Composition of behavioural assume-guarantee contracts

Shali, Brayan M.; van der Schaft, Arjan; Besselink, Bart

Published in:
IEEE Transactions on Automatic Control

DOI:
10.1109/TAC.2022.3233290

Composition of Behavioural Assume–Guarantee Contracts

Brayan M. Shali, *Graduate Student Member, IEEE*, Arjan van der Schaft, *Fellow, IEEE*, and Bart Besselink, *Member, IEEE*

***Abstract*—The growing complexity of modern engineering systems necessitates a method for design and analysis that is inherently modular. Methods based on using contracts for system design have successfully tackled this issue for a variety of system classes, but mostly in the context of discrete software systems. Motivated by this, we present assume–guarantee contracts for continuous linear dynamical systems with inputs and outputs. Such contracts serve as system specifications through two aspects. The assumptions specify the dynamic behavior of the environment of the system, which provides inputs for it, whereas, the guarantees specify the desired dynamic behavior of the output of the system when interconnected with a relevant environment. This is formalized by utilizing the behavioral approach to system theory. We define and characterize notions of contract implementation and contract refinement, where the latter is used to compare contracts. We also define and characterize two notions of contract composition that allow one to reason about two types of system interconnections: series and feedback. The properties of refinement and composition allow contracts to be used for modular design and analysis.**

***Index Terms*—Contract-based design, interconnected systems, linear systems, modular design.**

I. Introduction

Modern engineering systems, such as smart grids and intelligent transportation systems, are complex systems that often comprise a large number of interconnected components. These components can be quite complex themselves, which usually means that they have to be developed by (different) specialized manufacturers, possibly at different stages of the development of the overall system. Facilitating this requires a method for system design that is inherently *modular*, i.e., that allows components to be developed independently while still ensuring proper integration into the overall system. The necessity for such methods is especially recognized in the field of cyber-physical systems [1], [2]. In this article, we will focus on developing a method for modular analysis and design of physical components modeled by differential equations.

Various methods for modular analysis already exist in the control literature. Some of the most well-known ones are based on the theory of dissipativity [3], [4], which includes the celebrated small-gain theorem and passivity theorems. On the other hand, there are modular control methods, such as decentralized control [5], [6], [7], which refers to the design of controllers for components that use only local information to achieve a desired behavior of the overall system in which they are embedded. A major limitation of decentralized control is that the design of controllers typically requires an a priori model of the overall system. This limitation is addressed by Ishizaki et al. [8], see also [9] and [10], where a method called retrofit control was proposed. In this article, we propose an alternative method for modular analysis and design based on using *contracts*.

Contract-based design is a design philosophy that finds its origins in the field of software engineering [11]. It revolves around using contracts as specifications for system behavior, within a framework that allows the analysis and design of interconnected systems to be kept at the level of contracts. Contract-based design has attracted a lot of attention in the computer science community, see [12] and the references therein. However, the literature on contracts is focused mostly on discrete (software) systems, whereas continuous (physical) systems have been largely overlooked.

Motivated by this, we present assume–guarantee contracts as specifications for continuous linear dynamical systems with inputs and outputs. As a first contribution, we define contracts and provide a necessary and sufficient condition for contract *implementation*, which allows one to verify whether a given system satisfies the specification that a contract expresses. In particular, we define contracts as pairs of linear dynamical systems called *assumptions* and *guarantees*, both characterized in a behavioral framework [13]. The assumptions capture the available information about the dynamic behavior of the environment, which provides inputs for the system, thus leading to a class of *compatible environments*. The guarantees capture the desired dynamic behavior of the output of the system when interconnected with a compatible environment, thus leading to a class of *implementations*. The contracts in this article express a specification on the dynamic behavior of a system; hence, they provide an alternative to common methods for expressing system specifications in control, such as dissipativity [3] and set invariance [14], which are typically static in nature. The necessary and sufficient condition for contract implementation is an inclusion of behaviors involving the assumptions and guarantees, which can be verified in a systematic manner. This is illustrated with examples throughout this article.

Manuscript received 20 September 2022; accepted 14 December 2022. Date of publication 30 December 2022; date of current version 27 September 2023. Recommended by Associate Editor Y. Le Gorrec. *(Corresponding author: Brayan M. Shali.)*

The authors are with the Jan C. Willems Center for Systems and Control, and the Bernoulli Institute for Mathematics, Computer Science, and Artificial Intelligence, University of Groningen, 9747AG Groningen, The Netherlands (e-mail: b.m.shali@rug.nl; A.J.van.der.Schaft@rug.nl; b.besselink@rug.nl).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TAC.2022.3233290.

Digital Object Identifier 10.1109/TAC.2022.3233290

As a second contribution, we define and characterize contract *refinement*. The notion of contract refinement allows one to compare two contracts in order to determine if one contract expresses a stricter specification than the other contract. More precisely, a contract refines another contract if it has a larger class of compatible environments but a smaller class of implementations. We provide necessary and sufficient conditions for contract refinement in the form of two inclusions of behaviors involving the assumptions and guarantees of the two contracts. Broadly speaking, we show that a contract refines another contract if it has stricter guarantees and looser assumptions.

As a third contribution, we define and characterize two types of contract *composition*, corresponding to two types of interconnections: series and feedback. For each type, the composition of two contracts is such that the corresponding interconnection of any two of their implementations is guaranteed to implement the composition. Furthermore, the environment of each implementation within the interconnection is guaranteed to be compatible with the corresponding contract. We provide necessary and sufficient conditions for the existence of each composition in the form of inclusions of behaviors involving the assumptions and guarantees of the two contracts. We also provide an explicit expression for this composition when it exists.

Together, the notions of contract refinement and contract composition allow components within interconnected systems to be developed independently since the tasks of design and verification are kept at the level of contracts. In particular, given a contract for the overall system, one can use the notions of refinement and composition to determine appropriate contracts for the components such that their interconnection is guaranteed to implement the contract for the overall system. This facilitates independent design since the developer of an individual component can focus on implementing their assigned contract only, and can disregard the other components or their integration into the overall system.

Various notions of contracts have already been used as specifications for dynamical systems. Parameteric assume–guarantee contracts are introduced in [15] and used in [16] and [17], whereas the assume–guarantee contracts introduced in [18] are used in [19], [20], and [21]. We also refer to [22], [23], [24], [25], and [26] as further examples of works involving contracts. While the contracts in this article express specifications on the dynamics of continuous-time systems, the contracts in [15], [16], [17], and [25] are defined only for discrete-time systems, and the contracts in [18], [19], [20], [21], [22], and [27] cannot express specifications on dynamics. In this respect, the contracts in this article are most closely related to the contracts in [23], whereas [28], [29], and [30] contain related work on compositional reasoning. The contracts in [26] do not suffer from the abovementioned limitations, but their generality comes at the expense of algorithms for verification. Our work is specialized to linear systems, allowing for a more complete instantiation of the metatheory that includes algebraic characterization that can be verified algorithmically.

The rest of this article is organized as follows. In Section II, we introduce the class of systems that will be considered in this article. In Section III, we introduce contracts and define and characterize contract implementation and contract conjunction. In Section IV, we introduce three operations on systems: intersection, projection, and product. These are used in Section V, where we define and characterize two types of contract composition corresponding to two types of system interconnections: series and feedback. Finally, Section VI concludes this article. Throughout the article, we illustrate relevant concepts using simple examples.

Fig. 1. System Σ.

The notation in this article is mostly standard. The space of smooth functions from $\mathbb{R}$ to $\mathbb{R}^n$ is denoted by $\mathcal{C}_n^\infty$. A matrix whose entries are polynomials is called a *polynomial matrix*, and a matrix whose entries are rational functions is called a *rational matrix*. All polynomials are univariate and have real coefficients. A rational function is *proper* if the degree of its denominator is greater than or equal to the degree of its numerator. A rational matrix is proper if all of its entries are proper rational functions. A square polynomial matrix $P(s)$ is *invertible* if there exists a rational matrix $Q(s)$ such that $P(s)Q(s) = I$, and it is *unimodular* if there exists a polynomial matrix $Q(s)$ such that $P(s)Q(s) = I$. In both cases, $Q(s)$ is the *inverse* of $P(s)$ and is denoted by $P(s)^{-1}$. It is well known that $P(s)$ is invertible if and only if $\det P(s)$ is a nonzero polynomial, and $P(s)$ is unimodular if and only if $\det P(s)$ is a nonzero constant. Equivalently, $P(s)$ is invertible if and only if $P(\lambda)$ is invertible for all but finitely many $\lambda \in \mathbb{R}$, and it is unimodular if and only if $P(\lambda)$ is invertible for *all* λ in $\mathbb{R}$. Finally, a rational matrix $P(s)$ has *full row rank* if $P(\lambda)$ has full row rank for all but finitely many $\lambda \in \mathbb{R}$.

II. System Class

In this article, we consider systems of the form

$$\Sigma : \begin{cases} \dot{x} = Ax + Bu, \\ y = Cx + Du, \end{cases} \tag{1}$$

where $x \in \mathcal{C}_n^\infty$ is the state trajectory, $u \in \mathcal{C}_m^\infty$ is the input trajectory, and $y \in \mathcal{C}_p^\infty$ is the output trajectory. We regard u and y as external variables that can interact with the environment, whereas x is internal, as illustrated in Fig. 1.

Our goal is to develop a formal method for expressing specifications on the dynamic behavior of such systems, which is a part of a framework that facilitates the independent design of components within interconnected systems. Inspired by the metatheory of contracts presented in [12], we will do this by introducing contracts as specifications and developing appropriate notions of contract refinement and contract composition.

A distinguishing feature of using contracts as specifications is that they specify the desired behavior of a system when interconnected with its environment. As the environment of a system has access only to its external variables, this means that we are only interested in the behavior of the external variables u and y, whereas the behavior of the internal variable x can be disregarded. To formalize this, we will utilize the behavioral approach to systems theory [13], [31].

The *external behavior* of Σ is defined as

$$\mathfrak{B}(\Sigma) = \left\{ (u, y) \in \mathcal{C}_{m+p}^\infty \;\middle|\; \exists x \in \mathcal{C}_n^\infty \text{ s.t. } (1) \text{ holds} \right\}. \tag{2}$$

In the behavioral approach to systems theory, the system Σ is seen as a representation of its external behavior $\mathfrak{B}(\Sigma)$. In view of [32, Th. 6.2], the same external behavior can always be represented by a system of the form

$$\Sigma : P\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = Q\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u, \tag{3}$$

where $u \in \mathcal{C}_m^\infty$, $y \in \mathcal{C}_p^\infty$, and $P(s)$ and $Q(s)$ are polynomial matrices such that $P(s)$ is invertible and $P(s)^{-1}Q(s)$ is proper. If these conditions on $P(s)$ and $Q(s)$ are satisfied, then Σ of the form (3) is said to be in *input–output form* [13, Sec. 3.3]. Then, [32, Th. 6.2] says that the external behavior of any system of the form (1) is equal to the external behavior of an appropriately chosen system of the form (3) in input–output form, where the latter is defined as

$$\mathfrak{B}(\Sigma) = \left\{(u, y) \in \mathcal{C}_{m+p}^\infty \;\middle|\; (3) \text{ holds}\right\}. \tag{4}$$

However, systems of the form (3) are the more convenient alternative for analysis since they involve only the external variables u and y. Therefore, in the rest of this article, we will consider systems Σ of the form (3) in input–output form instead of systems of the form (1), and we stress that the two forms are completely interchangeable.

The concept of behavior allows one to compare different systems. In particular, if $\mathfrak{B}(\Sigma_1) \subset \mathfrak{B}(\Sigma_2)$, then for a given input trajectory $u \in \mathcal{C}_m^\infty$, the set of output trajectories produced by Σ_1 is contained in the set of output trajectories produced by Σ_2; hence, Σ_2 can be interpreted as having richer dynamics than Σ_1. Behavioral inclusion plays a major role in the definition of a contract and its related concepts. The following theorem, whose proof can be found in [33], see also [34], provides an algebraic characterization of behavioral inclusion that will be used in the following sections.

Theorem 1 ([33, Th. 2]): Consider the behaviors

$$\mathfrak{B}_j = \left\{w \in \mathcal{C}_k^\infty \;\middle|\; R_j\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) w = 0\right\},\; j \in \{1, 2\},$$

where $R_1(s)$ and $R_2(s)$ are polynomial matrices. Then, $\mathfrak{B}_1 \subset \mathfrak{B}_2$ if and only if there exists a polynomial matrix $M(s)$ such that $R_2(s) = M(s)R_1(s)$.

III. Contracts

In this section, we define contracts and introduce notions of contract implementation and contract refinement. We also establish necessary and sufficient conditions for both contract implementation and contract refinement, the latter being the main result of this section.

Let Σ be a system of the form (3) in input–output form. An *environment* E for Σ is a system of the form

$$\mathrm{E} : 0 = E\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u, \tag{5}$$

which defines the behavior

$$\mathfrak{B}_\mathrm{i}(\mathrm{E}) = \{u \in \mathcal{C}_m^\infty \mid (5) \text{ holds}\}. \tag{6}$$

Here, the subscript i indicates that the behavior $\mathfrak{B}_\mathrm{i}(\mathrm{E})$ is in terms of u, which is the input of Σ. Therefore, we will also refer to $\mathfrak{B}_\mathrm{i}(\mathrm{E})$ as an *input behavior*.

The interconnection of the system Σ and its environment E is given by

$$\mathrm{E} \wedge \Sigma : \begin{bmatrix} P(\frac{\mathrm{d}}{\mathrm{d}t}) \\ 0 \end{bmatrix} y = \begin{bmatrix} Q(\frac{\mathrm{d}}{\mathrm{d}t}) \\ E(\frac{\mathrm{d}}{\mathrm{d}t}) \end{bmatrix} u, \tag{7}$$

that is, we obtain $\mathrm{E} \wedge \Sigma$ by setting the input generated by E as input of Σ, as shown in Fig. 2. The interconnection $\mathrm{E} \wedge \Sigma$ defines

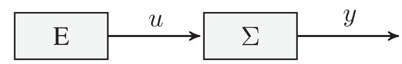


Fig. 2. Interconnection $\mathrm{E} \wedge \Sigma$.

the behavior

$$\mathfrak{B}_\mathrm{o}(\mathrm{E} \wedge \Sigma) = \left\{y \in \mathcal{C}_p^\infty \;\middle|\; \exists u \in \mathcal{C}_m^\infty \text{ s.t. } (7) \text{ holds}\right\}, \tag{8}$$

where the subscript o indicates that $\mathfrak{B}_\mathrm{o}(\mathrm{E} \wedge \Sigma)$ is in terms of y, which is the output of Σ. Analogously to $\mathfrak{B}_\mathrm{i}(\mathrm{E})$, we will refer to $\mathfrak{B}_\mathrm{o}(\mathrm{E} \wedge \Sigma)$ as an *output behavior*.

We are interested in guaranteeing properties of Σ when interconnected with relevant environments E. This will be formalized via the notion of a contract. To define a contract, we introduce another two systems: the *assumptions* A and the *guarantees* Γ. On the one hand, the assumptions A are a system of the form

$$\mathrm{A} : 0 = A(\tfrac{\mathrm{d}}{\mathrm{d}t})u, \tag{9}$$

and they define the input behavior $\mathfrak{B}_\mathrm{i}(\mathrm{A})$. On the other hand, the guarantees Γ are a system of the form

$$\Gamma : G(\tfrac{\mathrm{d}}{\mathrm{d}t})y = 0, \tag{10}$$

and they define the output behavior $\mathfrak{B}_\mathrm{o}(\Gamma)$.

Definition 1: A *contract* $\mathcal{C}$ is a pair (A, Γ) of assumptions A and guarantees Γ.

Contracts can be used as a formal specification for the external behavior of Σ in the following way.

Definition 2: Consider the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$.

1) An environment E is *compatible* with $\mathcal{C}$ if

$$\mathfrak{B}_\mathrm{i}(\mathrm{E}) \subset \mathfrak{B}_\mathrm{i}(\mathrm{A}). \tag{11}$$

2) A system Σ of the form (3) in input–output form *implements* $\mathcal{C}$ if

$$\mathfrak{B}_\mathrm{o}(\mathrm{E} \wedge \Sigma) \subset \mathfrak{B}_\mathrm{o}(\Gamma) \tag{12}$$

for all environments E compatible with $\mathcal{C}$. In this case, we say that Σ is an *implementation* of $\mathcal{C}$.

