Contract theory for linear control systems

Shali, Brayan

DOI:
10.33612/diss.830800648

Contract theory for linear control systems

Brayan M. Shali

university of groningen

The research reported in this dissertation has been carried out at the Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence, University of Groningen, The Netherlands.

disc dutch institute of systems and control

The research reported in this dissertation is part of the research program of the Dutch Institute of Systems and Control (DISC). The author has successfully completed the educational program of the Graduate School DISC.

Cover image by VectorStock:

https:// www.vectorstock.com/royalty-free-vector/tetris-pieces-vector-15532662

ISBN: 978-94-93353-40-4

university of groningen

Contract theory for linear control systems

PhD thesis

to obtain the degree of PhD at the
University of Groningen
on the authority of the
Rector Magnificus Prof. J.M.A. Scherpen
and in accordance with
the decision by the College of Deans.

This thesis will be defended in public on

Tuesday 5 December 2023 at 9.00 hours

by

Brayan Masoud Shali

born on 20 May 1995

Supervisors

Prof. B. Besselink
Prof. A.J. van der Schaft

Assessment Committee

Prof. H.L. Trentelman
Prof. A. Girard
Prof. S. Weiland

Acknowledgments

This thesis is the culmination of a long and enriching journey, and I owe its existence to the support and contributions of many people. In the following, I would like to take a moment to express my gratitude to all of those who have played important roles in my personal and professional development.

First and foremost, I want to express my deepest gratitude to my supervisors, Bart Besselink and Arjan van der Schaft. Bart, your unwavering support over the course of four years has been immeasurable. Your availability for discussions and your enthusiasm for my research, no matter how underwhelmed I sometimes felt, were constant sources of motivation. Perhaps more importantly, your approachability and understanding created an environment where I felt comfortable sharing my ideas and concerns, thus fostering a collaborative and enriching experience. Arjan, although our interactions were less frequent, I always had confidence in your wisdom and readiness to assist when I needed your help. Your quick and gracious responses, especially during those last-minute requests, were greatly appreciated.

I also want to express my gratitude to the members of my reading committee, Harry Trentelman, Antoine Girard, and Siep Weiland, for their thorough reading of my thesis and the valuable feedback they provided. Incidentally, I have had the pleasure of attending courses taught by each one of you; various bachelor and master level courses by Harry Trentelman, the EECI course on formal methods by Antoine Girard, and the DISC course on linear matrix inequalities by Siep Weiland. I have thoroughly enjoyed all of these courses, due in no small part to your enthusiasm and excellent teaching skills.

My heartfelt thanks extend to Anne-Men Huijzer and Armin Pirastehzad for accepting the role of my paranymphs. Anne-Men, our academic journey began when we were just bachelor students, and I deeply cherish the camaraderie we have shared ever since. Although our paths may now diverge, I am optimistic that our friendship will endure. Armin, you joined our group during the height of the pandemic, which presented unique challenges for us to get to know each other. As if to compensate for that, we had the opportunity to spend more than a week together in Stockholm, creating lasting memories and forging what I hope will be a lifelong friendship.

I want to express my sincere appreciation of Kanat Camlibel and Harry Trentelman, whose inspiration during my bachelor's and master's studies played a pivotal role in my decision to pursue a PhD degree. Similarly, I am thankful to Henk van Waarde for his invaluable mentorship throughout the last five years; as a master thesis supervisor at first, as a senior colleague later, and as a postdoc supervisor now. You have truly been a role model to me.

My PhD journey would not have been as fulfilling without my wonderful colleagues in the SCO (SCAA) group at the Bernoulli Institute. In particular, I am grateful to my current and former office mates, Armin, Yongzhang, Mark, and Jaap, for transforming our office into a dynamic space where the boundary between serious scientific discussions and lighthearted banter often became quite murky. I am also grateful to Amir, Hamin, Koorosh and Radu for being such great company during our afternoon walks. To all current, former, and temporary members of the SCO group, including Azka, Di, Juan, Huayuan, Junjie, Jiajia, Jiwei, Marieke, Paul, Stephan, Sumon, Sutrisno, Teke, and Zepeng, I am grateful for the many joyful moments during group lunches, board game evenings, pub quizzes and other fun activities.

