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_{P_1} \\ x_{P_2} \end{bmatrix} \\ \Sigma_{Q_1} \parallel_c \Sigma_{Q_2} : \quad \begin{bmatrix} \dot{x}_{Q_1} \\ \dot{x}_{Q_2} \\ y_{Q_1} \\ y_{Q_2} \end{bmatrix} &= \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_{Q_1} \\ x_{Q_2} \end{bmatrix} \end{aligned} \quad (21)$$

Thus, the interconnections $\Sigma_{P_1} \parallel_c \Sigma_{P_2}$ and $\Sigma_{Q_1} \parallel_c \Sigma_{Q_2}$ describe the same behavior so that there indeed exists a simulation relation. In fact, the two interconnections are even bisimilar. According to Theorem 3, however, there is no simulation relation of Σ_{P_1} by Σ_{Q_1} since the transfer functions of the two controllable systems Σ_{P_1} and Σ_{Q_1} do not match, $\frac{Y_{P_1}(s)}{U_{P_1}(s)} = \frac{1}{s} \neq \frac{Y_{Q_1}(s)}{U_{Q_1}(s)} = \frac{2}{s}$. ■

IV. ASSUME GUARANTEE REASONING

Suppose it has to be checked for given systems $\Sigma_i, i = \{P_1, P_2, Q_1, Q_2\}$ whether the following statement holds:

$$\Sigma_{P_1} \parallel_c \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel_c \Sigma_{Q_2} \quad (22)$$

Because of Proposition 3, we will apply assume guarantee reasoning only to systems with closed feedback interconnections. The basic idea of AGR is to split the proof obligation (22) into a sequence of obligations for components of the interconnection which are possibly easier to check than (22). A fundamental property concerning AGR rules is *soundness* or logical correctness, i.e. the question whether the assumptions in the AGR rule guarantee the conclusion. As a first example, we will investigate the following triangular rules for which only the existence of one simulation relation $\Sigma_{P_i} \preceq \Sigma_{Q_i}, i = 1, 2$, is required.

Proposition 5: Given linear continuous-time systems $\Sigma_i, i = \{P_1, P_2, Q_1, Q_2\}$ of the form (1). Then the following AGR rules are sound:

$$\begin{aligned} (A_1) \quad \Sigma_{P_1} & \preceq \Sigma_{Q_1} \\ (B_1) \quad \Sigma_{Q_1} \parallel_c \Sigma_{P_2} & \preceq \Sigma_{Q_1} \parallel_c \Sigma_{Q_2} \\ \hline (C_1) \quad \Sigma_{P_1} \parallel_c \Sigma_{P_2} & \preceq \Sigma_{Q_1} \parallel_c \Sigma_{Q_2} \end{aligned} \quad (23)$$

$$\begin{aligned} (A_2) \quad \Sigma_{P_2} & \preceq \Sigma_{Q_2} \\ (B_2) \quad \Sigma_{P_1} \parallel_c \Sigma_{Q_2} & \preceq \Sigma_{Q_1} \parallel_c \Sigma_{Q_2} \\ \hline (C_2) \quad \Sigma_{P_1} \parallel_c \Sigma_{P_2} & \preceq \Sigma_{Q_1} \parallel_c \Sigma_{Q_2} \end{aligned} \quad (24)$$

Proof: The proof relies on the modularity properties of simulation relations for linear continuous-time systems. From Proposition 2, one can deduce from (A₁) that $\Sigma_{P_1} \parallel_c \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel_c \Sigma_{P_2}$ holds when interconnected with Σ_{P_2} . Then by transitivity of simulation, one obtains (C₁) from (B₁),

$$\Sigma_{P_1} \parallel_c \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel_c \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel_c \Sigma_{Q_2} \quad (25)$$

The same arguments also hold for the second rule. ■

The above rules are examples of non-circular AGR where the assumption of antecedent (B_i), namely the existence of a simulation relation of Σ_{P_1} by Σ_{Q_1} , is guaranteed by antecedent (A_i). As in other applications (e. g. [2]), these rules are sound without any further conditions.