A contract gives a formal specification for the external behavior of a system through two aspects. First, the assumptions specify the class of environments in which the system is supposed to operate. Second, the guarantees characterize the desired external behavior of the system, which needs to be achieved for any compatible environment.

Remark 1: According to Definition 2, when using the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ as a specification, only the behaviors $\mathfrak{B}_\mathrm{i}(\mathrm{A})$ and $\mathfrak{B}_\mathrm{o}(\Gamma)$ are relevant, not their particular representations A and Γ. This means that, without loss of generality, we can assume that A and Γ are minimal representations of $\mathfrak{B}_\mathrm{i}(\mathrm{A})$ and $\mathfrak{B}_\mathrm{o}(\Gamma)$, that is, A and Γ are of the form (9) and (10), respectively, with $A(s)$ and $G(s)$ being polynomial matrices that have full row rank, see [13, Sec. 2.5.6].

According to Definition 1, verifying that a system Σ implements the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ requires the explicit construction of all compatible environments E and the confirmation of (12) for each one of them. The following theorem shows that this is not necessary and contract implementation can be verified directly from the assumptions and guarantees.

Theorem 2: A system Σ of the form (3) in input–output form implements $\mathcal{C} = (\mathrm{A}, \Gamma)$ if and only if

$$\mathfrak{B}_{\mathrm{o}}\left(\mathrm{A} \wedge \Sigma\right) \subset \mathfrak{B}_{\mathrm{o}}\left(\Gamma\right). \tag{13}$$

Proof: Suppose that (13) holds. Let E be an environment compatible with $\mathcal{C}$. Note that u and y satisfy (7) if and only if $(u, y) \in \mathfrak{B}(\Sigma)$ and $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{E})$; hence, $y \in \mathfrak{B}_{\mathrm{o}}(\mathrm{E} \wedge \Sigma)$ if and only if there exists $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{E})$ such that $(u, y) \in \mathfrak{B}(\Sigma)$. Let $y \in \mathfrak{B}_{\mathrm{o}}(\mathrm{E} \wedge \Sigma)$ and let $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{E})$ be such that $(u, y) \in \mathfrak{B}(\Sigma)$. Since E is compatible with $\mathcal{C}$, it follows that $\mathfrak{B}_{\mathrm{i}}(\mathrm{E}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$ and, thus, $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$. But then, $y \in \mathfrak{B}_{\mathrm{o}}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma)$, which shows that $\mathfrak{B}_{\mathrm{o}}(\mathrm{E} \wedge \Sigma) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma)$ for all environments E compatible with $\mathcal{C}$, i.e., Σ implements $\mathcal{C}$.

Conversely, suppose that Σ implements $\mathcal{C}$. Then, (13) holds because A is an environment compatible with $\mathcal{C}$. ∎

Remark 2: As guarantees do not restrict the input, we have that $\mathfrak{B}_{\mathrm{o}}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma)$ if and only if $\mathfrak{B}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}(\Gamma)$, where the external behaviors of $\mathrm{A} \wedge \Sigma$ and Γ are defined in the obvious way, namely, as the spaces of smooth functions (u, y) that satisfy the respective equations. In view of Theorems 1 and 2, this implies that a system Σ of the form (3) in input–output form implements the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$, where A is given by (9) and Γ is given by (10), if and only if there exist polynomial matrices $M_1(s)$ and $M_2(s)$ such that

$$\begin{bmatrix} G(s) & 0 \end{bmatrix} = \begin{bmatrix} M_1(s) & M_2(s) \end{bmatrix} \begin{bmatrix} P(s) & -Q(s) \\ 0 & -A(s) \end{bmatrix}. \tag{14}$$

The existence of such polynomial matrices $M_1(s)$ and $M_2(s)$ can be verified using the Smith canonical form of the right-hand side of (14), as shown in [33, Lemma 1].

Remark 3: We point out that if Σ implements the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ and Σ' is such that $\mathfrak{B}(\Sigma') \subset \mathfrak{B}(\Sigma)$, then $\mathfrak{B}_{\mathrm{o}}(\mathrm{A} \wedge \Sigma_1') \subset \mathfrak{B}_{\mathrm{o}}(\mathrm{A} \wedge \Sigma)$ and, thus, Σ' also implements $\mathcal{C}$. This means that we can replace Σ by Σ' without verifying that Σ' is an implementation, as long as it is known that $\mathfrak{B}(\Sigma') \subset \mathfrak{B}(\Sigma)$.

We will illustrate how contracts can be used as specifications in practice with a simple example.

Example 1: Suppose that we have two ships on the open sea, one much bigger than the other. The large ship has a crane that moves cargo to the smaller ship. We want the crane to be such that the cargo descends to the smaller ship at a given rate. To make this more concrete, let q_l and q_s denote the vertical displacements of the large and small ships, respectively. The dynamics of q_l and q_s can be modeled simply as

$$\tau_l \dot{q}_l = -q_l + d, \quad \tau_s \dot{q}_s = -q_s + d, \tag{15}$$

where τ_l and τ_s are constants, and d is the water surface displacement caused by waves. We assume that τ_l is much larger than τ_s because the influence of the waves on the large ship is much smaller. Let q_c denote the vertical displacement of the cargo, which the crane needs to control. We want q_c to converge to q_s with a given rate $k > 0$, that is, we want

$$\dot{q}_c - \dot{q}_s = -k(q_c - q_s). \tag{16}$$

In order to achieve this, we assume that the crane has the vertical displacements of both ships and the vertical velocity of the large ship available for measurement.

We will express this specification for the crane in the form of a contract. First, we note that the input is given by

$$u = \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix}^\top = \begin{bmatrix} q_s & q_l & \dot{q}_l \end{bmatrix}^\top \tag{17}$$

and the output is given by

$$y = \begin{bmatrix} y_1 & y_2 \end{bmatrix}^\top = \begin{bmatrix} q_s & q_c \end{bmatrix}^\top. \tag{18}$$

We have that $\dot{u}_2 = u_3$, while subtracting the two equations in (15) yields

$$\tau_s \dot{u}_1 + u_1 - u_2 - \tau_l u_3 = 0. \tag{19}$$

Therefore, we can take the assumptions A as in (9) with

$$A(s) = \begin{bmatrix} 0 & s & -1 \\ \tau_s s + 1 & -1 & -\tau_l \end{bmatrix}. \tag{20}$$

Note that we make an assumption only on the relative motion of the two ships on the open sea, i.e., we make no assumption on the water surface displacement d. Meanwhile, in view of (16), we have the guarantees Γ as in (10) with

$$G(s) = \begin{bmatrix} s + k & -s - k \end{bmatrix}. \tag{21}$$

Now, the specification on the crane is captured by the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$, that is, the crane is a system Σ that needs to implement $\mathcal{C}$. We claim that the crane satisfies the specification if it is designed to lower the cargo according to

$$\dot{q}_c = -k q_c + \left(k - \frac{1}{\tau_s}\right) q_s + \frac{1}{\tau_s} q_l + \frac{\tau_l}{\tau_s} \dot{q}_l. \tag{22}$$

Since $u_1 = q_s = y_1$, it follows that:

$$\begin{aligned} y_1 &= u_1 \\ \dot{y}_2 + k y_2 &= \left(k - \frac{1}{\tau_s}\right) u_1 + \frac{1}{\tau_s} u_2 + \frac{\tau_l}{\tau_s} u_3. \end{aligned} \tag{23}$$

Therefore, the claim is that the system Σ given by (3) with

$$P(s) = \begin{bmatrix} 1 & 0 \\ 0 & s + k \end{bmatrix}, \quad Q(s) = \begin{bmatrix} 1 & 0 & 0 \\ k - \frac{1}{\tau_s} & \frac{1}{\tau_s} & \frac{\tau_l}{\tau_s} \end{bmatrix} \tag{24}$$

implements $\mathcal{C}$. Note that Σ is in input–output form, i.e., it can be represented as a system of the form (1), and (14) holds for

$$M_1(s) = \begin{bmatrix} s + k & -1 \end{bmatrix}, \quad M_2(s) = \begin{bmatrix} 0 & -\frac{1}{\tau_s} \end{bmatrix}, \tag{25}$$

which, due to Remark 2, implies that Σ implements $\mathcal{C}$. Note also that we have artificially included the input q_s as part of the output in order to express (16) as guarantees on the output.

We proceed to developing a notion of contract refinement, which is an essential ingredient in a contract theory. It allows contracts to be compared in order to determine if one contract represents a stricter specification than another contract. Formally, we have the following definition.

Definition 3: The contract $\mathcal{C}_1$ *refines* the contract $\mathcal{C}_2$ if the following conditions hold:

1) if E is compatible with $\mathcal{C}_2$, then E is compatible with $\mathcal{C}_1$;
2) if Σ implements $\mathcal{C}_1$, then Σ implements $\mathcal{C}_2$.

In other words, $\mathcal{C}_1$ refines $\mathcal{C}_2$ if it has a larger class of compatible environments and a smaller class of implementations. Then, it is clear that $\mathcal{C}_1$ expresses a more restrictive specification than $\mathcal{C}_2$.

Just like contract implementation, contract refinement can be verified directly from the assumptions and guarantees. Given $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$, it is easily seen from Definition 2 that the first condition in Definition 3 is equivalent to $\mathfrak{B}_\mathrm{i}(\mathrm{A}_2) \subset \mathfrak{B}_\mathrm{i}(\mathrm{A}_1)$. However, it is not immediately clear what the second condition is equivalent to. To resolve this, we will make use of autonomous implementations. A system Σ is *autonomous* if it can be represented by

$$\Sigma : P\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = 0, \tag{26}$$

where $P(s)$ is an invertible polynomial matrix. Note that autonomous systems are of the form (3) with $Q(s) = 0$ and are, thus, in input–output form. Since autonomous systems do not admit inputs, we have that $\mathfrak{B}_\mathrm{o}(\mathrm{A}_1 \wedge \Sigma) = \mathfrak{B}_\mathrm{o}(\Sigma)$ if Σ is autonomous; hence, by Theorem 2, an autonomous Σ implements $\mathcal{C}_1$ if and only if $\mathfrak{B}_\mathrm{o}(\Sigma) \subset \mathfrak{B}_\mathrm{o}(\Gamma_1)$. Similarly, an autonomous Σ implements $\mathcal{C}_2$ if and only if $\mathfrak{B}_\mathrm{o}(\Sigma) \subset \mathfrak{B}_\mathrm{o}(\Gamma_2)$. With this in mind, we state and prove the following result regarding autonomous systems and behavioral inclusion.

Lemma 3: If $\mathfrak{B}_\mathrm{o}(\Sigma) \subset \mathfrak{B}_\mathrm{o}(\Gamma_1)$ implies $\mathfrak{B}_\mathrm{o}(\Sigma) \subset \mathfrak{B}_\mathrm{o}(\Gamma_2)$ for all autonomous Σ, then $\mathfrak{B}_\mathrm{o}(\Gamma_1) \subset \mathfrak{B}_\mathrm{o}(\Gamma_2)$.

Proof: Let Γ_1 and Γ_2 be given by

$$\Gamma_1 : G_1\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = 0 \quad \text{and} \quad \Gamma_2 : G_2\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = 0, \tag{27}$$

where $G_1(s)$ and $G_2(s)$ are polynomial matrices. In view of Remark 1, we can assume that $G_1(s)$ has full row rank. This means that there exists a polynomial matrix $G_1'(s)$ such that

$$\begin{bmatrix} G_1(s) \\ G_1'(s) \end{bmatrix} \tag{28}$$

is invertible. Thus, for any positive integer k, the system

$$\Sigma_k : P_k\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = 0, \tag{29}$$

is autonomous, where

$$P_k(s) = \begin{bmatrix} G_1(s) \\ s^k G_1'(s) \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & s^k I \end{bmatrix} \begin{bmatrix} G_1(s) \\ G_1'(s) \end{bmatrix}. \tag{30}$$

Furthermore, since

$$G_1(s) = \begin{bmatrix} I & 0 \end{bmatrix} P_k(s), \tag{31}$$

it follows from Theorem 1 that $\mathfrak{B}_\mathrm{o}(\Sigma_k) \subset \mathfrak{B}_\mathrm{o}(\Gamma_1)$, which implies that $\mathfrak{B}_\mathrm{o}(\Sigma_k) \subset \mathfrak{B}_\mathrm{o}(\Gamma_2)$ by assumption. Due to Theorem 1, the latter holds if and only if there exists a polynomial matrix $M_k(s)$ such that

$$G_2(s) = M_k(s) P_k(s). \tag{32}$$

Using (30), we find that (32) holds if and only if

$$G_2(s) \begin{bmatrix} G_1(s) \\ G_1'(s) \end{bmatrix}^{-1} = M_k(s) \begin{bmatrix} I & 0 \\ 0 & s^k I \end{bmatrix}. \tag{33}$$

Note that the left-hand side of (33) does not depend on k. Moreover, as the right-hand side is a polynomial matrix, every entry of the left-hand side of (33) is a polynomial. Take k to be larger than the degree of any of these polynomials. This means that the product of s^k with any nonzero polynomial yields a polynomial whose degree is larger than the degree of any of the polynomial entries in the left-hand side of (33). Consequently, (33) holds only if

$$M_k(s) = \begin{bmatrix} M(s) & 0 \end{bmatrix} \tag{34}$$

for some polynomial matrix $M(s)$. Then, (33) yields

$$G_2(s) = \begin{bmatrix} M(s) & 0 \end{bmatrix} \begin{bmatrix} G_1(s) \\ G_1'(s) \end{bmatrix} = M(s) G_1(s) \tag{35}$$

and, thus, $\mathfrak{B}_\mathrm{o}(\Gamma_1) \subset \mathfrak{B}_\mathrm{o}(\Gamma_2)$ due to Theorem 2. ■

Lemma 3 can be used to obtain necessary and sufficient conditions for contract refinement. This is done in the following theorem, which is the main result of this section.

Theorem 4: The contract $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ refines the contract $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ if and only if

$$\mathfrak{B}_\mathrm{i}(\mathrm{A}_2) \subset \mathfrak{B}_\mathrm{i}(\mathrm{A}_1) \quad \text{and} \quad \mathfrak{B}_\mathrm{o}(\Gamma_1) \subset \mathfrak{B}_\mathrm{o}(\Gamma_2). \tag{36}$$

Proof: Suppose that (36) holds. Let E be compatible with $\mathcal{C}_2$ and Σ be an implementation of $\mathcal{C}_1$. Then, $\mathfrak{B}_\mathrm{i}(\mathrm{E}) \subset \mathfrak{B}_\mathrm{i}(\mathrm{A}_2) \subset \mathfrak{B}_\mathrm{i}(\mathrm{A}_1)$; hence, E is compatible with $\mathcal{C}_1$ and the first condition in Definition 3 is satisfied. On the other hand, due to Theorem 2, we have that $\mathfrak{B}_\mathrm{o}(\mathrm{A}_1 \wedge \Sigma) \subset \mathfrak{B}_\mathrm{o}(\Gamma_1) \subset \mathfrak{B}_\mathrm{o}(\Gamma_2)$. As $\mathfrak{B}_\mathrm{i}(\mathrm{A}_2) \subset \mathfrak{B}_\mathrm{i}(\mathrm{A}_1)$, it follows that $\mathfrak{B}_\mathrm{o}(\mathrm{A}_2 \wedge \Sigma) \subset \mathfrak{B}_\mathrm{o}(\mathrm{A}_1 \wedge \Sigma)$ and, thus, $\mathfrak{B}_\mathrm{o}(\mathrm{A}_2 \wedge \Sigma) \subset \mathfrak{B}_\mathrm{o}(\Gamma_2)$. This implies that Σ implements $\mathcal{C}_2$ and the second condition in Definition 3 is also satisfied, that is, $\mathcal{C}_1$ refines $\mathcal{C}_2$.