I also want to thank my colleagues from EnTeG for all the fun times at DISC courses and conferences. I had the pleasure of experiencing the most exciting presentation session together with Carmen at the Benelux workshop in Rotterdam. I also cherish the playful, although sometimes brutal, banter with Kathinka, both during train rides to Utrecht and our trip to Mexico. In addition, I want to acknowledge Jasper and Wouter, who are (still) part of the Bourbaki 2.0 group that originated during our master's studies. We shared numerous pleasant dinners back then, and I hope there will be opportunities to recreate those in the future.

Finally, I want to thank my friends in the Netherlands for making my stay here so pleasant, and my friends and family in Bulgaria for their unwavering support and confidence in my success. Specifically, I want to acknowledge Vlad, Jonathan, Maike, Paula, Ruben, Stefanos, Mario, Monika, Deyvid, Zori, Niki, Bobeto, Kiki, Gogo, and, of course, my mother, father, brother, aunt, uncle, and cousin. Each one of you has played a unique and invaluable role in my academic and personal development. Thank you!

Contents

1 Introduction **1**
- 1.1 Relevant literature . . . 3
- 1.2 Objective and contributions . . . 6
- 1.3 Outline . . . 8

2 Meta-theory of contracts **9**
- 2.1 Contracts as specifications . . . 9
- 2.2 Independent design . . . 12

3 Behavioural contracts **17**
- 3.1 Polynomial and rational matrices . . . 18
- 3.2 System classes and behaviours . . . 29
- 3.3 Contracts . . . 34
- 3.4 Consistency . . . 40
- 3.5 Refinement . . . 50
- 3.6 Conjunction . . . 54
- 3.7 Discussion . . . 61

4 Composition of behavioural contracts **63**
- 4.1 System interconnections . . . 64
  - 4.1.1 Series interconnection . . . 65
  - 4.1.2 Feedback interconnection . . . 66
- 4.2 Series composition with output guarantees . . . 72
- 4.3 Feedback composition with output guarantees . . . 78
- 4.4 Feedback composition . . . 83
- 4.5 Series composition . . . 90
- 4.6 External interconnections . . . 92
- 4.7 Discussion . . . 97

5 Simulation contracts **99**
- 5.1 Preliminaries on simulation . . . 101
- 5.2 Contracts . . . 108
- 5.3 Consistency . . . 113

5.4 Control for implementation . . . 118
5.5 Illustrative example . . . 121
5.6 Refinement . . . 125
5.7 Series composition . . . 127
5.8 Comparison with behavioural contracts . . . 135
5.9 Discussion . . . 142

6 Conclusion **145**
6.1 Future research . . . 147

A Lemmas **149**

B Proofs **155**
B.1 Proof of Proposition 4.1 . . . 155
B.2 Proof of Proposition 4.2 . . . 156
B.3 Proof of Lemma 4.4 . . . 159
B.4 Proof of Lemma 4.6 . . . 160
B.5 Proof of Lemma 4.8 . . . 163
B.6 Proof of Lemma 4.9 . . . 165
B.7 Proof of Lemma 4.10 . . . 167
B.8 Proof of Theorem 4.5 . . . 169
B.9 Proof of Lemma 5.6 . . . 172
B.10 Proof of Theorem 5.2 . . . 174
B.11 Proof of Lemma 5.8 . . . 176
B.12 Proof of Theorem 5.3 . . . 179
B.13 Proof of Lemma 5.9 . . . 181
B.14 Proof of Lemma 5.10 . . . 185
B.15 Proof of Lemma 5.11 . . . 191

Bibliography **197**

Summary **205**

Samenvatting **207**

Chapter 1

Introduction

Advances in technology and automation are driving a considerable increase in the complexity of modern engineering systems. These systems often comprise a large number of interconnected components that incorporate different types of physical processes, such as electrical, mechanical, structural, thermal, and biological. In addition, we are seeing computing and communication capabilities being embedded in these systems in order to control physical processes. Such systems, i.e., systems that comprise a number of *physical* components connected through *cyber* elements for computation and communication, are broadly referred to as cyber-physical systems [1–4]. Examples of cyber-physical systems include flight control systems in airplanes, autonomous vehicles, intelligent transportation systems, smart grids, smart manufacturing systems, smart buildings, assisted living devices, and artificial heart pacemakers, to name a few. In many of these examples, the incorporation of cyber elements dramatically increases the efficiency and performance of an otherwise purely physical system.