On the contrary, circular rules use assumptions yet to be proven in both the antecedents. Such a circular AGR rule is given by

$$\begin{aligned} (A) \quad & \Sigma_{P_1} \parallel_c \Sigma_{Q_2} \preceq \Sigma_{Q_1} \parallel_c \Sigma_{Q_2} \\ (B) \quad & \Sigma_{Q_1} \parallel_c \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel_c \Sigma_{Q_2} \\ (C) \quad & \Sigma_{P_1} \parallel_c \Sigma_{P_2} \preceq \Sigma_{Q_1} \parallel_c \Sigma_{Q_2} \end{aligned} \quad (26)$$

Note that (26) is weaker than the non-circular AGR rule (23) since by Proposition 2, (A) is implied by (A_1), but the converse is not true for closed feedback interconnections as stated in Proposition 4.

Example 1: Consider the following example systems

$$\Sigma_{P_1} : \begin{cases} \dot{\mathbf{x}}_{P_1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mathbf{x}_{P_1} + \begin{bmatrix} 1 \\ 1 \end{bmatrix} u_{P_1} \\ y_{P_1} = \begin{bmatrix} 1 & 0 \end{bmatrix} \mathbf{x}_{P_1} \end{cases} \quad (27)$$

$$\Sigma_{Q_1} : \begin{cases} \dot{\mathbf{x}}_{Q_1} = \begin{bmatrix} 2 & 0 \\ 0 & -1 \end{bmatrix} \mathbf{x}_{Q_1} + \begin{bmatrix} 1 \\ 1 \end{bmatrix} u_{P_1} \\ y_{Q_1} = \begin{bmatrix} 1 & 0 \end{bmatrix} \mathbf{x}_{Q_1} \end{cases}$$

$$\Sigma_{Q_2} : \begin{cases} \dot{\mathbf{x}}_{Q_2} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mathbf{x}_{Q_2} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u_{P_1} \\ y_{Q_2} = \begin{bmatrix} 1 & -1 \end{bmatrix} \mathbf{x}_{Q_2} \end{cases}$$

Clearly, $\Sigma_{P_1} \not\preceq \Sigma_{Q_1}$ since their transfer functions do not match, $G_{P_1} = \frac{1}{s-1} \neq G_{Q_1} = \frac{1}{s-2}$.

Considering their interconnections with Σ_{Q_2} , there does exist a simulation relation S of $\Sigma_{P_1} \parallel_c \Sigma_{Q_2}$ by $\Sigma_{Q_1} \parallel_c \Sigma_{Q_2}$ given by $S = \{(0, x_{P_1}^1, x_{Q_2}^1, 0, x_{Q_1}^1, 0, x_{Q_2}^1, 0) \mid x_{P_1}^1 = x_{Q_1}^1, (x_{P_1}^1, 0, x_{Q_2}^1, 0) \in \mathcal{X}_{P_1} \times \mathcal{X}_{Q_2}, (x_{Q_1}^1, 0, x_{Q_2}^1, 0) \in \mathcal{X}_{Q_1} \times \mathcal{X}_{Q_2}\}$. Thus, the proof obligation (A) is indeed weaker than (A_1).

We investigate the soundness of the AGR rule (26) for linear continuous-time systems without external disturbances, i.e. $G_i \equiv 0, i = \{P_1, P_2, Q_1, Q_2\}$. In the proof, the following lemma will be used.

Lemma 1: Given two deterministic linear continuous-time systems $\Sigma_i, i = 1, 2$ with the same Markov parameters, i.e. $C_1 A_1^k B_1 = C_2 A_2^k B_2, k = 0, 1, \dots$

Then for all $(x_1, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2$ such that

$$C_1 x_1 = C_2 x_2 \quad (28)$$

it holds that

$$\begin{aligned} C_1(A_1 - B_1 C_1)^k x_1 &= C_2(A_2 - B_2 C_2)^k x_2, \quad k = 1, 2, \dots \\ &\iff \\ C_1 A_1^k x_1 &= C_2 A_2^k x_2, \quad k = 1, 2, \dots \end{aligned} \quad (29)$$

Proof: We will prove (29) by induction.