Conversely, suppose that $\mathcal{C}_1$ refines $\mathcal{C}_2$. As A_2 is compatible with $\mathcal{C}_2$, from the first condition in Definition 3, we get that A_2 is compatible with $\mathcal{C}_1$ and, thus, $\mathfrak{B}_\mathrm{i}(\mathrm{A}_2) \subset \mathfrak{B}_\mathrm{i}(\mathrm{A}_1)$. On the other hand, if Σ is autonomous, then

$$\mathfrak{B}_\mathrm{o}(\mathrm{A}_1 \wedge \Sigma) = \mathfrak{B}_\mathrm{o}(\Sigma) = \mathfrak{B}_\mathrm{o}(\mathrm{A}_2 \wedge \Sigma),$$

hence, by Theorem 2, Σ implements $\mathcal{C}_i$, $i \in \{1, 2\}$, if and only if $\mathfrak{B}_\mathrm{o}(\Sigma) \subset \mathfrak{B}_\mathrm{o}(\Gamma_i)$. Therefore, from the second condition in Definition 3, we get that $\mathfrak{B}_\mathrm{o}(\Sigma) \subset \mathfrak{B}_\mathrm{o}(\Gamma_1)$ implies $\mathfrak{B}_\mathrm{o}(\Sigma) \subset \mathfrak{B}_\mathrm{o}(\Gamma_2)$ for all autonomous Σ, and thus, $\mathfrak{B}_\mathrm{o}(\Gamma_1) \subset \mathfrak{B}_\mathrm{o}(\Gamma_2)$ due to Lemma 3. This shows that (36) holds. ■

Remark 4: The sufficiency of the conditions in (36) is fairly easy to see. However, their necessity is somewhat surprising. In particular, the fact that the inclusion $\mathfrak{B}_\mathrm{o}(\Gamma_1) \subset \mathfrak{B}_\mathrm{o}(\Gamma_2)$ is necessary indicates that the satisfaction of the second property in Definition 3 does not depend on the assumptions of either contract, even though their classes of implementations do, as can be seen from Theorem 2. This is because the subclasses of autonomous implementations are independent of the assumptions, and rich enough to necessitate that $\mathfrak{B}_\mathrm{o}(\Gamma_1) \subset \mathfrak{B}_\mathrm{o}(\Gamma_2)$, as can be seen from Lemma 3.

Remark 5: Refinement defines a preorder, as can be easily verified from the definition. In view of Theorem 4, $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ refines $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ and vice versa if and only if $\mathfrak{B}_\mathrm{i}(\mathrm{A}_1) = \mathfrak{B}_\mathrm{i}(\mathrm{A}_2)$ and $\mathfrak{B}_\mathrm{o}(\Gamma_1) = \mathfrak{B}_\mathrm{o}(\Gamma_2)$. Since the latter might hold even if $\mathrm{A}_1 \neq \mathrm{A}_2$ or $\Gamma_1 \neq \Gamma_2$, it follows that refinement does not define a partial order. Nevertheless, the greatest lower bound of two contracts always exists. It is typically referred to as the *conjunction* of contracts, which is treated in [33]. The least upper bound also exists, and can be found similarly to the greatest lower bound.

We will illustrate how Theorem 4 can be used in practice with a simple example.

Example 2: Consider the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ with

$$\mathrm{A}_1 : A_1\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u = 0 \qquad \Gamma_1 : G_1\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = 0, \tag{37}$$

$$\mathrm{A}_2 : A_2\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u = 0 \qquad \Gamma_2 : G_2\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = 0, \tag{38}$$

and $A_1(s)$, $A_2(s)$, $G_1(s)$, and $G_2(s)$ given by

$$A_1(s) = \begin{bmatrix} s^3 - 2s^2 - s + 2 & s^2 - s - 2 \end{bmatrix}, \tag{39}$$

$$A_2(s) = \begin{bmatrix} s^2 - 1 & s + 1 \end{bmatrix}, \tag{40}$$

$$G_1(s) = s^3 + s^2 + s + 1, \tag{41}$$

$$G_2(s) = s^4 - 1. \tag{42}$$

To find out whether $\mathcal{C}_1$ refines $\mathcal{C}_2$ using Theorem 4, we need to check if $\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma_2)$ and $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$.

In view of Theorem 1, we have that $\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma_2)$ if and only if $G_2(s) = M(s)G_1(s)$ for some polynomial $M(s)$. Since $G_1(s)$ is a nonzero polynomial, the latter holds if and only if $M(s) = G_2(s)G_1(s)^{-1}$ is a polynomial, which is the case because $G_2(s)G_1(s)^{-1} = s - 1$.

On the other hand, we have that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ if and only if there exists a polynomial matrix $N(s)$ such that $A_1(s) = N(s)A_2(s)$. We will make use of [33, Lemma 1] to establish if such a polynomial matrix $N(s)$ exists. To do this, we first need to bring $A_2(s)$ to its Smith form. Note that adding $s-1$ times the second column to the first column of $A_2(s)$ and interchanging the columns of the resulting matrix yields $\begin{bmatrix} s+1 & 0 \end{bmatrix}$, which is in Smith form. Therefore,

$$A_2(s) = U(s) \begin{bmatrix} D(s) & 0 \end{bmatrix} V(s) \tag{43}$$

for $U(s) = 1$, $D(s) = s + 1$ and

$$V(s)^{-1} = \begin{bmatrix} 1 & 0 \\ s-1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & s-1 \end{bmatrix}. \tag{44}$$

Then, [33, Lemma 1] tells us that there exists a polynomial matrix $N(s)$ such that $A_1(s) = N(s)A_2(s)$ if and only if:

1) $A_1(s)V(s)^{-1} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 0$;
2) $A_1(s)V(s)^{-1} \begin{bmatrix} D(s)^{-1} \\ 0 \end{bmatrix}$ is a polynomial.

It is easily seen that both items hold since

$$A_1(s)V(s)^{-1} = \begin{bmatrix} s^2 - s - 2 & 0 \end{bmatrix} = D(s) \begin{bmatrix} s-2 & 0 \end{bmatrix}, \tag{45}$$

hence, there exists a polynomial matrix $N(s)$ such that $A_1(s) = N(s)A_2(s)$, and thus $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$. In conclusion, we have that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ and $\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma_2)$, hence $\mathcal{C}_1$ refines $\mathcal{C}_2$ due to Theorem 4.

IV. Projection, Intersection, and Product

In this section, we define three operations on behaviors and the systems representing them, namely, projection, intersection, and product. These will play a role in characterizing contract composition in the next section. In particular, when defining contract composition, we will consider interconnections of systems, where only parts of the inputs and outputs are used for the interconnection. This will inevitably lead us to consider projections, intersections, and products.

With this in mind, consider the behavior

$$\mathfrak{B} = \left\{ w \in \mathcal{C}_k^\infty \;\middle|\; R\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) w = 0 \right\}$$

and the partitioning $w = (w_1, w_2)$. We denote the *projection* of $\mathfrak{B}$ on w_1 or w_2 as $\Pi_1\mathfrak{B}$ or $\Pi_2\mathfrak{B}$, respectively. More precisely, if $w_1 \in \mathcal{C}_{k_1}^\infty$ and $w_2 \in \mathcal{C}_{k_2}^\infty$, then we define

$$\Pi_1\mathfrak{B} = \left\{ w_1 \in \mathcal{C}_{k_1}^\infty \;\middle|\; \exists w_2 \in \mathcal{C}_{k_2}^\infty \text{ s.t. } (w_1, w_2) \in \mathfrak{B} \right\},$$

$$\Pi_2\mathfrak{B} = \left\{ w_2 \in \mathcal{C}_{k_2}^\infty \;\middle|\; \exists w_1 \in \mathcal{C}_{k_1}^\infty \text{ s.t. } (w_1, w_2) \in \mathfrak{B} \right\}.$$

In view of [13, Th. 6.2.6], there exist polynomial matrices $R^{\pi_1}(s)$ and $R^{\pi_2}(s)$ satisfying

$$\Pi_j\mathfrak{B} = \left\{ w_j \in \mathcal{C}_{k_j}^\infty \;\middle|\; R^{\pi_j}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) w_j = 0 \right\}, \quad j \in \{1, 2\}.$$

Remark 6: Checking if a projection of the behavior $\mathfrak{B}$ is contained in another behavior $\mathfrak{B}_1$ can be done by using Theorem 1 without explicitly constructing a representation of the projection of $\mathfrak{B}$. For example, suppose that we have to check if $\Pi_1\mathfrak{B} \subset \mathfrak{B}_1$, where

$$\mathfrak{B}_1 = \left\{ w_1 \in \mathcal{C}_{k_1}^\infty \;\middle|\; R_1\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) w_1 = 0 \right\}. \tag{46}$$

Naively using Theorem 1 to do this would require the construction of $R^{\pi_1}(s)$. We can avoid this by using the fact that $\Pi_1\mathfrak{B} \subset \mathfrak{B}_1$ if and only if $\mathfrak{B} \subset \mathfrak{B}_1^e$, where

$$\mathfrak{B}_1^e = \left\{ w \in \mathcal{C}_k^\infty \;\middle|\; \begin{bmatrix} R_1\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) & 0 \end{bmatrix} w = 0 \right\} \tag{47}$$

is the extension of $\mathfrak{B}_1$ to the full external variable w. Using Theorem 1, $\mathfrak{B} \subset \mathfrak{B}_1^e$ if and only if there exists a polynomial matrix $M(s)$ such that

$$\begin{bmatrix} R_1(s) & 0 \end{bmatrix} = M(s)R(s). \tag{48}$$

Therefore, to check if $\Pi_1\mathfrak{B} \subset \mathfrak{B}_1$, we can check if there exists a polynomial matrix $M(s)$ such that (48) holds, which does not require the explicit construction of $R^{\pi_1}(s)$.

On the other hand, we denote the *intersection* of $\mathfrak{B}$ with $w_2 = 0$ or $w_1 = 0$ by $\mathrm{I}_1\mathfrak{B}$ or $\mathrm{I}_2\mathfrak{B}$, respectively. More precisely, we define

$$\mathrm{I}_1\mathfrak{B} = \left\{ w_1 \in \mathcal{C}_{k_1}^\infty \;\middle|\; (w_1, 0) \in \mathfrak{B} \right\},$$

$$\mathrm{I}_2\mathfrak{B} = \left\{ w_2 \in \mathcal{C}_{k_2}^\infty \;\middle|\; (0, w_2) \in \mathfrak{B} \right\}.$$

It is easily verified that

$$\mathrm{I}_j\mathfrak{B} = \left\{ w_j \in \mathcal{C}_{k_j}^\infty \;\middle|\; R^{i_j}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) w_j = 0 \right\}, \quad j \in \{1, 2\},$$

where $R^{i_1}(s)$ and $R^{i_1}(s)$ are polynomial matrices that partition $R(s)$ as $R(s) = \begin{bmatrix} R^{i_1}(s) & R^{i_2}(s) \end{bmatrix}$.

The projection and intersection operations on behaviors and the polynomial matrices that represent them can straightforwardly be extended to operations on *systems*. The following definition does so for assumptions and guarantees.

Definition 4: Consider the assumptions A given by (9), and the partition $u = (u_1, u_2)$. For $j \in \{1, 2\}$, the projected assumptions $\Pi_j\mathrm{A}$ and the intersected assumptions $\mathrm{I}_j\mathrm{A}$ are defined as

$$\Pi_j\mathrm{A} : A^{\pi_j}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u = 0 \quad \text{and} \quad \mathrm{I}_j\mathrm{A} : A^{i_j}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u = 0.$$

Consider the guarantees Γ given by (10), and the partition $y = (y_1, y_2)$. For $j \in \{1, 2\}$, the projected guarantees $\Pi_j\Gamma$ and the intersected guarantees $\mathrm{I}_j\Gamma$ are defined as

$$\Pi_j\Gamma : G^{\pi_j}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = 0 \quad \text{and} \quad \mathrm{I}_j\Gamma : G^{i_j}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = 0.$$

Finally, we define the *product* of systems as a representation of the Cartesian product of their behaviors. This is done for assumptions and guarantees in the following definition.

Definition 5: Consider the assumptions A_1 and A_2, and the guarantees Γ_1 and Γ_2, given by (37) and (38). The product assumptions $\mathrm{A}_1 \times \mathrm{A}_2$ are defined as

$$\mathrm{A}_1 \times \mathrm{A}_2 : 0 = \begin{bmatrix} A_1\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) & 0 \\ 0 & A_2\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \end{bmatrix} u, \tag{49}$$

and the product guarantees $\Gamma_1 \times \Gamma_2$ are defined as

$$\Gamma_1 \times \Gamma_2 : \begin{bmatrix} G_1\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) & 0 \\ 0 & G_2\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \end{bmatrix} y = 0. \tag{50}$$

It is easily seen that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \times \mathrm{A}_2) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \times \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ and $\mathfrak{B}_{\mathrm{o}}(\Gamma_1 \times \Gamma_2) = \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_2)$.

V. Composition

In order to facilitate the independent design of components within interconnected systems, we will introduce methods for contract composition. Loosely speaking, our goal is to answer the following question: Given implementations Σ_1 and Σ_2 of the contracts $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, what contract does the interconnection of Σ_1 and Σ_2 implement? Naturally, the answer to this question depends on the type of interconnection that is considered. In this article, we consider two types of interconnection, namely, the series interconnection and the feedback interconnection. The definitions of these interconnections are fairly general, which will ultimately allow us to analyze and design a large class of interconnected systems by decomposing them into a sequence of series and feedback interconnections. Before we proceed to defining and characterizing the corresponding contract compositions, we will briefly discuss how they enable the independent design of components within interconnected systems.

A. Interconnected System Design

When designing an interconnected system, a designer starts with a given specification for the overall system in the form of a contract $\mathcal{C}$. As a simple example, suppose that this contract $\mathcal{C}$ needs to be implemented by an interconnection of two systems Σ_1 and Σ_2, denoted by $\Sigma_1 \otimes \Sigma_2$. These systems often need to be developed independently, possibly by different developers. Therefore, the goal of the designer is to assign specifications for Σ_1 and Σ_2, in the form of contracts $\mathcal{C}_1$ and $\mathcal{C}_2$, such that the following property holds: if Σ_1 implements $\mathcal{C}_1$ and Σ_2 implements $\mathcal{C}_2$, then the interconnection $\Sigma_1 \otimes \Sigma_2$ implements $\mathcal{C}$. Indeed, then each developer is only concerned with developing an implementation of their assigned contract and need not concern themselves with the development of the implementation of the other contract. In other words, the correct choice of $\mathcal{C}_1$ and $\mathcal{C}_2$ ensures that the interconnected system implements the overall contract $\mathcal{C}$.

With an appropriate notion of contract composition, the designer can ensure that if Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, then the interconnection $\Sigma_1 \otimes \Sigma_2$ implements the composition $\mathcal{C}_1 \otimes \mathcal{C}_2$, where the definition of $\mathcal{C}_1 \otimes \mathcal{C}_2$ mirrors that of $\Sigma_1 \otimes \Sigma_2$. To ensure that $\Sigma_1 \otimes \Sigma_2$ implements $\mathcal{C}$ as well, the designer can make use of the notion of contract refinement. In particular, the designer can design $\mathcal{C}_1$ and $\mathcal{C}_2$ such that $\mathcal{C}_1 \otimes \mathcal{C}_2$ refines $\mathcal{C}$. Then, any implementation of $\mathcal{C}_1 \otimes \mathcal{C}_2$ implements $\mathcal{C}$ as well, thus $\Sigma_1 \otimes \Sigma_2$ implements $\mathcal{C}$. The following example makes these ideas a bit more concrete.

Example 3: Consider the interconnection of Σ_1 and Σ_2 depicted in Fig. 4. Suppose that we want this interconnection to implement the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ with A as in (9), Γ as in (10), and $A(s)$ and $G(s)$ given by

$$A(s) = \begin{bmatrix} s+1 & 0 \\ 0 & s \end{bmatrix}, \quad G(s) = \begin{bmatrix} s^2 - 1 & s^2 + 3s \end{bmatrix}. \tag{51}$$

Our goal is to do this by allowing Σ_1 and Σ_2 to be developed independently. In other words, our goal is to determine contracts $\mathcal{C}_1$ and $\mathcal{C}_2$ such that the interconnection of Σ_1 and Σ_2 is guaranteed to implement $\mathcal{C}$ whenever Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. In the next section, we will show that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ with

$$\mathrm{A}_1 : A_1\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u_1 = 0, \qquad \Gamma_1 : G_1\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y_1 = 0, \tag{52}$$

$$\mathrm{A}_2 : A_2\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u_2 = 0, \qquad \Gamma_2 : G_2\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y_2 = 0, \tag{53}$$

and $A_1(s)$, $G_1(s)$, $A_2(s)$, and $G_2(s)$ given by

$$A_1(s) = s + 1, \tag{54}$$

$$G_1(s) = \begin{bmatrix} s & -1 \\ s+1 & -s-1 \end{bmatrix}, \tag{55}$$

$$A_2(s) = \begin{bmatrix} s^2 - 1 & s \end{bmatrix}, \tag{56}$$

$$G_2(s) = s^2 + 3s, \tag{57}$$

achieve our goal. This will be done in Example 4.