Many challenges arise in the development of modern engineering systems, particularly in the realm of cyber-physical systems. To begin with, these systems are heterogeneous by nature. Even the relatively simple example of an adaptive cruise control system involves mechanical parts, the engine, sensors, actuators, embedded computing units, and software. More complex examples, such as smart manufacturing systems, also involve completely different types of physical processes, e.g., mechanical, chemical, and thermal. This means that the components of the system often have to be designed by different teams coming from different engineering disciplines.

In addition to heterogeneity, two recurring aspects of emerging cyber-physical systems are high complexity and large scale. For example, intelligent transportation systems involve a large number of vehicles that need to be coordinated in a constantly changing environment that involves many complex behaviours, notably that of humans. On the other hand, smart grids involve

a large number of generators and an even larger number of consumers that need to interact over large distances. Dealing with such complexity and scale is a major challenge.

Another challenge relates to the merging of various types of requirements. These are technical requirements as well as requirements on reliability, cost, and time-to-market. Additionally, the technical requirements themselves are often multifaceted, including aspects like functionality, efficiency, safety, etc. For example, an autonomous vehicle must be able to traverse complex trajectories, including intricate city streets and challenging terrains. It must do so efficiently, optimizing factors such as travel time and fuel consumption. More importantly, it must do so safely, avoiding obstacles such as pedestrians, cyclists, other vehicles, traffic signs, etc. In other words, modern engineering systems often need to exhibit complex behaviour that adheres to, sometimes conflicting, requirements coming from different viewpoints.

Considering all of the aforementioned factors, it is no surprise that the development of modern engineering systems and, specifically, cyber-physical systems is a formidable task. The prevailing approach is based on using mathematical models to represent and simulate components. Each component is typically developed in isolation according to some specification but with only ad hoc assumptions about the other components. Because of this, the components are not guaranteed to keep functioning according to their specification once they are interconnected, i.e., components do not necessarily integrate correctly. Consequently, the resulting interconnected system needs to be simulated and subjected to rigorous testing. If the outcomes prove unsatisfactory, the components are returned for further development. As there are no guarantees that the upgraded components will integrate correctly, this process might have to be repeated multiple times, which can be very costly and time-consuming.

To address the challenges that arise in the development of cyber-physical systems, we require a method for expressing specifications for components with the following aspects. First, to deal with the complexity of cyber-physical systems, this method should enable the expression of *rich specifications* for components. Second, to deal with the large-scale, heterogeneous, and multidisciplinary nature of cyber-physical systems, this method should be inherently *modular*. In other words, it should allow components to be considered *independently* and, in particular, it should provide guarantees on the correct integration of components. Contract-based design has been recognized as one such method. However, contract theories have mainly been developed for system classes modelling cyber components, i.e., systems with discrete variables in discrete time. Motivated by this, our objective in this thesis is to develop a contract theory for physical components, specifically those modelled by dynamical control systems with continuous variables in continuous time.

1.1 Relevant literature

To provide additional context, we will briefly discuss some of the existing methods for expressing specifications on dynamical control systems, as well as existing methods for modular analysis and design. Then, we will provide a brief overview of the relevant literature on contract-based design.

Specifications. Specifications on dynamical control systems typically come in the form of requirements on stability, passivity or performance, where the latter is generally expressed as a bounded gain for a suitably chosen input-output pair. Such specifications have in common that they can be captured in the elegant framework of dissipativity as introduced in [5] and developed in [6–8]. Other common specifications, such as constraint satisfaction and safety, can be seen as instances of set-invariance [9]. However, the complexity of modern engineering systems requires the expression of specifications that go beyond dissipativity and set invariance. This has motivated the development of formal methods in control [10, 11], where specifications are expressed using linear temporal logic formulas. Although such logic formulas have very high expressive power, their satisfaction is difficult to verify for continuous systems. Therefore, formal methods typically rely on abstractions to discrete, and often finite, systems. One consequence of this is the so-called "curse of dimensionality", which refers to the fact that the state space of such abstractions can easily become intractably large.

Another well-known method for expressing specifications is with a reference system that captures the desired behaviour of the system under consideration. A specification expressed in this manner is satisfied if the system behaves exactly like the reference system. This is typically formalized using a notion of system equivalence, such as equality of behaviour or bisimulation. The problem of control in this setting is explored for various system classes in the literature, see, e.g., [12–21]. Exact model matching [22–25], also known as model following [26], is conceptually similar, but with equivalence typically expressed as equality of transfer matrices or impulse responses.