For $k = 1$ we obtain

$$\begin{aligned} C_1(A_1 - B_1 C_1)x_1 &= C_2(A_2 - B_2 C_2)x_2 \\ &\iff \\ C_1 A_1 x_1 - C_1 B_1 C_1 x_1 &= C_2 A_2 x_2 - C_2 B_2 C_2 x_2 \\ &\iff \\ C_1 A_1 x_1 &= C_2 A_2 x_2 \end{aligned}$$

since $C_1 B_1 C_1 x_1 = C_2 B_2 C_2 x_2$ by assumption (28) and the equality of the first Markov parameters $C_1 B_1 = C_2 B_2$.

Assuming that (29) holds for a certain k , we conclude

$$\begin{aligned} C_1(A_1 - B_1 C_1)^{k+1} x_1 &= C_2(A_2 - B_2 C_2)^{k+1} x_2 \\ &\iff \\ C_1(A_1 - B_1 C_1)^k A_1 x_1 - C_1(A_1 - B_1 C_1)^k B_1 C_1 x_1 &= \\ = C_2(A_2 - B_2 C_2)^k A_2 x_2 - C_2(A_2 - B_2 C_2)^k B_2 C_2 x_2 & \\ &\iff \\ C_1(A_1 - B_1 C_1)^k A_1 x_1 &= C_2(A_2 - B_2 C_2)^k A_2 x_2 \\ &\iff \\ C_1 A_1^{k+1} x_1 &= C_2 A_2^{k+1} x_2 \end{aligned}$$

where we made use of

$$C_1(A_1 - B_1 C_1)^k B_1 C_1 x_1 = C_2(A_2 - B_2 C_2)^k B_2 C_2 x_2. \quad (30)$$

As before, $C_1 \tilde{x}_1 := C_1 B_1 C_1 x_1 = C_2 B_2 C_2 x_2 =: C_2 \tilde{x}_2$ so that we can apply the hypothesis (29) on

$$C_1(A_1 - B_1 C_1)^k \tilde{x}_1 = C_2(A_2 - B_2 C_2)^k \tilde{x}_2.$$

Equation (30) then reduces to the equality of the $(k+1)$ -th Markov parameters $C_1 A_1^k B_1 = C_2 A_2^k B_2$. ■

Proposition 6: Given the linear continuous-time systems $\Sigma_i, i = P_1, P_2, Q_1, Q_2$ and the conditions (A) and (B) of the circular AGR rule (26). Define the linear subspace

$$\begin{aligned} S &\subset \mathcal{X}_{P_1} \times \mathcal{X}_{P_2} \times \mathcal{X}_{Q_1} \times \mathcal{X}_{Q_2} := (31) \\ &= \{(x_{P_1}, x_{P_2}, x_{Q_1}, x_{Q_2}) \mid \exists x'_{Q_2} : (x_{P_1}, x_{Q_2}, x_{Q_1}, x'_{Q_2}) \\ &\in S_1 \wedge \exists x'_{Q_1} : (x_{Q_1}, x_{P_2}, x'_{Q_1}, x_{Q_2}) \in S_2\} \end{aligned}$$

Then the subspace S defines a simulation relation of $\Sigma_{P_1} \parallel \Sigma_{P_2}$ by $\Sigma_{Q_1} \parallel \Sigma_{Q_2}$ as defined by (C).

Moreover, if $S_i, i = 1, 2$, are maximal then S defines a full simulation relation as well. Hence the circular AGR rule (26) for deterministic linear continuous-time systems is sound.

Proof:

S defines a linear subspace:

This can easily be verified.

S defines a simulation relation of $\Sigma_{P_1} \parallel \Sigma_{P_2}$ by $\Sigma_{Q_1} \parallel \Sigma_{Q_2}$:

Take any $\mathbf{x} = (x_{P_1}, x_{P_2}, x_{Q_1}, x_{Q_2}) \in S$. Since $\mathbf{x} \in S$, property 2,(ii) is readily fulfilled, namely that $C_{P_i} x_{P_i} = C_{Q_i} x_{Q_i}, i = 1, 2$ and moreover also $C_j x_j = C_j x'_j, j = Q_1, Q_2$. Construct

$$\begin{aligned} \dot{x}'_{Q_2} &:= A_{Q_2} x'_{Q_2} + B_{Q_2} C_{Q_1} x_{Q_1} \\ \dot{x}'_{Q_1} &:= A_{Q_1} x_{Q_1} - B_{Q_1} C_{Q_2} x_{Q_2} \end{aligned} \quad (32)$$