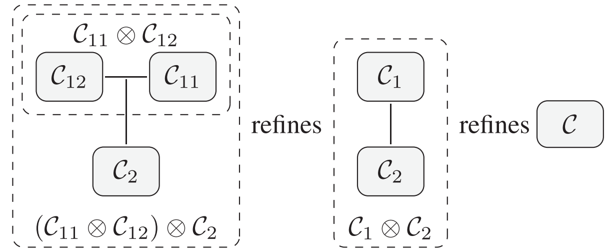


Fig. 3. Interconnected system design with contracts.

The ideas presented so far can be taken even further. If the notion of contract composition is such that $\mathcal{C}_1' \otimes \mathcal{C}_2'$ refines $\mathcal{C}_1 \otimes \mathcal{C}_2$ whenever $\mathcal{C}_1'$ refines $\mathcal{C}_1$ and $\mathcal{C}_2'$ refines $\mathcal{C}_2$, then individual developers can also design interconnected systems to implement their assigned contracts. For example, the first developer can design $\mathcal{C}_{11}$ and $\mathcal{C}_{12}$ such that $\mathcal{C}_{11} \otimes \mathcal{C}_{12}$ refines $\mathcal{C}_1$, and since $\mathcal{C}_2$ refines itself, this would imply that $(\mathcal{C}_{11} \otimes \mathcal{C}_{12}) \otimes \mathcal{C}_2$ refines $\mathcal{C}_1 \otimes \mathcal{C}_2$, which in turn refines $\mathcal{C}$, as illustrated in Fig. 3. Then, instead of developing an implementation Σ_1 of $\mathcal{C}_1$, the first developer can develop implementations Σ_{11} and Σ_{12} of $\mathcal{C}_{11}$ and $\mathcal{C}_{12}$, respectively, and the interconnection $(\Sigma_{11} \otimes \Sigma_{12}) \otimes \Sigma_2$ would be guaranteed to implement the overall contract $\mathcal{C}$.

We conclude this section by noting that the use of contracts for the design of interconnected systems greatly simplifies component substitution. Indeed, if one wants to replace the component Σ_{11} with a new component Σ_{11}' while still ensuring that the interconnection $(\Sigma_{11}' \otimes \Sigma_{12}) \otimes \Sigma_2$ implements the overall contract $\mathcal{C}$, then it is enough to verify that Σ_{11}' implements $\mathcal{C}_{11}$. In particular, it is not necessary to verify that $(\Sigma_{11}' \otimes \Sigma_{12}) \otimes \Sigma_2$ implements $\mathcal{C}$, which can be much more difficult due to the high complexity of $(\Sigma_{11}' \otimes \Sigma_{12}) \otimes \Sigma_2$ as compared with Σ_{11}'.

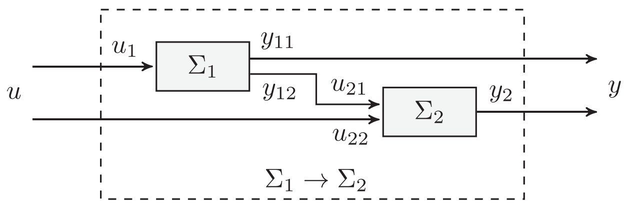


Fig. 4. Series interconnection $\Sigma_1 \to \Sigma_2$.

B. Series Composition

We will first consider the series interconnection. We will begin by defining the series interconnection of two systems and the corresponding notion or series composition of two contracts. We will then characterize the latter, which will lead us to necessary and sufficient conditions for the existence of the series composition of contracts, and an explicit expression for it when it exists.

Let Σ_1 and Σ_2 be systems of the form (3) in input–output form. Typically, the series interconnection of Σ_1 to Σ_2 is obtained by setting the output of Σ_1 as input of Σ_2. In this article, we will consider a slightly more general type of series interconnection, where we set *part* of the output of Σ_1 as *part* of the input of Σ_2.

Definition 6: Denote the input and output of Σ_1 by u_1 and y_1, respectively, and the input and output of Σ_2 by u_2 and y_2, respectively. Suppose that y_1 is partitioned as $y_1 = (y_{11}, y_{12})$, and u_2 as $u_2 = (u_{21}, u_{22})$, where y_{12} has the same dimension as u_{21}. The *series interconnection* of Σ_1 to Σ_2, denoted by $\Sigma_1 \to \Sigma_2$, is obtained by setting $y_{21} = u_{21}$, as shown in Fig. 4. The input of $\Sigma_1 \to \Sigma_2$ is given by (u_1, u_{22}), and the output by (y_{11}, y_2).

Following the metatheory in [12], we define the series composition of contracts as follows.

Definition 7: The *series composition* of the contract $\mathcal{C}_1$ to the contract $\mathcal{C}_2$, denoted by $\mathcal{C}_1 \to \mathcal{C}_2$, is the *smallest* (with respect to refinement) contract $\mathcal{C}$ that satisfies the following implication: if Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and E is an environment compatible with $\mathcal{C}$, then:

1) the environment of Σ_1 in $\mathrm{E} \wedge (\Sigma_1 \to \Sigma_2)$ is compatible with $\mathcal{C}_1$;
2) the environment of Σ_2 in $\mathrm{E} \wedge (\Sigma_1 \to \Sigma_2)$ is compatible with $\mathcal{C}_2$;
3) $\Sigma_1 \to \Sigma_2$ implements $\mathcal{C}_1 \to \mathcal{C}_2$.

The definition of the series composition $\mathcal{C}_1 \to \mathcal{C}_2$ has the following aspects. First, $\mathcal{C}_1 \to \mathcal{C}_2$ must satisfy properties that would support independent development, as described in Section V-A. Second, $\mathcal{C}_1 \to \mathcal{C}_2$ must be the smallest contract that satisfies these properties. In view of Theorem 4, this means that the $\mathcal{C}_1 \to \mathcal{C}_2$ assumes the least while still ensuring that the components of $\Sigma_1 \to \Sigma_2$ operate in interconnection with environments compatible with their respective contracts, and guarantees the most while still ensuring that $\Sigma_1 \to \Sigma_2$ is an implementation.

The series composition does not necessarily exist. On the one hand, a contract that satisfies the implementation in Definition 7 might not exist. On the other hand, even if such a contract exists, the smallest one might not exist. In the following, we will show that a contract that satisfies the implication in Definition 7 does exists under certain conditions, and when these conditions are met, the smallest such contract also exists.

Definition 7 is quite abstract in its current form. To make it more concrete, recall that the environment of a system is another system that generates inputs for it. Therefore, if $\mathcal{C} = (\mathrm{A}, \Gamma)$, $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$, and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$, then the conditions in Definition 7 hold if and only if the input of Σ_1 in $\mathrm{E} \wedge (\Sigma_1 \to \Sigma_2)$ is contained in $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$, the input of Σ_2 in $\mathrm{E} \wedge (\Sigma_1 \to \Sigma_2)$ is contained in $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$, and the output of Σ_2 in $\mathrm{E} \wedge (\Sigma_1 \to \Sigma_2)$ is contained in $\mathfrak{B}_{\mathrm{o}}(\Gamma)$. In view of the interconnection structure of $\Sigma_1 \to \Sigma_2$, which is depicted in Fig. 4, these conditions hold if and only if the following implication holds:

$$\left.\begin{array}{r}(u_1, u_{22}) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{E}) \\ (u_1, y_{11}, u_{21}) \in \mathfrak{B}(\Sigma_1) \\ (u_{21}, u_{22}, y_2) \in \mathfrak{B}(\Sigma_2)\end{array}\right\} \Rightarrow \left\{\begin{array}{l}u_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \\ (u_{21}, u_{22}) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \\ (y_{11}, y_2) \in \mathfrak{B}_{\mathrm{o}}(\Gamma).\end{array}\right. \tag{58}$$

Stated differently, the implication in Definition 7 is satisfied if and only if the implication (58) is satisfied for all Σ_1, Σ_2, and E such that Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and E is compatible with $\mathcal{C}$. While the latter is certainly more concrete, it still does not clarify what conditions A and Γ should satisfy in order for $\mathcal{C}$ to satisfy the implication in Definition 7. To determine these, we can make use of *autonomous* implementations and Lemma 3 again. The subclass of autonomous implementations is rich enough to yield necessary and sufficient conditions for the satisfactions of the implication in Definition 7, as it was for refinement, see Remark 4. In particular, by restricting ourselves to autonomous implementations, we can obtain necessary conditions for the satisfaction of the implication in Definition 7, which we can then show to be sufficient, even without the restriction to autonomous implementations. This is done in the following lemma, whose proof can be found in the Appendix.

Lemma 5: Suppose that $\mathcal{C} = (\mathrm{A}, \Gamma)$, $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$, and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$. Then, the implication in Definition 7 is satisfied if and only if

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \times \mathrm{I}_2 \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2), \tag{59}$$

$$\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathrm{I}_1 \mathfrak{B}_{\mathrm{o}}(\Gamma) \times \mathrm{I}_1 \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2), \tag{60}$$

$$\mathfrak{B}_{\mathrm{o}}(\Gamma_2) \subset \mathrm{I}_2 \mathfrak{B}_{\mathrm{o}}(\Gamma). \tag{61}$$

Note that the conditions in Lemma 5 are in terms of A and Γ only, i.e., they do not refer to implementations or compatible environments. Furthermore, while (59) and (61) strongly depend on $\mathcal{C}$, (60) is partially independent of it. Indeed, (60) holds only if $\Pi_2 \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathrm{I}_1 \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$, and the latter depends solely on $\mathcal{C}_1$ and $\mathcal{C}_2$. This suggests that the inclusion $\Pi_2 \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathrm{I}_1 \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ is a necessary condition for the existence of $\mathcal{C}_1 \to \mathcal{C}_2$. This turns out to be true. In fact, the following theorem, which is the main result of this section, shows that this condition is both necessary and sufficient for the existence of $\mathcal{C}_1 \to \mathcal{C}_2$, and provides an explicit expression for $\mathcal{C}_1 \to \mathcal{C}_2$ when it exists.

Theorem 6: The series composition of $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ to $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ exists if and only if

$$\Pi_2 \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathrm{I}_1 \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2). \tag{62}$$

If the series composition exists, then it is given by

$$\mathcal{C}_1 \to \mathcal{C}_2 = (\mathrm{A}_1 \times \mathrm{I}_2 \mathrm{A}_2, \Pi_1 \Gamma_1 \times \Gamma_2). \tag{63}$$

Proof: We begin by proving necessity of (62). Suppose that the series composition $\mathcal{C}_1 \to \mathcal{C}_2$ exists. Then, there exists a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies the implication in Definition 7. Due to Lemma 5, this implies that (60) holds and, thus, $\Pi_2 \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathrm{I}_1 \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$.

We proceed by proving sufficiency of (62). Suppose that (62) holds and let $\mathcal{C} = (\mathrm{A}, \Gamma)$. We will show that (59), (60), and (61) hold if and only if

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \times \mathrm{I}_2\mathrm{A}_2), \tag{64}$$

$$\mathfrak{B}_{\mathrm{o}}(\Pi_1\Gamma_1 \times \Gamma_2) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma). \tag{65}$$

To this end, note that (59) is equivalent to (64) because $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \times \mathrm{I}_2\mathrm{A}_2) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \times \mathrm{I}_2\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$, as follows from Definitions 4 and 5. On the other hand, under the assumption that (62) holds, we have that (60) is equivalent to $\Pi_1\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathrm{I}_1\mathfrak{B}_{\mathrm{i}}(\Gamma)$. Then, it is immediate that (60) and (61) both hold if and only if

$$\mathfrak{B}_{\mathrm{o}}(\Pi_1\Gamma_1 \times \Gamma_2) \subset \mathrm{I}_1\mathfrak{B}_{\mathrm{o}}(\Gamma) \times \mathrm{I}_2\mathfrak{B}_{\mathrm{o}}(\Gamma), \tag{66}$$

where we used $\mathfrak{B}_{\mathrm{o}}(\Pi_1\Gamma_1 \times \Gamma_2) = \Pi_1\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_2)$.

We claim that (66) holds if and only if (65) holds. It is easily seen that $\mathrm{I}_1\mathfrak{B}_{\mathrm{o}}(\Gamma) \times \mathrm{I}_2\mathfrak{B}_{\mathrm{o}}(\Gamma) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma)$, which shows that (66) implies (65). To show the converse, suppose that (65) holds and let $(y_{11}, y_2) \in \mathfrak{B}_{\mathrm{o}}(\Pi_1\Gamma_1 \times \Gamma_2)$. This implies that $y_{11} \in \mathfrak{B}_{\mathrm{o}}(\Pi_1\Gamma_1)$ and $y_2 \in \mathfrak{B}_{\mathrm{o}}(\Gamma_2)$. But $0 \in \mathfrak{B}_{\mathrm{o}}(\Gamma_2)$ and $0 \in \mathfrak{B}_{\mathrm{o}}(\Pi_1\Gamma_1)$; hence, $(y_{11}, 0) \in \mathfrak{B}_{\mathrm{o}}(\Pi_1\Gamma_1 \times \Gamma_2)$ and $(0, y_2) \in \mathfrak{B}_{\mathrm{o}}(\Pi_1\Gamma_1 \times \Gamma_2)$. Since (65) holds, it follows that $(y_{11}, 0) \in \mathfrak{B}_{\mathrm{o}}(\Gamma)$ and $(0, y_2) \in \mathfrak{B}_{\mathrm{o}}(\Gamma)$, which yields $y_{11} \in \mathrm{I}_1\mathfrak{B}_{\mathrm{o}}(\Gamma)$ and $y_2 \in \mathrm{I}_2\mathfrak{B}_{\mathrm{o}}(\Gamma)$. Then, $(y_{11}, y_2) \in \mathrm{I}_1\mathfrak{B}_{\mathrm{o}}(\Gamma) \times \mathrm{I}_2\mathfrak{B}_{\mathrm{o}}(\Gamma)$ and thus (66) holds.

We now know that (59) is equivalent to (64), and (60) and (61) together are equivalent to (65). Due to Theorem 4, (64) and (65) hold if and only if $\mathcal{C}$ refines $\mathcal{C}_1 \to \mathcal{C}_2$, with $\mathcal{C}_1 \to \mathcal{C}_2$ as defined in (63). In view of Lemma 5, this means that $\mathcal{C}$ satisfies the implication in Definition 7 if and only if $\mathcal{C}$ refines $\mathcal{C}_1 \to \mathcal{C}_2$; hence, $\mathcal{C}_1 \to \mathcal{C}_2$ is the smallest contract that satisfies the implication in Definition 7, that is, $\mathcal{C}_1 \to \mathcal{C}_2$ is indeed the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$. ■

The condition (62) in Theorem 6 is quite intuitive. It effectively says that any output behavior that an implementation of $\mathcal{C}_1$ can generate must be behavior that an environment compatible with $\mathcal{C}_2$ can generate. Nevertheless, it is still surprising that this condition is both necessary and sufficient. In fact, the necessity of (62) follows only because of the existence of autonomous implementations, which is the case because guarantees specify only an output behavior, rather than a relation between inputs and outputs.

To see how Theorem 6 can be used in practice, consider the following example.