Modularity. There are various methods for modular analysis and design in the control literature. Some of the most well-known ones are based on the theory of dissipativity [5, 8], with the celebrated small-gain theorem and various passivity theorems being prime examples. These theorems allow one to reason about the global properties of the interconnected system based on the local properties of its components. In a similar vein, there are control methods, such as decentralized control [27–29], that deal with the design of controllers which use only local information to achieve a desired global objective. This restriction of information generally results in simpler local controllers that are computationally easier to implement than a global controller that achieves the same objective.

Contract-based design. An alternative method for expressing specifications that also supports modular analysis and design is based on so-called contracts. The notion of contract was first introduced by Meyer [30, 31] in the context of the programming language Eiffel, building upon earlier ideas from Floyd-Hoare logic [32, 33]. Meyer's goal was to establish a methodology of object-oriented software construction that would enhance the reliability of software systems. Although the pragmatic techniques presented in [30] represent a considerable contribution towards this goal, they do not offer infallible methods to guarantee reliability. Nevertheless, they have served as inspiration for contract-based reasoning in various contexts. For example, rely-guarantee rules are introduced in [34] to deal with programs that operate concurrently, while the popularization of interface theories [35–38] has spurred the development of contract-based techniques for cyber-physical systems [39–45].

There is a wide variety of approaches to contract-based design in the literature that, nevertheless, share a common philosophy. This is clarified in [46], where a mathematical meta-theory of contracts that focuses on semantic concepts is developed. This meta-theory formalizes the basic idea of a contract and its associated notions without referring to a specific instantiation. In particular, it shows that contract theories are distinguished by the following features:

- Contracts take the environment in which a component operates explicitly into account. This can ease the design burden on the component since the specification expressed by the contract needs to be satisfied *only* when the component is interconnected with a relevant environment. Furthermore, it can ensure that the component integrates correctly by explicitly stating the expected behaviour of the other components as part of the specification.

- Contracts are equipped with notions of refinement and composition that enable the independent design of components within interconnected systems. The basic idea is as follows. Suppose that we want to design an interconnected system that satisfies some global specification, as shown in Figure 1.1. Designing the components of this system independently means that each component is designed according to some local specification, as shown in Figure 1.2. We want the satisfaction of these local specifications to guarantee that the resulting interconnected system satisfies the global specification that we started with. To this end, a natural first step is to deduce that the interconnected system satisfies some composite specification that is obtained by composing the local specifications, as shown in Figure 1.3. This is captured by the notion of composition. Then, the second step is to ensure that satisfaction of the composite specification implies satisfaction of the global specification that we started with. This is captured by the notion of refinement.

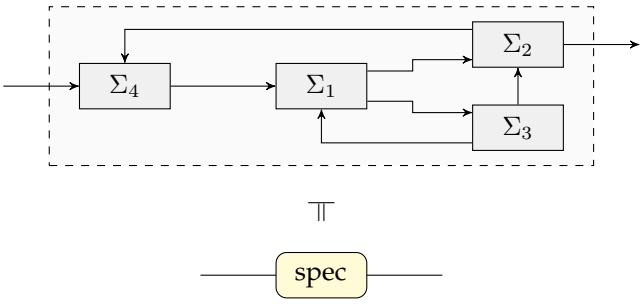

Figure 1.1: Global specification.

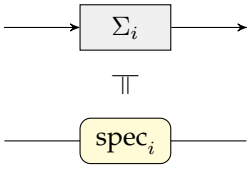

Figure 1.2: Local specification.

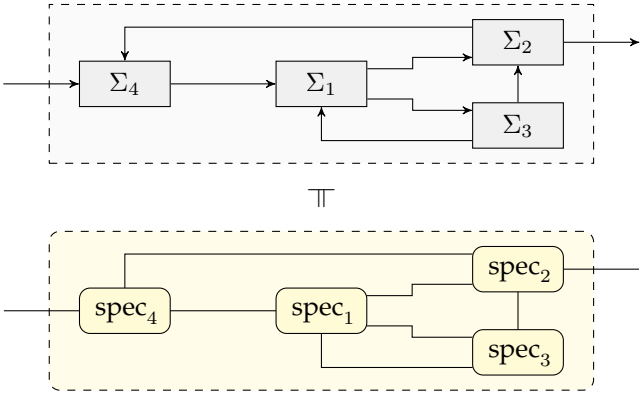

Figure 1.3: Composite specification.