Then

$$\begin{bmatrix} \dot{x}_{P_1} \\ \dot{x}_{Q_2} \\ \dot{x}_{Q_1} \\ \dot{x}'_{Q_2} \end{bmatrix} = \begin{bmatrix} A_{P_1} x_{P_1} - B_{P_1} C_{Q_2} x_{Q_2} \\ B_{Q_2} C_{P_1} x_{P_1} + A_{Q_2} x_{Q_2} \\ A_{Q_1} x_{Q_1} - B_{Q_1} C_{Q_2} x'_{Q_2} \\ B_{Q_2} C_{Q_1} x_{Q_1} + A_{Q_2} x'_{Q_2} \end{bmatrix} \in S_2 \quad (33)$$

and similarly $(\dot{x}_{Q_1}, \dot{x}_{P_2}, \dot{x}'_{Q_1}, \dot{x}_{Q_2}) \in S_2$.

S defines a full simulation relation :

Assuming S_1 and S_2 are maximal one can explicitly characterize the subspaces S_1 and S_2 in a kernel representation as stated in Theorem 4. The maximal simulation relations S_1^{max} can therefore be written as

$$S_1^{max} = \bigcap_{i=0}^k \ker \begin{bmatrix} C_1(A_1 - B_1C_1)^i & -C_2(A_2 - B_2C_2)^i \end{bmatrix} \quad (34)$$

Since we are considering deterministic systems, the assumptions of Lemma 1 are fulfilled which renders (34) equivalent to

$$S_1^{max} = \bigcap_{i=0}^k \ker \begin{bmatrix} C_1A_1^i & -C_2A_2^i \end{bmatrix} \quad (35)$$

Partitioning S_1^{max} , one obtains the desired kernel representation

$$S_1 = \{(x_{P_1}, x_{Q_2}, x_{Q_1}, x'_{Q_2}) \mid P_1^1 x_{P_1} + Q_2^1 x_{Q_2} + Q_1^1 x_{Q_1} + Q_2^{1'} x'_{Q_2} = 0\} \quad (36)$$

where

$$P_1^1 = \begin{bmatrix} C_{P_1} \\ 0 \\ C_{P_1}A_{P_1} \\ 0 \\ \vdots \\ C_{P_1}A_{P_1}^k \end{bmatrix}, Q_1^1 = \begin{bmatrix} C_{Q_1} \\ 0 \\ C_{Q_1}A_{Q_1} \\ \vdots \\ C_{Q_1}A_{Q_1}^k \end{bmatrix}$$

$$Q_2^1 = Q_2^{1'} = \begin{bmatrix} 0 \\ C_{Q_2} \\ 0 \\ C_{Q_2}A_{Q_2} \\ 0 \\ \vdots \\ C_{Q_2}A_{Q_2}^k \end{bmatrix}$$

with $\text{im}P_1^1 \subset \text{im}Q_1^1 + \text{im}Q_2^{1'}$ since S_1 is full. Similarly for S_2 , one obtains

$$S_2 = \{(x_{Q_1}, x_{P_2}, x'_{Q_1}, x_{Q_2}) \mid Q_1^2 x_{Q_1} + P_2^2 x_{P_2} + Q_1^{1'} x'_{Q_1} + Q_2^2 x_{Q_2} = 0\} \quad (37)$$

for some matrices $P_2^2, Q_2^1, Q_2^{1'}, Q_2^2$ such that $Q_1^2 = Q_1^{1'}$ and $\text{im}P_2^2 \subset \text{im}Q_1^{1'} + \text{im}Q_2^2$.

Following the construction (31), S is given by

$$S = \left\{ (x_{P_1}, x_{P_2}, x_{Q_1}, x_{Q_2}) \mid \exists x'_{Q_1}, x'_{Q_2} : \begin{bmatrix} P_1^1 \\ 0 \end{bmatrix} x_{P_1} + \begin{bmatrix} 0 \\ P_2^2 \end{bmatrix} x_{P_2} + \begin{bmatrix} Q_1^1 & Q_2^1 \\ Q_2^1 & Q_2^2 \end{bmatrix} \begin{bmatrix} x_{Q_1} \\ x_{Q_2} \end{bmatrix} + \begin{bmatrix} Q_2^{1'} \\ 0 \end{bmatrix} x'_{Q_2} + \begin{bmatrix} 0 \\ Q_1^{1'} \end{bmatrix} x'_{Q_1} = 0 \right\}$$