Example 4: We continue from the end of Example 3. Note that the output of Σ_1 is partitioned into two single outputs as $y_1 = (y_{11}, y_{12})$, and the input of Σ_2 is partitioned into two single inputs as $u_2 = (u_{21}, u_{22})$. The series interconnection $\Sigma_1 \to \Sigma_2$ is obtained by setting $y_{12} = u_{21}$, and has (u_1, u_{22}) as input and (y_{11}, y_2) as output. To check whether the series composition $\mathcal{C}_1 \to \mathcal{C}_2$ exists, we need to check whether (62) holds. In view of Remark 6, we can do this using Theorem 1 without constructing an explicit representation of $\Pi_2\mathfrak{B}_{\mathrm{o}}(\Gamma_1)$. In particular, since

$$\mathrm{I}_1\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) = \left\{ u_{21} \in \mathcal{C}_1^\infty \;\middle|\; A_2^{i_1}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u_{21} = 0 \right\}, \tag{67}$$

where $A_2^{i_1}(s) = s^2 - 1$ is the first entry of $A_2(s)$, it follows that (62) holds if and only if

$$\begin{bmatrix} 0 & A_2^{i_1}(s) \end{bmatrix} = M(s)G_1(s) \tag{68}$$

for some polynomial matrix $M(s)$. But $G_1(s)$ is invertible; hence, (68) holds if and only if $\begin{bmatrix} 0 & A_2^{i_1}(s) \end{bmatrix} G_1(s)^{-1}$ is a polynomial matrix. We can compute

$$\begin{bmatrix} 0 & A_2^{i_1}(s) \end{bmatrix} G_1(s)^{-1} = \begin{bmatrix} 0 & s^2 - 1 \end{bmatrix} \begin{bmatrix} \frac{1}{s-1} & -\frac{1}{s^2-1} \\ \frac{1}{s-1} & -\frac{s}{s^2-1} \end{bmatrix} \tag{69}$$

$$= \begin{bmatrix} s+1 & -s \end{bmatrix}, \tag{70}$$

which shows that (68) holds. This implies that (62) holds and thus the series composition $\mathcal{C}_1 \to \mathcal{C}_2$ exists.

Now, (63) provides an explicit expression for $\mathcal{C}_1 \to \mathcal{C}_2$. It is easily seen that the assumptions of $\mathcal{C}_1 \to \mathcal{C}_2$ are given by

$$\mathrm{A}_1 \times \mathrm{I}_2\mathrm{A}_2 : 0 = \vec{A}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u, \tag{71}$$

where

$$\vec{A}(s) = \begin{bmatrix} A_1(s) & 0 \\ 0 & A_2^{i_2}(s) \end{bmatrix} = \begin{bmatrix} s+1 & 0 \\ 0 & s \end{bmatrix}. \tag{72}$$

On the other hand, to find the guarantees of $\mathcal{C}_1 \to \mathcal{C}_2$, we first need a description of $\Pi_1\Gamma_1$, or, more specifically, an expression for $G_1^{\pi_1}(s)$. To this end, note that

$$U(s) = \begin{bmatrix} 1 & 0 \\ -s-1 & 1 \end{bmatrix} \tag{73}$$

is a unimodular matrix such that

$$U(s)G_1(s) = \begin{bmatrix} s & -1 \\ -s^2+1 & 0 \end{bmatrix}, \tag{74}$$

hence $G_1^{\pi_1}(s) = -s^2 + 1$ due to [13, Th. 6.2.6]. Then, it follows that the guarantees of $\mathcal{C}_1 \to \mathcal{C}_2$ are given by

$$\Pi_1\Gamma_1 \times \Gamma_2 : \vec{G}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = 0, \tag{75}$$

where

$$\vec{G}(s) = \begin{bmatrix} G_1^{\pi_1}(s) & 0 \\ 0 & G_2(s) \end{bmatrix} = \begin{bmatrix} -s^2+1 & 0 \\ 0 & s^2+3s \end{bmatrix}. \tag{76}$$

Finally, note that $\vec{A}(s) = A(s)$ and

$$G(s) = \begin{bmatrix} -1 & 1 \end{bmatrix} \vec{G}(s). \tag{77}$$

In view of Theorem 1, this means that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \times \mathrm{I}_2\mathrm{A}_2)$ and $\mathfrak{B}_{\mathrm{o}}(\Pi_1\Gamma_1 \times \Gamma_2) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma)$. Therefore, due to Theorem 4, $\mathcal{C}_1 \to \mathcal{C}_2$ refines $\mathcal{C}$, and thus $\Sigma_1 \to \Sigma_2$ implements $\mathcal{C}$ for any Σ_1 and Σ_2 that implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively.

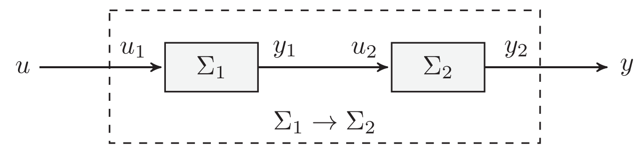


Fig. 5. Full series interconnection $\Sigma_1 \to_f \Sigma_2$.

Theorem 6 can be simplified when considering the full series interconnection. In particular, without partitioning the output of Σ_1 or the input of Σ_2, the *full series interconnection* of Σ_1 to Σ_2, denoted by $\Sigma_1 \to_f \Sigma_2$, is obtained by setting the whole output of Σ_1 as the whole input of Σ_2, as shown in Fig. 5. The corresponding *full series composition* of $\mathcal{C}_1$ to $\mathcal{C}_2$ is denoted by $\mathcal{C}_1 \rightarrow_f \mathcal{C}_2$, and its definition is the same as the one for the series composition. However, because of the simpler structure of $\Sigma_1 \rightarrow_f \Sigma_2$, (58) is reduced to the following implication:

$$\left.\begin{aligned} u_1 &\in \mathfrak{B}_{\mathrm{i}}(\mathrm{E}) \\ (u_1, u_2) &\in \mathfrak{B}(\Sigma_1) \\ (u_2, y_2) &\in \mathfrak{B}(\Sigma_2) \end{aligned}\right\} \Rightarrow \begin{cases} u_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \\ u_2 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \\ y_2 \in \mathfrak{B}_{\mathrm{o}}(\Gamma). \end{cases} \tag{78}$$

Consequently, we obtain the following corollary of Theorem 6.

Corollary 7: The full series composition of $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ to $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ exists if and only if

$$\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2). \tag{79}$$

If the full series composition exists, then it is given by

$$\mathcal{C}_1 \rightarrow_f \mathcal{C}_2 = (\mathrm{A}_1, \Gamma_2). \tag{80}$$

We conclude this section with another consequence of Theorem 6, namely, that the series composition satisfies the compositionality property described in Section V-A. This is shown in the following proposition.

Proposition 8: If $\mathcal{C}_1'$ refines $\mathcal{C}_1$, $\mathcal{C}_2'$ refines $\mathcal{C}_2$, and $\mathcal{C}_1 \rightarrow \mathcal{C}_2$ exists, then $\mathcal{C}_1' \rightarrow \mathcal{C}_2'$ exists and refines $\mathcal{C}_1 \rightarrow \mathcal{C}_2$.

Proof: For $j \in \{1, 2\}$, let $\mathcal{C}_j' = (\mathrm{A}_j,' \Gamma_j')$, $\mathcal{C}_j = (\mathrm{A}_j, \Gamma_j)$, and note that, by Theorem 4,

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_j) \subset \mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}_j'\right) \quad \text{and} \quad \mathfrak{B}_{\mathrm{o}}\left(\Gamma_j'\right) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma_j). \tag{81}$$

In view of Theorem 6 and the assumption that $\mathcal{C}_1 \rightarrow \mathcal{C}_2$ exists, it follows that (62) holds and $\mathcal{C}_1 \rightarrow \mathcal{C}_2$ is given by (63). Using (81) with (62) implies that

$$\Pi_2 \mathfrak{B}_{\mathrm{o}}(\Gamma_1') \subset \Pi_2 \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathrm{I}_1 \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathrm{I}_1 \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2'), \tag{82}$$

which shows that $\mathcal{C}_1' \rightarrow \mathcal{C}_2'$ exists and is given by

$$\mathcal{C}_1' \rightarrow \mathcal{C}_2' = (\mathrm{A}_1' \times \mathrm{I}_2 \mathrm{A}_2,' \Pi_1 \Gamma_1' \times \Gamma_2'). \tag{83}$$

Finally, (81) also implies that

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \times \mathrm{I}_2 \mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1' \times \mathrm{I}_2 \mathrm{A}_2'), \tag{84}$$

$$\mathfrak{B}_{\mathrm{o}}(\Pi_1 \Gamma_1' \times \Gamma_2') \subset \mathfrak{B}_{\mathrm{o}}(\Pi_1 \Gamma_1 \times \Gamma_2), \tag{85}$$

hence $\mathcal{C}_1' \rightarrow \mathcal{C}_2'$ refines $\mathcal{C}_1 \rightarrow \mathcal{C}_2$ due to Theorem 4. ■

The fact that the series composition satisfies the compositionality property is no coincidence. In fact, it is a key property of refinement and the series composition, and can be obtained directly from their definitions, even in the abstract metatheoretic setting in [12].

C. Feedback Composition

We will now consider the feedback interconnection. The feedback interconnection that we consider in this article is meant to capture bidirectional interconnections of stand-alone components, i.e., it does not necessarily represent the interconnection of a plant and its controller. We will begin by defining the feedback interconnection of two systems and the corresponding notion of feedback composition of two contracts. Characterizing the latter will prove to be somewhat more challenging than characterizing the series composition, but will ultimately lead to necessary and sufficient conditions for the existence of the feedback composition of contracts, and an explicit expression for it when it exists.

Let Σ_1 and Σ_2 be systems of the form (3) in input–output form. The feedback interconnection of Σ_1 to Σ_2 is obtained by setting *part* of the output of Σ_1 as the input of Σ_2, and the output of Σ_2 as *part* of the input of Σ_1.

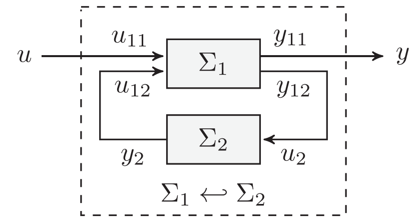


Fig. 6. Feedback interconnection $\Sigma_1 \hookleftarrow \Sigma_2$.

Definition 8: Denote the input and output of Σ_1 by u_1 and y_1, respectively, and the input and output of Σ_2 by u_2 and y_2, respectively. Suppose that u_1 and y_1 are partitioned as $u_1 = (u_{11}, u_{12})$ and $y_1 = (y_{11}, y_{12})$, where u_{12} has the same dimension as y_2, and y_{12} has the same dimension as u_2. The feedback interconnection of Σ_1 to Σ_2, denoted by $\Sigma_1 \hookleftarrow \Sigma_2$, is obtained by setting $y_{12} = u_2$ and $y_2 = u_{12}$, as shown in Fig. 6. Note that the input and output of $\Sigma_1 \hookleftarrow \Sigma_2$ are given by u_{11} and y_{11}, respectively.

Remark 7: The feedback interconnection $\Sigma_1 \hookleftarrow \Sigma_2$ can be obtained from the series interconnection $\Sigma_1 \rightarrow \Sigma_2$ by setting part of the input of $\Sigma_1 \rightarrow \Sigma_2$ equal to part of its output. In particular, without partitioning the input of Σ_2, we obtain $\Sigma_1 \rightarrow \Sigma_2$ by setting $y_{12} = u_2$. Then, the input and output of $\Sigma_1 \rightarrow \Sigma_2$ are given by (u_{11}, u_{12}) and (y_{11}, y_2), respectively, and setting $y_2 = u_{12}$ results in $\Sigma_1 \hookleftarrow \Sigma_2$.

The feedback composition of contracts is defined similarly to the series composition.

Definition 9: The *feedback composition* of a contract $\mathcal{C}_1$ to a contract $\mathcal{C}_2$, denoted by $\mathcal{C}_1 \hookleftarrow \mathcal{C}_2$, is the smallest contract $\mathcal{C}$ that satisfies the following implication: if Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, $\Sigma_1 \hookleftarrow \Sigma_2$ is in input–output form, and E is an environment compatible with $\mathcal{C}$, then:

1) the environment of Σ_1 in $\mathrm{E} \wedge (\Sigma_1 \hookleftarrow \Sigma_2)$ is compatible with $\mathcal{C}_1$;
2) the environment of Σ_2 in $\mathrm{E} \wedge (\Sigma_1 \hookleftarrow \Sigma_2)$ is compatible with $\mathcal{C}_2$;
3) $\Sigma_1 \hookleftarrow \Sigma_2$ implements $\mathcal{C}_1 \hookleftarrow \mathcal{C}_2$.

The definition of the feedback composition $\mathcal{C}_1 \hookleftarrow \mathcal{C}_2$ has the same aspects as the series composition, namely, $\mathcal{C}_1 \hookleftarrow \mathcal{C}_2$ assumes the least while still ensuring that the components of $\Sigma_1 \hookleftarrow \Sigma_2$ operate in interconnection with environments compatible with their respective contracts, and guarantees the most while still ensuring that $\Sigma_1 \hookleftarrow \Sigma_2$ is an implementation. The only difference with the series composition is in the requirement that $\Sigma_1 \hookleftarrow \Sigma_2$ is in input–output form. This is a natural requirement, especially considering that, by definition, only systems in input–output form can be implementations. This requirement was not necessary for the series composition because $\Sigma_1 \rightarrow \Sigma_2$ is guaranteed to be in input–output form if Σ_1 and Σ_2 are in input–output form. In fact, the condition that $\Sigma_1 \hookleftarrow \Sigma_2$ is in input–output form can be related to the condition of *well-posedness* in feedback interconnections, [35, Sec. 5.2]. In other words, the requirement that the feedback interconnection of two systems of the form (3) is in input–output form is equivalent to the requirement that the feedback interconnection of two systems of the form (1) is well-posed.

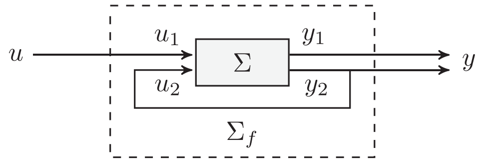


Fig. 7. System Σ_f.

We can characterize the feedback composition similarly to the series composition. Given the interconnection structure of $\Sigma_1 \hookleftarrow \Sigma_2$, we find that the conditions in Definition 9 hold if and only if the following implication holds:

$$\left.\begin{array}{r} u_{11} \in \mathfrak{B}_{\mathrm{i}}\left(\mathrm{E}\right) \\ (u_{11}, u_{12}, y_{11}, u_2) \in \mathfrak{B}\left(\Sigma_1\right) \\ (u_2, u_{12}) \in \mathfrak{B}\left(\Sigma_2\right) \end{array}\right\} \Rightarrow \begin{cases} (u_{11}, u_{12}) \in \mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}_1\right) \\ u_2 \in \mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}_2\right) \\ y_{11} \in \mathfrak{B}_{\mathrm{o}}\left(\Gamma\right). \end{cases} \tag{86}$$

We can use autonomous implementations and Lemma 3 to find what conditions A and Γ should satisfy in order for $\mathcal{C}$ to satisfy the implication in Definition 9. Similarly to the series composition, this will lead to necessary conditions for the satisfaction of the latter, namely, that

$$\mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}\right) \subset \mathrm{I}_1\mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}_1\right), \tag{87}$$

$$\mathfrak{B}_{\mathrm{o}}\left(\Gamma_1\right) \subset \mathfrak{B}_{\mathrm{o}}\left(\Gamma\right) \times \mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}_2\right), \tag{88}$$

$$\mathfrak{B}_{\mathrm{o}}\left(\Gamma_2\right) \subset \mathrm{I}_2\mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}_1\right), \tag{89}$$

where we note that (89) is independent and (88) is partially independent of A and Γ, similarly to (60). However, in contrast to the series composition, it will take more effort to show that these conditions are also sufficient. The difficulty here lies in "closing the loop" of the feedback interconnection. In Remark 7, we explained that the feedback interconnection $\Sigma_1 \hookleftarrow \Sigma_2$ can be obtained from the series interconnection $\Sigma_1 \to \Sigma_2$ by setting part of the input of $\Sigma_1 \to \Sigma_2$ as part of its output. While we understand how the behavior of $\Sigma_1 \to \Sigma_2$ relates to that of Σ_1 and Σ_2, it is not immediately clear how the behavior of $\Sigma_1 \hookleftarrow \Sigma_2$ relates to that of $\Sigma_1 \to \Sigma_2$.

To resolve this, we will first consider a simpler scenario, where only a single system is involved. Let Σ be a system of the form (3) in input–output form. Suppose that the input u and output y of Σ are partitioned as $u = (u_1, u_2)$ and $y = (y_1, y_2)$. The system Σ_f is obtained from Σ by setting $u_2 = y_2$, as shown in Fig. 7. The input and output of Σ_f are given by u_1 and (y_1, y_2), respectively. Note that, in view of Remark 2, the only difference between $\Sigma_1 \hookleftarrow \Sigma_2$ and $(\Sigma_1 \to \Sigma_2)_f$ is that output of the former is given by y_{11}, whereas the output of the latter is given by (y_{11}, y_{12}). Therefore, we can determine how the behavior of $\Sigma_1 \hookleftarrow \Sigma_2$ relates to that of $\Sigma_1 \to \Sigma_2$ by determining how the behavior of $(\Sigma_1 \to \Sigma_2)_f$ relates to that of $\Sigma_1 \to \Sigma_2$.

With this in mind, the following lemma, whose proof can be found in the Appendix, shows how the behavior of Σ_f relates to that of Σ, under a condition related to (89).

Lemma 9: If Σ implements the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$, where $\Pi_2\mathfrak{B}_{\mathrm{o}}(\Gamma) \subset \mathrm{I}_2\mathfrak{B}_{\mathrm{i}}(\mathrm{A})$, and Σ_f is in input–output form, then Σ_f implements the contract $\mathcal{C}_f = (\mathrm{I}_1\mathrm{A}, \Gamma)$.

Using Lemma 9, we can show that (87), (88), and (89) are not only necessary for $\mathcal{C}$ to satisfy the implication in Definition 9, but also sufficient. This is done in the following lemma, whose proof can also be found in the Appendix.

Lemma 10: Suppose that $\mathcal{C} = (\mathrm{A}, \Gamma)$, $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$, and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$. Then, the implication in Definition 7 is satisfied if and only if (87), (88), and (89) hold.

As already mentioned, the conditions in Lemma 10 are partially independent of $\mathcal{C}$, similarly to the conditions in Lemma 5. Indeed, (88) holds only if $\Pi_2\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$, which depends solely on $\mathcal{C}_1$ and $\mathcal{C}_2$, as does (89). This suggests that $\Pi_2\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ and $\mathfrak{B}_{\mathrm{o}}(\Gamma_2) \subset \mathrm{I}_2\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ are necessary conditions for the existence of $\mathcal{C}_1 \hookleftarrow \mathcal{C}_2$. The following theorem, which is the main result of this section, shows that these conditions are not only necessary but also sufficient for the existence of $\mathcal{C}_1 \hookleftarrow \mathcal{C}_2$, and provides an explicit expression for it when it exists.

Theorem 11: The feedback composition of $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ to $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ exists if and only if

$$\Pi_2\mathfrak{B}_{\mathrm{o}}\left(\Gamma_1\right) \subset \mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}_2\right) \quad \text{and} \quad \mathfrak{B}_{\mathrm{o}}\left(\Gamma_2\right) \subset \mathrm{I}_2\mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}_1\right). \tag{90}$$

If the feedback composition exists, then it is given by

$$\mathcal{C}_1 \hookleftarrow \mathcal{C}_2 = (\mathrm{I}_1\mathrm{A}_1, \Pi_1\Gamma_1). \tag{91}$$

Proof: We begin by proving necessity. Suppose that the feedback composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ exists. Then, there exists a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies the implication in Definition 9. From Lemma 10, it follows that (88) and (89) hold, which implies (90) holds as well.

We proceed by proving sufficiency. Suppose that (90) holds. This immediately implies that (89) holds as well. We will show that (87) and (88) hold if and only if

$$\mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}\right) \subset \mathfrak{B}_{\mathrm{i}}\left(\mathrm{I}_1\mathrm{A}_1\right), \tag{92}$$

$$\mathfrak{B}_{\mathrm{o}}\left(\Pi_1\Gamma_1\right) \subset \mathfrak{B}_{\mathrm{o}}\left(\Gamma\right). \tag{93}$$

To this end, note that (87) is equivalent to (92) by definition of $\mathrm{I}_1\mathrm{A}_1$. On the other hand, we have that (88) holds only if $\Pi_1\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma)$, which is equivalent to (93) by definition of $\Pi_1\Gamma_1$. For the converse, suppose that (93) holds, and let $(y_{11}, y_{12}) \in \mathfrak{B}_{\mathrm{o}}(\Gamma_1)$. It follows that $y_{11} \in \Pi_1\mathfrak{B}_{\mathrm{o}}(\Gamma_1)$ and $y_{12} \in \Pi_2\mathfrak{B}_{\mathrm{o}}(\Gamma_1)$; hence, $y_{11} \in \mathfrak{B}_{\mathrm{o}}(\Gamma)$ and $y_{12} \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ due to (93) and (90), respectively. In other words, we have that $(y_{11}, y_{12}) \in \mathfrak{B}_{\mathrm{o}}(\Gamma) \times \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$, which shows that (88) holds.

Now, we have shown that (87), (88), and (89) hold if and only if (92) and (93) hold. From Lemma 10, we know that (87), (88), and (89) hold if and only if the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies the implication in Definition 9. On the other hand, due to Theorem 4, (92) and (93) hold if and only if $\mathcal{C}$ refines $\mathcal{C}_1 \hookleftarrow \mathcal{C}_2$, with $\mathcal{C}_1 \hookleftarrow \mathcal{C}_2$, as defined in (91). This means that $\mathcal{C}$ satisfies the implication in Definition 9 if and only if it refines $\mathcal{C}_1 \hookleftarrow \mathcal{C}_2$; hence, $\mathcal{C}_1 \hookleftarrow \mathcal{C}_2$ is the smallest contract that satisfies the implication in Definition 9, that is, $\mathcal{C}_1 \hookleftarrow \mathcal{C}_2$ is indeed the feedback composition of $\mathcal{C}_1$ to $\mathcal{C}_2$. ■

Remark 8: In the feedback interconnection $\Sigma_1 \hookleftarrow \Sigma_2$, the component Σ_2 does not have external inputs or outputs. This allows us to focus on the main ideas in deriving Theorem 11 without being overwhelmed by technical details, but it is not essential. In fact, it might be more appropriate to define the feedback interconnection $\Sigma_1 \hookleftarrow \Sigma_2$, as shown in Fig. 8, with input and output given by (u_{11}, u_{22}) and (y_{11}, y_{22}), respectively. In such a case, the feedback composition of $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ to

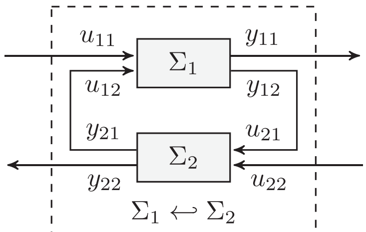


Fig. 8. General feedback interconnection $\Sigma_1 \leftrightarrow \Sigma_2$.

$\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ exists if and only if

$$\Pi_2 \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathrm{I}_1 \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \quad \text{and} \quad \Pi_1 \mathfrak{B}_{\mathrm{o}}(\Gamma_2) \subset \mathrm{I}_2 \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1), \tag{94}$$

and if the feedback composition exists, then it is given by

$$\mathcal{C}_1 \leftrightarrow \mathcal{C}_2 = (\mathrm{I}_1\mathrm{A}_1 \times \mathrm{I}_2\mathrm{A}_2, \Pi_1\Gamma_1 \times \Pi_2\Gamma_2). \tag{95}$$

The proof of this result follows the same reasoning as the proof of Theorem 11. In particular, necessity is proven using autonomous implementations, and sufficiency is proven by utilizing Lemma 9 after noting that the feedback interconnection $\Sigma_1 \leftrightarrow \Sigma_2$ can still be obtained from the series interconnection $\Sigma_1 \rightarrow \Sigma_2$, albeit in a more convoluted way than the one described in Remark 7.

Like the condition in Theorem 6, the conditions in Theorem 11 are quite intuitive. Nevertheless, showing that they are both necessary and sufficient is not straightforward. As in Theorem 6, the proof of necessity in Theorem 11 requires the use of autonomous implementations, which is only possible because the guarantees specify an output behavior instead of an input–output relation. On the other hand, the proof of sufficiency is hindered by the fact that the feedback interconnection contains a loop, and it is not immediately clear how "closing the loop" impacts system behavior.

As the conditions in Theorem 11 are similar to the condition in Theorem 6, Example 4 is already a good illustration of how Theorem 11 can be used in practice, hence we will not provide an additional example. Instead, we conclude this section by showing that, like the series composition, the feedback composition satisfies the compositionality property described in the last paragraph of Section V-A.

Proposition 12: If $\mathcal{C}_1'$ refines $\mathcal{C}_1$, $\mathcal{C}_2'$ refines $\mathcal{C}_2$, and $\mathcal{C}_1 \leftrightarrow \mathcal{C}_2$ exists, then $\mathcal{C}_1' \leftrightarrow \mathcal{C}_2'$ exists and refines $\mathcal{C}_1 \leftrightarrow \mathcal{C}_2$.

Proof: The proof follows the same reasoning as the proof of Proposition 8. For $j \in \{1, 2\}$, let $\mathcal{C}_j' = (\mathrm{A}_j,' \Gamma_j')$, $\mathcal{C}_j = (\mathrm{A}_j, \Gamma_j)$, and note that

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_j) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_j') \quad \text{and} \quad \mathfrak{B}_{\mathrm{o}}(\Gamma_j') \subset \mathfrak{B}_{\mathrm{o}}(\Gamma_j). \tag{96}$$

In view of Theorem 11 and the assumption that $\mathcal{C}_1 \leftrightarrow \mathcal{C}_2$ exists, it follows that (90) holds and $\mathcal{C}_1 \leftrightarrow \mathcal{C}_2$ is given by (91). Using (96) with (90) implies that

$$\Pi_2 \mathfrak{B}_{\mathrm{o}}(\Gamma_1') \subset \Pi_2 \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \quad \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \quad \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2'), \tag{97}$$

$$\mathfrak{B}_{\mathrm{o}}(\Gamma_2') \subset \quad \mathfrak{B}_{\mathrm{o}}(\Gamma_2) \subset \mathrm{I}_2 \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \subset \mathrm{I}_2 \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1') \tag{98}$$

which shows that $\mathcal{C}_1' \leftrightarrow \mathcal{C}_2'$ exists and is given by

$$\mathcal{C}_1' \leftrightarrow \mathcal{C}_2' = (\mathrm{I}_1\mathrm{A}_1,' \Pi_1\Gamma_1'). \tag{99}$$

Finally, (96) also implies that

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{I}_1\mathrm{A}_1) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{I}_1\mathrm{A}_1'), \quad \mathfrak{B}_{\mathrm{o}}(\Pi_1\Gamma_1') \subset \mathfrak{B}_{\mathrm{o}}(\Pi_1\Gamma_1), \tag{100}$$

hence $\mathcal{C}_1' \leftrightarrow \mathcal{C}_2'$ refines $\mathcal{C}_1 \leftrightarrow \mathcal{C}_2$ due to Theorem 4. ■

VI. Conclusion

We presented assume–guarantee contracts for linear dynamical systems with inputs and outputs. An assume–guarantee contract serves as a specification on the external behavior of a system through two aspects. First, the assumptions describe the class of compatible environments, i.e., the environments that the system is expected to operate in. Second, the guarantees describe the desired output behavior of the system when interconnected with a compatible environment.

We found necessary and sufficient conditions for contract implementation in the form of a single behavioral inclusion involving only the assumptions and guarantees of the contract. On the other hand, we defined a notion of contract refinement that allows us to compare two contracts, and we characterized it as a pair of behavioral inclusions relating the assumptions and guarantees of the two contracts.

Finally, we defined two notions of contract composition that allow us to reason about two types of interconnections: series and feedback. In both cases, the composition of two contracts is such that any interconnection of implementations is an implementation of the composition, and when this interconnection is interconnected with a compatible environment of the composition, each component operates in interconnection with an environment compatible with its contract. We found necessary and sufficient conditions for the existence of each type of contract composition, and provided an explicit expression for it when it exists. Furthermore, we showed that contract composition satisfies a desirable compositionality property related to contract refinement.

We suggest two directions for future work on contracts. First, the theory presented in this article can be expanded by solving relevant control problems, e.g., designing plant controllers that achieve contract implementation. Second, the theory presented in this article can be developed for a more general type of contract, e.g., one where the guarantees specify not only an output behavior but a relationship between inputs and outputs, see [36] for the first step in this direction.

Appendix

A. Proof of Lemma 5

Recall that the implication in Definition 7 is equivalent to

$$\left.\begin{array}{r} (u_1, u_{22}) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{E}) \\ (u_1, y_{11}, u_{21}) \in \mathfrak{B}(\Sigma_1) \\ (u_{21}, u_{22}, y_2) \in \mathfrak{B}(\Sigma_2) \end{array}\right\} \Rightarrow \left\{\begin{array}{l} u_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \\ (u_{21}, u_{22}) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \\ (y_{11}, y_2) \in \mathfrak{B}_{\mathrm{o}}(\Gamma). \end{array}\right. \tag{101}$$

Lemma 5 states that the inclusions

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \times \mathrm{I}_2 \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2), \tag{102}$$

$$\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathrm{I}_1 \mathfrak{B}_{\mathrm{o}}(\Gamma) \times \mathrm{I}_1 \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2), \tag{103}$$

$$\mathfrak{B}_{\mathrm{o}}(\Gamma_2) \subset \mathrm{I}_2 \mathfrak{B}_{\mathrm{o}}(\Gamma), \tag{104}$$

are necessary and sufficient for the implication in Definition 7 to be satisfied.

Proof of Lemma 5: We begin by proving the necessity of (102), (103), and (104). Suppose that the implication in Definition 7 is satisfied. Then, (101) holds for all environments E compatible with $\mathcal{C}$, and all implementations Σ_1 and Σ_2 of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Note that A is an environment compatible with $\mathcal{C}$, and the systems

$$\Sigma_1 : y = 0 \quad \text{and} \quad \Sigma_2 : y = 0, \tag{105}$$

implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. These implementations are such that $(u_1, 0, 0) \in \mathfrak{B}(\Sigma_1)$ and $(0, u_{22}, 0) \in \mathfrak{B}(\Sigma_2)$ for all $(u_1, u_{22}) \in \mathfrak{B}_\mathrm{i}(\mathrm{A})$. In view of (101), this implies that $u_1 \in \mathfrak{B}_\mathrm{i}(\mathrm{A}_1)$ and $(0, u_{22}) \in \mathfrak{B}_\mathrm{i}(\mathrm{A}_2)$ for all $(u_1, u_{22}) \in \mathfrak{B}_\mathrm{i}(\mathrm{A})$, which shows that (102) holds.

Next, let Σ_1 be autonomous with $\mathfrak{B}_\mathrm{o}(\Sigma_1) \subset \mathfrak{B}_\mathrm{o}(\Gamma_1)$, and let Σ_2 be given as in (105). It is easily seen that Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Furthermore, for all $(y_{11}, u_{21}) \in \mathfrak{B}_\mathrm{o}(\Sigma_1)$, we have $(0, 0) \in \mathfrak{B}_\mathrm{i}(\mathrm{A})$, $(0, y_{11}, u_{21}) \in \mathfrak{B}(\Sigma_1)$, and $(u_{21}, 0, 0) \in \mathfrak{B}(\Sigma_2)$, hence $(u_{21}, 0) \in \mathfrak{B}_\mathrm{i}(\mathrm{A}_2)$ and $(y_{11}, 0) \in \mathfrak{B}_\mathrm{o}(\Gamma)$ due to (101). In other words, we have that $\mathfrak{B}_\mathrm{o}(\Sigma_1) \subset \mathfrak{B}_\mathrm{o}(\Gamma_1)$ implies $\mathfrak{B}_\mathrm{o}(\Sigma_1) \subset \mathrm{I}_1\mathfrak{B}_\mathrm{i}(\mathrm{A}_2) \times \mathrm{I}_1\mathfrak{B}_\mathrm{o}(\Gamma)$ for all autonomous Σ_1, thus (103) holds due to Lemma 3.