Then, S is a full simulation relation if

$$\text{im} \begin{bmatrix} P_1^1 & 0 \\ 0 & P_2^2 \end{bmatrix} \subset \text{im} \begin{bmatrix} Q_1^1 & Q_2^1 \\ Q_2^1 & Q_2^2 \end{bmatrix} + \text{im} \begin{bmatrix} Q_2^{1'} \\ 0 \end{bmatrix} + \text{im} \begin{bmatrix} 0 \\ Q_1^{1'} \end{bmatrix} \quad (38)$$

Knowing that S_1 and S_2 are full and $\text{im}Q_1^2 = \text{im}Q_2^{1'}$, $\text{im}Q_2^1 = \text{im}Q_2^{1'}$ from (36) and (37), respectively, it holds that

$$\text{im} \begin{bmatrix} P_1^1 \\ 0 \end{bmatrix} \subset \text{im} \begin{bmatrix} Q_1^1 \\ Q_2^1 \end{bmatrix} + \text{im} \begin{bmatrix} Q_2^{1'} \\ 0 \end{bmatrix} + \text{im} \begin{bmatrix} 0 \\ Q_1^{1'} \end{bmatrix}$$

$$\text{im} \begin{bmatrix} 0 \\ P_2^2 \end{bmatrix} \subset \text{im} \begin{bmatrix} Q_2^1 \\ Q_2^2 \end{bmatrix} + \text{im} \begin{bmatrix} Q_2^{1'} \\ 0 \end{bmatrix} + \text{im} \begin{bmatrix} 0 \\ Q_1^{1'} \end{bmatrix}$$

Thus, (38) is fulfilled which makes S a full simulation relation.

Finally, by (A) and (B) there exist full simulation relations S_1 and S_2 implying that also the maximal simulation relations for (A) and (B) are full. Hence S as defined in (31) is a full simulation relation. ■

V. CONCLUSIONS

In this paper, we started to develop a framework for compositional and assume guarantee reasoning for linear dynamical systems. For the open type of interconnection, modularity of simulation relations is the main property. Thus, statements with respect to interacting subsystems can be reduced to statements with respect to the individual components and vice versa. When closed interconnections are considered, assume guarantee reasoning can simplify the analysis of complex interconnections. To that aim, we presented both circular and non-circular AGR rules. As a subject of future research, the fundamental properties of the latter, especially its soundness, are to be investigated also for non-deterministic systems. Furthermore, generalizations to classes of nonlinear or hybrid systems and other types of interconnections would be desirable.

REFERENCES

- [1] R. Alur, T. A. Henzinger, G. Lafferriere, and G. J. Pappas. Discrete abstractions of hybrid systems. *Proceedings of the IEEE*, 88:971–984, 2000.
- [2] G. Frehse. *Compositional Verification of Hybrid Systems using Simulation Relations*. PhD thesis, Radboud Universiteit Nijmegen, 2005.
- [3] T. A. Henzinger, M. Minea, and V. Prabh. Assume-guarantee reasoning for hierarchical hybrid systems. In *HSCC 2001*, pages 275 – 290, 2001.
- [4] T. A. Henzinger, S. Qadeer, and S. K. Rajamani. You Assume, We Guarantee: Methodology and Case Studies. In *CAV 1998*, pages 440–451, 1998.
- [5] R. Milner. *Communication and Concurrency*. Prentice Hall, 1989.
- [6] J. Misra and K. M. Chandy. Proofs of networks of processes. *IEEE Trans. Softw. Eng.*, 7(4):417–426, 1981.
- [7] G. J. Pappas, G. Lafferriere, and S. Sastry. Hierarchically consistent control systems. *IEEE Transactions on Automatic Control*, 45(6):1144–1160, 2000.
- [8] A. Pnueli. In transition from global to modular temporal reasoning about programs. *Logic and Models of Concurrent Systems*, pages 123–144, 1984.
- [9] A. J. van der Schaft. Equivalence of dynamical systems by bisimulation. *IEEE Transactions on Automatic Control*, 49(12):2160–2172, 2004.