Finally, let Σ_1 be given as in (105), and let Σ_2 be autonomous with $\mathfrak{B}_\mathrm{o}(\Sigma_2) \subset \mathfrak{B}_\mathrm{o}(\Gamma_2)$. Again, it is easily seen that Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Furthermore, for all $y_2 \in \mathfrak{B}_\mathrm{o}(\Sigma_2)$, we have $(0, 0) \in \mathfrak{B}_\mathrm{i}(\mathrm{A})$, $(0, 0, 0) \in \mathfrak{B}(\Sigma_1)$, and $(0, 0, y_2) \in \mathfrak{B}(\Sigma_2)$, hence $(0, y_2) \in \mathfrak{B}_\mathrm{o}(\Gamma)$ due to (101). Therefore, $\mathfrak{B}_\mathrm{o}(\Sigma_2) \subset \mathfrak{B}_\mathrm{o}(\Gamma_2)$ implies $\mathfrak{B}_\mathrm{o}(\Sigma_2) \subset \mathrm{I}_2\mathfrak{B}_\mathrm{o}(\Gamma)$ for all autonomous Σ_2, hence (104) holds due to Lemma 3. This concludes the proof of necessity.

We proceed by proving sufficiency. Suppose that (102), (103), and (104) hold. Let E be an environment compatible with $\mathcal{C}$, and let Σ_1 and Σ_2 be implementations of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Our goal is to show that (101) holds. To this end, let $(u_1, u_{22}) \in \mathfrak{B}_\mathrm{i}(\mathrm{E})$, $(u_1, y_{11}, u_{21}) \in \mathfrak{B}(\Sigma_1)$, and $(u_{21}, u_{22}, y_2) \in \mathfrak{B}(\Sigma_2)$. Since E is compatible with $\mathcal{C}$, it follows that $\mathfrak{B}_\mathrm{i}(\mathrm{E}) \subset \mathfrak{B}_\mathrm{i}(\mathrm{A})$ and $(u_1, u_{22}) \in \mathfrak{B}_\mathrm{i}(\mathrm{A})$. Then, $u_1 \in \mathfrak{B}_\mathrm{i}(\mathrm{A}_1)$ and $u_{22} \in \mathrm{I}_2\mathfrak{B}_\mathrm{i}(\mathrm{A}_2)$ due to (102). From the former, we can conclude that $(u_1, y_{11}, u_{21}) \in \mathfrak{B}(\mathrm{A}_1 \wedge \Sigma_1)$, hence $(y_{11}, u_{21}) \in \mathfrak{B}_\mathrm{o}(\Gamma_1)$ because Σ_1 implements $\mathcal{C}_1$, that is, $\mathfrak{B}_\mathrm{o}(\mathrm{A}_1 \wedge \Sigma_1) \subset \mathfrak{B}_\mathrm{o}(\Gamma_1)$. Then, (103) implies that $y_{11} \in \mathrm{I}_1\mathfrak{B}_\mathrm{o}(\Gamma)$ and $u_{21} \in \mathrm{I}_1\mathfrak{B}_\mathrm{i}(\mathrm{A}_2)$. The latter, together with $u_{22} \in I_2\mathfrak{B}_\mathrm{i}(\mathrm{A}_2)$, gives $(u_{21}, u_{22}) \in \mathfrak{B}_\mathrm{i}(A_2)$. Summarizing, we have shown $u_1 \in \mathfrak{B}_\mathrm{i}(\mathrm{A}_1)$ and $(u_{21}, u_{22}) \in \mathfrak{B}_\mathrm{i}(\mathrm{A}_2)$, which are the first two desired results in the implication (101).

We still need to show that $(y_{11}, y_2) \in \mathfrak{B}_\mathrm{o}(\Gamma)$. Since $(u_{21}, u_{22}) \in \mathfrak{B}_\mathrm{i}(\mathrm{A}_2)$ and $(u_{21}, u_{22}, y_2) \in \mathfrak{B}(\Sigma_2)$, it follows that $(u_{21}, u_{22}, y_2) \in \mathfrak{B}(\mathrm{A}_2 \wedge \Sigma_2)$, hence $y_2 \in \mathfrak{B}_\mathrm{o}(\Gamma_2)$ because Σ_2 implements $\mathcal{C}_2$. Then, $y_2 \in \mathrm{I}_2\mathfrak{B}_\mathrm{o}(\Gamma)$ due to (104), thus $(y_{11}, y_2) \in \mathfrak{B}_\mathrm{o}(\Gamma)$ because $y_{11} \in \mathrm{I}_1\mathfrak{B}_\mathrm{o}(\Gamma)$. With this, we have shown that (101) holds and, thus, the implication in Definition 7 is satisfied. ■

B. Proof of Lemma 9

Before giving the proof of Lemma 9, we need the following two technical results.

Lemma 13: If the polynomial matrix $B(s)$ has full row rank, then there exists an invertible rational matrix $T(s)$ such that $T(s)B(s) = B_\infty + B_\mathrm{sp}(s)$, where B_∞ is a real matrix that has full row rank, and $B_\mathrm{sp}(s)$ is a strictly proper rational matrix.

Proof: To find the desired $T(s)$, we will first transform $B(s)$ to *row-reduced* form. Let k_i be the degree of the polynomial with the highest degree on the ith row of $B(s)$, and let r be the number of rows of $B(s)$. Then, we can write

$$B(s) = D(s)B_h + B_l(s), \tag{106}$$

where B_h is a real matrix

$$D(s) = \mathrm{diag}(s^{k_1}, s^{k_2}, \dots, s^{k_r}), \tag{107}$$

and $B_l(s)$ is a polynomial matrix such that $D(s)^{-1}B_l(s)$ is strictly proper. We say that $B(s)$ is row-reduced if B_h has full row rank, see [37, Sec. 6.3] or [38, Sec. 2.5] for a detailed treatment. It is known that any full row rank polynomial matrix can be transformed to row-reduced form by a sequence of elementary row operations. In other words, as $B(s)$ has full row rank, there exists a unimodular matrix $U(s)$ such that $U(s)B(s)$ is in row-reduced form. Therefore, if k_i now denotes the degree of the polynomial with the highest degree on the ith row of $U(s)B(s)$, then we can write

$$U(s)B(s) = D(s)B_\infty + B_l(s), \tag{108}$$

where B_∞ is a real matrix that has full row rank, $D(s)$ is defined as in (107), and $D(s)^{-1}B_l(s)$ is strictly proper. Then, $T(s) = D(s)^{-1}U(s)$ is the desired invertible rational matrix, and $B_\mathrm{sp}(s) = D(s)^{-1}B_l(s)$. ■

Lemma 14: If $A(s)$ is a polynomial matrix, $B(s)$ is a polynomial matrix that has full row rank, and $C(s)$ is a proper rational matrix such that

$$A(s)B(s) = B(s)C(s), \tag{109}$$

then $\det A(s)$ is constant.

Proof: Since $B(s)$ has full row rank, it follows that $B(s)B(s)^\top$ is invertible and

$$A(s) = B(s)C(s)B(s)^\top \left(B(s)B(s)^\top\right)^{-1}, \tag{110}$$

which implies that

$$\det A(s) = \frac{\det\left(B(s)C(s)B(s)^\top\right)}{\det\left(B(s)B(s)^\top\right)}. \tag{111}$$

Due to Lemma 13, there exists an invertible rational matrix $T(s)$ such that $T(s)B(s) = B_\infty + B_\mathrm{sp}(s)$, where B_∞ has full row rank and $B_\mathrm{sp}(s)$ is a strictly proper rational matrix. Let $\tilde{B}(s) = T(s)B(s)$ and note that

$$\det A(s) = \frac{\det\left(\tilde{B}(s)C(s)\tilde{B}(s)^\top\right)}{\det\left(\tilde{B}(s)\tilde{B}(s)^\top\right)}. \tag{112}$$

Since $C(s)$ is proper, there exists a real matrix C_∞ such that

$$\lim_{s\to\infty} C(s) = C_\infty. \tag{113}$$

This implies that

$$\lim_{s\to\infty} \det A(s) = \frac{\det\left(B_\infty C_\infty B_\infty^\top\right)}{\det\left(B_\infty B_\infty^\top\right)} \tag{114}$$

because B_∞ has full row rank and $\det(B_\infty B_\infty^\top) \neq 0$. Then, $\det A(s)$ is a polynomial that converges as $s \to \infty$, which is possible only if $\det A(s)$ is constant. ■

We are now ready to prove Lemma 9.

Proof of Lemma 9: Let Σ be given by (3), where we partition $Q(s) = \begin{bmatrix} Q_1(s) & Q_2(s) \end{bmatrix}$ and $P(s) = \begin{bmatrix} P_1(s) & P_2(s) \end{bmatrix}$ according to the partition of u and y, respectively. Then,

$$\Sigma_f : \begin{bmatrix} P_1\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) & P_2\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) - Q_2\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \end{bmatrix} y = Q_1\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) u, \quad (115)$$

where the polynomial matrix

$$P_f(s) = \begin{bmatrix} P_1(s) & P_2(s) - Q_2(s) \end{bmatrix} \quad (116)$$

is invertible because Σ_f is assumed to be in input–output form.

Let A and Γ be given by (9) and (10), where we partition $A(s) = \begin{bmatrix} A_1(s) & A_2(s) \end{bmatrix}$ and $G(s) = \begin{bmatrix} G_1(s) & G_2(s) \end{bmatrix}$ according to the partition of u and y, respectively. By Theorem 2, Σ_f implements $\mathcal{C}_f$ if and only if

$$\mathfrak{B}_{\mathrm{o}}\left(\mathrm{I}_1\mathrm{A} \wedge \Sigma_f\right) \subset \mathfrak{B}_{\mathrm{o}}\left(\Gamma\right), \quad (117)$$

which, by Remark 2, holds if and only if there exist polynomial matrices $N_1(s)$ and $N_2(s)$ such that

$$\begin{bmatrix} G(s) & 0 \end{bmatrix} = \begin{bmatrix} N_1(s) & N_2(s) \end{bmatrix} \begin{bmatrix} P_f(s) & -Q_1(s) \\ 0 & -A_1(s) \end{bmatrix}. \quad (118)$$

Therefore, we can focus on finding such $N_1(s)$ and $N_2(s)$.

To this end, we have that $\mathfrak{B}_{\mathrm{o}}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma)$ because Σ implements $\mathcal{C}$, hence, by Remark 2, there exist polynomial matrices $M_1(s)$ and $M_2(s)$ such that

$$\begin{bmatrix} G(s) & 0 \end{bmatrix} = \begin{bmatrix} M_1(s) & M_2(s) \end{bmatrix} \begin{bmatrix} P(s) & -Q(s) \\ 0 & -A(s) \end{bmatrix}. \quad (119)$$

Then, $G(s) = M_1(s)P(s)$ and $M_2(s)A_2(s) = -M_1(s)Q_2(s)$, which implies that

$$G(s) + M_2(s) \begin{bmatrix} 0 & A_2(s) \end{bmatrix} = M_1(s)P_f(s). \quad (120)$$

In view of Remark 6, $\Pi_2\mathfrak{B}_{\mathrm{o}}(\Gamma) \subset \mathrm{I}_2\mathfrak{B}_{\mathrm{i}}(\mathrm{A})$ if and only if there exists a polynomial matrix $L(s)$ such that

$$\begin{bmatrix} 0 & A_2(s) \end{bmatrix} = L(s)G(s)$$

which we can substitute in (120) to obtain

$$(I + M_2(s)L(s))G(s) = G(s)P(s)^{-1}P_f(s), \quad (121)$$

where we used that $M_1(s) = G(s)P(s)^{-1}$ $P(s)$ is invertible because Σ is assumed to be in input–output form. Note that

$$P(s)^{-1}P_f(s) = I - P(s)^{-1} \begin{bmatrix} 0 & Q_2(s) \end{bmatrix}$$

is a proper rational matrix because Σ is in input–output form, that is, $P(s)^{-1}Q(s)$ is proper. Furthermore, due to Remark 1, we can assume that $G(s)$ has full row rank. Then, Lemma 14 and (121) imply that $\det I + M_2(s)L(s)$ is constant. But we know that $P(s)^{-1}P_f(s)$ is invertible because $P_f(s)$ is invertible; hence, $I + M_2(s)L(s)$ is invertible because $G(s)$ has full row rank and (121) holds. Therefore, $I + M_2(s)L(s)$ is an invertible polynomial matrix with constant determinant, which implies that $I + M_2(s)L(s)$ is unimodular.

As $I + M_2(s)L(s)$ is unimodular, from (121) it follows that

$$N_1(s) = (I + M_2(s)L(s))^{-1}M_1(s) \quad (122)$$

is a polynomial matrix such that $G(s) = N_1(s)P_f(s)$. Note that $M_1(s)Q_1(s) = -M_2(s)A_1(s)$ due to (119), hence

$$N_1(s)Q_1(s) = -(I + M_2(s)L(s))^{-1}M_2(s)A_1(s)$$

and the polynomial matrix

$$N_2(s) = (I - M_2(s)L(s))^{-1}M_2(s) \quad (123)$$

is such that $N_1(s)Q_1(s) + N_2(s)A_1(s) = 0$. Then, $N_1(s)$ and $N_2(s)$ as defined in (122) and (123) are polynomial matrices satisfying (118), which shows that (117) holds, as desired. ■

C. Proof of Lemma 10

Recall that the implication in Definition 9 is equivalent to

$$\left.\begin{array}{r} u_{11} \in \mathfrak{B}_{\mathrm{i}}\left(\mathrm{E}\right) \\ \left(u_{11}, u_{12}, y_{11}, u_2\right) \in \mathfrak{B}\left(\Sigma_1\right) \\ \left(u_2, u_{12}\right) \in \mathfrak{B}\left(\Sigma_2\right) \end{array}\right\} \Rightarrow \begin{cases} \left(u_{11}, u_{12}\right) \in \mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}_1\right) \\ u_2 \in \mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}_2\right) \\ y_{11} \in \mathfrak{B}_{\mathrm{o}}\left(\Gamma\right). \end{cases} \quad (124)$$

Lemma 10 states the inclusions

$$\mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}\right) \subset \mathrm{I}_1\mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}_1\right), \quad (125)$$

$$\mathfrak{B}_{\mathrm{o}}\left(\Gamma_1\right) \subset \mathfrak{B}_{\mathrm{o}}\left(\Gamma\right) \times \mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}_2\right), \quad (126)$$

$$\mathfrak{B}_{\mathrm{o}}\left(\Gamma_2\right) \subset \mathrm{I}_2\mathfrak{B}_{\mathrm{i}}\left(\mathrm{A}_1\right), \quad (127)$$

are necessary and sufficient for the implication in Definition 9 to be satisfied.

Proof of Lemma 10: We begin by proving the necessity of (125), (126), and (127), following a similar approach as in the proof of Lemma 5. Suppose that the implication in Definition 9 is satisfied. Then, (124) holds for all environments E compatible with $\mathcal{C}$, and implementations Σ_1 and Σ_2 of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Note that A is an environment compatible with $\mathcal{C}$, and the systems

$$\Sigma_1 : y = 0 \quad \text{and} \quad \Sigma_2 : y = 0, \quad (128)$$

implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Also, for all $u_{11} \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$, we have $(u_{11}, 0, 0, 0) \in \mathfrak{B}(\Sigma_1)$ and $(0, 0) \in \mathfrak{B}(\Sigma_2)$, hence $(u_{11}, 0) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ due to (124). This shows that (125) holds.

Next, let Σ_1 be autonomous with $\mathfrak{B}_{\mathrm{o}}(\Sigma_1) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma_1)$, and let Σ_2 be given as in (128). Then, Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and for all $(y_{11}, u_2) \in \mathfrak{B}_{\mathrm{o}}(\Sigma_1)$, we have $0 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$, $(0, 0, y_{11}, u_2) \in \mathfrak{B}(\Sigma_1)$ and $(u_2, 0) \in \mathfrak{B}(\Sigma_2)$, hence $u_2 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ and $y_{11} \in \mathfrak{B}_{\mathrm{o}}(\Gamma)$ due to (124). Consequently, $\mathfrak{B}_{\mathrm{o}}(\Sigma_1) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma_1)$ implies $\mathfrak{B}_{\mathrm{o}}(\Sigma_1) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma) \times \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ for all autonomous Σ_1, hence (126) holds due to Lemma 3.

Finally, let Σ_1 be given as in (128), and let Σ_2 be autonomous with $\mathfrak{B}_{\mathrm{o}}(\Sigma_2) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma_2)$. Note that Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively. Moreover, for all $u_{12} \in \mathfrak{B}_{\mathrm{o}}(\Sigma_2)$, we have $0 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$, $(0, u_{12}, 0, 0) \in \mathfrak{B}(\Sigma_1)$, and $(0, u_{12}) \in \mathfrak{B}(\Sigma_2)$, hence $(0, u_{12}) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ due to (124). Then, $\mathfrak{B}_{\mathrm{o}}(\Sigma_2) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma_2)$ implies $\mathfrak{B}_{\mathrm{o}}(\Sigma_2) \subset \mathrm{I}_2\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ for all autonomous Σ_1, hence (127) holds due to Lemma 3.

We proceed by proving sufficiency. Suppose that (125), (126), and (127) hold. Let E be compatible with $\mathcal{C}$, and let Σ_1 and Σ_2 be implementations of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, such that $\Sigma_1 \hookleftarrow \Sigma_2$ is in input–output form. We will make use of the relationship between $\Sigma_1 \hookleftarrow \Sigma_2$ and $\Sigma_1 \to \Sigma_2$ described in Remark 7, as well as Lemma 9. Recall that the only difference between $\Sigma_1 \hookleftarrow \Sigma_2$ and $(\Sigma_1 \to \Sigma_2)_f$ is that output of the former is given by y_{11} while the output of the latter is given by (y_{11}, y_2). Given that their inputs and dynamics are the same, and $\Sigma_1 \hookleftarrow \Sigma_2$ is assumed to be in input–output form, this implies that $(\Sigma_1 \to \Sigma_2)_f$ is also in input–output form.

Furthermore, (126) implies that $\Pi_2\mathfrak{B}_{\rm o}(\Gamma_1) \subset \mathfrak{B}_{\rm i}(\mathrm{A}_2)$, hence, due to Theorem 6, $\mathcal{C}_1 \to \mathcal{C}_2$ exists and is given by

$$\mathcal{C}_1 \to \mathcal{C}_2 = (\mathrm{A}_1, \Pi_1\Gamma_1 \times \Gamma_2). \tag{129}$$

Furthermore, $\Sigma_1 \to \Sigma_2$ implements $\mathcal{C}_1 \to \mathcal{C}_2$, and

$$\Pi_2\mathfrak{B}_{\rm o}\left(\Pi_1\Gamma_1 \times \Gamma_2\right) = \mathfrak{B}_{\rm o}\left(\Gamma_2\right) \subset \mathrm{I}_2\mathfrak{B}_{\rm i}\left(\mathrm{A}_1\right) \tag{130}$$

because of (127). Using Lemma 9, we find that $(\Sigma_1 \to \Sigma_2)_f$ implements the contract

$$(\mathcal{C}_1 \to \mathcal{C}_2)_f = (\mathrm{I}_1\mathrm{A}_1, \Pi_1\Gamma_1 \times \Gamma_2), \tag{131}$$

hence, due to Theorem 2, we have that

$$\mathfrak{B}_{\rm o}\left(\mathrm{I}_1\mathrm{A}_1 \times (\Sigma_1 \to \Sigma_2)_f\right) \subset \mathfrak{B}_{\rm o}\left(\Pi_1\Gamma_1 \times \Gamma_2\right). \tag{132}$$

Now, let $u_{11} \in \mathfrak{B}_{\rm i}(\mathrm{E})$, $(u_{11}, u_{12}, y_{11}, u_2) \in \mathfrak{B}(\Sigma_1)$ and $(u_2, u_{12}) \in \mathfrak{B}(\Sigma_2)$. Our goal is to show that (124) holds. To this end, we have that $\mathfrak{B}_{\rm i}(\mathrm{E}) \subset \mathfrak{B}_{\rm i}(\mathrm{A})$ because E is compatible with $\mathcal{C}$. Then, $u_{11} \in \mathfrak{B}_{\rm i}(\mathrm{A})$, which yields $u_{11} \in \mathrm{I}_1\mathfrak{B}_{\rm i}(\mathrm{A}_1)$ due to (125). On the other hand, we have that $(u_{11}, u_{12}, y_{11}, u_{12}) \in \mathfrak{B}(\Sigma_1 \to \Sigma_2)$ and thus $(u_{11}, y_{11}, u_{12}) \in \mathfrak{B}((\Sigma_1 \to \Sigma_2)_f)$. In view of (132), this implies that $(y_{11}, u_{12}) \in \mathfrak{B}_{\rm o}(\Pi_1\Gamma_1 \times \Gamma_2)$, and, in particular, that $y_{11} \in \Pi_1\mathfrak{B}_{\rm o}(\Gamma_1)$ and $u_{12} \in \mathfrak{B}_{\rm o}(\Gamma_2)$. Then, $y_{11} \in \mathfrak{B}_{\rm o}(\Gamma)$ due to (126), and $u_{12} \in \mathrm{I}_2\mathfrak{B}_{\rm i}(\mathrm{A}_1)$ due to (127). Given that $u_{11} \in \mathrm{I}_1\mathfrak{B}_{\rm i}(\mathrm{A}_1)$ and $u_{12} \in \mathrm{I}_2\mathfrak{B}_{\rm i}(\mathrm{A}_1)$, we have that $(u_{11}, 0) \in \mathfrak{B}_{\rm i}(\mathrm{A}_1)$ and $(0, u_{12}) \in \mathfrak{B}_{\rm i}(\mathrm{A}_1)$, hence $(u_{11}, u_{12}) \in \mathfrak{B}_{\rm i}(\mathrm{A}_1)$. We still need to show that $u_2 \in \mathfrak{B}_{\rm i}(\mathrm{A}_2)$ before we can conclude that (124) holds. To do this, we note that $(y_{11}, u_2) \in \mathfrak{B}_{\rm o}(\mathrm{A}_1 \wedge \Sigma_1)$ because $(u_{11}, u_{12}) \in \mathfrak{B}_{\rm i}(\mathrm{A}_1)$ and $(u_{11}, u_{12}, y_{11}, u_2) \in \mathfrak{B}(\Sigma_1)$. But $\mathfrak{B}_{\rm o}(\mathrm{A}_1 \wedge \Sigma_1) \subset \mathfrak{B}_{\rm o}(\Gamma_1)$ because Σ_1 implements $\mathcal{C}_1$, hence $(y_{11}, u_2) \in \mathfrak{B}_{\rm o}(\Gamma_1)$ and thus $u_2 \in \mathfrak{B}_{\rm i}(\mathrm{A}_2)$ due to (126). With this, we have shown that $(u_{11}, u_{12}) \in \mathfrak{B}_{\rm i}(\mathrm{A}_1)$, $u_2 \in \mathfrak{B}_{\rm i}(\mathrm{A}_2)$ and $y_{11} \in \mathfrak{B}_{\rm o}(\Gamma)$, which shows that (124) holds and the implication in Definition 9 is satisfied. ∎

References

[1] A. Sangiovanni-Vincentelli, W. Damm, and R. Passerone, "Taming Dr. Frankenstein: Contract-based design for cyber-physical systems," *Eur. J. Control*, vol. 18, no. 3, pp. 217–238, 2012.

[2] S. Tripakis, "Compositionality in the science of system design," *Proc. IEEE*, vol. 104, no. 5, pp. 960–972, May 2016.

[3] J. C. Willems, "Dissipative dynamical systems Part I: General theory," *Arch. Rational Mech. Anal.*, vol. 45, no. 5, pp. 321–351, 1972.

[4] A. J. van der Schaft, *L^2-Gain and Passivity Techniques in Nonlinear Control*. Cham, Switzerland: Springer, 2017.

[5] D. D. Šiljak, "Mathematics in science and engineering," in *Decentralized Control of Complex Systems*. Boston, MA, USA: Acad. Press, 1991.

[6] M. Rotkowitz and S. Lall, "A characterization of convex problems in decentralized control," *IEEE Trans. Autom. Control*, vol. 50, no. 12, pp. 1984–1996, Dec. 2005.

[7] L. Bakule, "Decentralized control: An overview," *Annu. Rev. Control*, vol. 32, no. 1, pp. 87–98, 2008.

[8] T. Ishizaki, T. Sadamoto, J. Imura, H. Sandberg, and K. H. Johansson, "Retrofit control: Localization of controller design and implementation," *Automatica*, vol. 95, pp. 336–346, 2018.

[9] T. Ishizaki, T. Kawaguchi, H. Sasahara, and J. Imura, "Retrofit control with approximate environment modeling," *Automatica*, vol. 107, pp. 442–453, 2019.

[10] T. Ishizaki, H. Sasahara, M. Inoue, T. Kawaguchi, and J. Imura, "Modularity-in-design of dynamical network systems: Retrofit control approach," *IEEE Trans. Autom. Control*, vol. 66, no. 11, pp. 5205–5220, Nov. 2021.

[11] B. Meyer, "Applying 'design by contract," *Computer*, vol. 25, no. 10, pp. 40–51, 1992.

[12] A. Benveniste et al., *Contracts for System Design. Foundations and Trends in Electronic Design Automation*. Hanover, MA, USA: Now Publishers, 2018.

[13] J. W. Polderman and J. C. Willems, *Introduction to Mathematical Systems Theory*. New York, NY, USA: Springer, 1998.

[14] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747–1767, 1999.

[15] E. S. Kim, M. Arcak, and S. A. Seshia, "A small gain theorem for parametric assume-guarantee contracts," in *Proc. 20th Int. Conf. Hybrid Syst.: Comput. Control*, 2017, pp. 207–216.

[16] M. A. Khatib and M. Zamani, "Controller synthesis for interconnected systems using parametric assume-guarantee contracts," in *Proc. Amer. Control Conf.*, 2020, pp. 5419–5424.

[17] Y. Chen, J. Anderson, K. Kalsi, A. D. Ames, and S. H. Low, "Safety-critical control synthesis for network systems with control barrier functions and assume-guarantee contracts," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 1, pp. 487–499, Mar. 2021.

[18] A. Saoud, A. Girard, and L. Fribourg, "On the composition of discrete and continuous-time assume-guarantee contracts for invariance," in *Proc. Eur. Control Conf.*, 2018, pp. 435–440.

[19] A. Saoud, A. Girard, and L. Fribourg, "Contract-based design of symbolic controllers for safety in distributed multiperiodic sampled-data systems," *IEEE Trans. Autom. Control*, vol. 66, no. 3, pp. 1055–1070, Mar. 2021.

[20] I. D. Loreto, A. Borri, and M. D. Di Benedetto, "An assume-guarantee approach to sampled-data quantized glucose control," in *Proc. IEEE Conf. Decis. Control*, 2020, pp. 3401–3406.

[21] D. Zonetti, A. Saoud, A. Girard, and L. Fribourg, "A symbolic approach to voltage stability and power sharing in time-varying DC microgrids," in *Proc. Eur. Control Conf.*, 2019, pp. 903–909.

[22] A. Eqtami and A. Girard, "A quantitative approach on assume-guarantee contracts for safety of interconnected systems," in *Proc. Eur. Control Conf.*, 2019, pp. 536–541.

[23] B. Besselink, K. H. Johansson, and A. J. van der Schaft, "Contracts as specifications for dynamical systems in driving variable form," in *Proc. Eur. Control Conf.*, 2019, pp. 263–268.

[24] K. Ghasemi, S. Sadraddini, and C. Belta, "Compositional synthesis via a convex parameterization of assume-guarantee contracts," in *Proc. Int. Conf. Hybrid Syst., Comput. Control*, 2020, pp. 1–10.

[25] M. Sharf, B. Besselink, A. Molin, Q. Zhao, and K. H. Johansson, "Assume/guarantee contracts for dynamical systems: Theory and computational tools," in *Proc. 7th IFAC Conf. Anal. Des. Hybrid Syst.*, 2021, pp. 25–30.

[26] A. Saoud, A. Girard, and L. Fribourg, "Assume-guarantee contracts for continuous-time systems," *Automatica*, vol. 134, 2021, Art. no. 109910.

[27] A. Saoud, A. Girard, and L. Fribourg, "Contract based design of symbolic controllers for interconnected multiperiodic sampled-data systems," in *Proc. IEEE Conf. Decis. Control*, 2018, pp. 773–779.

[28] F. Kerber and A. van der Schaft, "Assume-guarantee reasoning for linear dynamical systems," in *Proc. Eur. Control Conf.*, 2009, pp. 5015–5020.

[29] F. Kerber and A. van der Schaft, "Compositional analysis for linear systems," *Syst. Control Lett.*, vol. 59, no. 10, pp. 645–653, 2010.

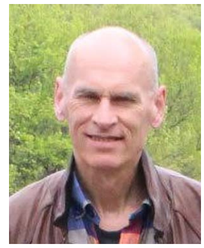
[30] F. Kerber and A. J. van der Schaft, "Decentralized control using compositional analysis techniques," in *Proc. IEEE Conf. Decis. Control Eur. Control Conf.*, 2011, pp. 2699–2704.

[31] J. C. Willems, "The behavioral approach to open and interconnected systems," *IEEE Control Syst. Mag.*, vol. 27, no. 6, pp. 46–99, Dec. 2007.

[32] J. C. Willems, "Input-output and state-space representations of finite-dimensional linear time-invariant systems," *Linear Algebra Appl.*, vol. 50, pp. 581–608, 1983.
[33] B. M. Shali, A. J. van der Schaft, and B. Besselink, "Behavioural contracts for linear dynamical systems: Input assumptions and output guarantees," in *Proc. Eur. Control Conf.*, 2021, pp. 564–569.
[34] J. W. Polderman, "A new and simple proof of the equivalence theorem for behaviors," *Syst. Control Lett.*, vol. 41, no. 3, pp. 223–224, 2000.
[35] K. Zhou, J. C. Doyle, and K. Glover, *Robust and Optimal Control*. Upper Saddle River, NJ, USA: Prentice Hall, 1996.
[36] B. M. Shali, A. J. van der Schaft, and B. Besselink, "Behavioural assume-guarantee contracts for linear dynamical systems," in *Proc. IEEE Conf. Decis. Control*, 2021, pp. 2002–2007.
[37] T. Kailath, *Linear Systems*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1980.
[38] W. A. Wolovich, *Linear Multivariable Systems*. New York, NY, USA: Springer, 1974.

Brayan M. Shali (Graduate Student Member, IEEE) received the B.Sc. and M.Sc. (summa cum laude) degrees in applied mathematics in 2017 and 2019, respectively, from the University of Groningen, Groningen, The Netherlands, where he is currently working toward the Ph.D. degree in systems and control with the Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence.

His research interests include mathematical systems theory for the design and analysis of large-scale interconnected systems, contract-based design, behavioral systems theory, and networks of dynamical systems.



Arjan van der Schaft (Fellow, IEEE) received the undergraduate and Ph.D. degrees in mathematics from the University of Groningen, Groningen, The Netherlands, in 1979, and 1983, respectively.

In 1982, he joined the Department of Applied Mathematics, University of Twente, Twente, The Netherlands. In 2005, he returned to his Alma Mater as Professor in mathematics. He has authored many books, including *Variational and Hamiltonian Control Systems* (1987, with P.E. Crouch), *Nonlinear Dynamical Control Systems* (1990, 2016, with H. Nijmeijer), *L2-Gain and Passivity Techniques in Nonlinear Control* (1996, 2000, 2017), *An Introduction to Hybrid Dynamical Systems* (2000, with J. M. Schumacher), and *Port-Hamiltonian Systems: An Introductory Overview* (2014, with D. Jeltsema).

Dr. Schaft is a Fellow of the International Federation of Automatic Control (IFAC). He was the recipient of the 2013 three-yearly awarded Certificate of Excellent Achievements of the IFAC Technical Committee on Nonlinear Systems. He was invited as Speaker with the International Congress of Mathematicians, Madrid, 2006.

Bart Besselink (Member, IEEE) received the M.Sc. (cum laude) and Ph.D. degrees in mechanical engineering from the Eindhoven University of Technology, Eindhoven, The Netherlands, in 2008 and 2012, respectively. Since 2016, he has been an Assistant Professor with the Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence, University of Groningen, Groningen, The Netherlands. He was a short-term Visiting Researcher with the Tokyo Institute of Technology, Tokyo, Japan, in 2012. Between 2012 and 2016, he was a Postdoctoral Researcher with the ACCESS Linnaeus Centre and Department of Automatic Control, KTH Royal Institute of Technology, Stockholm, Sweden. His research interests include mathematical systems theory for large-scale interconnected systems, with emphasis on contract-based design and control, compositional analysis, model reduction, and applications in intelligent transportation systems and neuromorphic computing.

Dr. Besselink was the recipient (with Xiaodong Cheng and Jacquelien Scherpen) of the 2020 Automatica Paper Prize.