The success of contract theories in the field of computer science has inspired a growing interest in contract-based design in the field of systems and control. Indeed, parametric assume-guarantee contracts are introduced in [47] and used to prove a small-gain theorem. These contracts are also used in [48] for controller synthesis, and in [49] for safety-critical control synthesis in network systems. On the other hand, assume-guarantee contracts that capture invariance properties are introduced in [50] and used for symbolic controller synthesis in [51, 52]. Other applications of these contracts can be found in [53, 54], while the contracts in [55, 56] can be seen as extensions. Contracts are also used to express safety requirements in [57], specifications on dynamics for continuous linear systems in [58], and finite-time reach and infinite-time avoidance in [59]. It is worth noting that the contracts in [47–49] are defined only for discrete-time systems, whereas the contracts in [50–54,57] cannot be used to express specifications on dynamics. The contracts introduced in [55] do not suffer from these limitations, but their generality comes at the expense of algorithms for verification. Finally, although this is not made explicit, the works on compositional and assume-guarantee reasoning in [60–62] are also in the spirit of contract-based design.

1.2 Objective and contributions

The objective of this thesis is to introduce a novel method for expressing rich specifications on dynamical control systems that has the following aspects.

- *Specifications on dynamics.* In contrast to dissipativity and set-invariance, where specifications are typically time-invariant, e.g., time-invariant supply rates and invariant sets, we want this method to enable the expression of specifications on dynamics. Furthermore, in contrast to formal methods, which typically rely on discrete abstractions, we want this method to enable the expression of specifications directly in the continuous domain.

- *Independent design.* We want this method to fully support the independent design of components within interconnected systems. As such, this method would also provide guarantees on the correct integration of components within interconnected systems.

To attain this objective, we draw inspiration from contract theories in computer science and, specifically, the meta-theory in [46]. In particular, we introduce assume-guarantee contracts for linear dynamical systems with inputs and outputs. These contracts serve as specifications through two aspects. First, the assumptions capture the available information about the behaviour of the environment in which the system is expected to operate. Second, the

guarantees capture the required behaviour of the system when it is interconnected with a relevant environment. More precisely, the assumptions represent a set of input trajectories that the system can expect as inputs, whereas the guarantees represent a set of input-output trajectories that the system is permitted to generate. As such, the contracts in this thesis express specifications on dynamics.

The definitions of a contract and its associated notions are formalized using a notion for system comparison. We consider two such notions in this thesis: behavioural inclusion and simulation. The behaviour [63] of a system is defined as the set of trajectories that satisfy the system's equations. Two systems can be compared via their behaviour in the following sense: if the behaviour of one system is contained in the behaviour of another, then the latter can generate a larger variety of trajectories and, thus, has richer dynamics. Similarly, two systems can be compared using the notion of simulation. Simulation is the one-sided version of the notion of bisimulation [64, 65], which is a notion of system equivalence first introduced in the theory of concurrent processes [66]. As already noted in the latter, simulation is stronger than behavioural inclusion if the systems under consideration are non-deterministic, which is the case in this thesis. More importantly, unlike behavioural inclusion, simulation is supported by efficient numerical procedures for verification based on the (controlled) invariant subspace algorithm [67, 68].

We develop a contract theory based on each of the two notions for system comparison. The contracts based on behavioural inclusion are referred to as behavioural contracts, and the contracts based on simulation are referred to as simulation contracts. With this in mind, we make the following contributions in this thesis.

Behavioural contracts. We introduce behavioural contracts as specifications for linear dynamical input-output systems. We develop notions of implementation, refinement and conjunction, which allow us to express, compare and combine specifications using contracts. We characterize implementation and refinement in terms of behavioural inclusions, which, as we show, can be verified algorithmically. Furthermore, we provide necessary and sufficient conditions under which a given contract has an implementation, and we provide a systematic procedure for the construction of an implementation if one exists. This allows behavioural contracts to be used for design as well as verification.

We also introduce two notions of composition for behavioural contracts based on two types of interconnections: series and feedback. Loosely speaking, the composition of two contracts is such that the interconnection of any of their implementations is guaranteed to implement the composition. As such, the notion of composition allows us to reason about interconnected systems based on the contracts for their components. Although our results are stated

only for simple series and feedback interconnections, they can be easily extended to any interconnected system that can be obtained from a sequence of series and feedback interconnections. Furthermore, together with our results on refinement, our results on composition enable the independent design of components within interconnected systems.

Simulation contracts. Even though behavioural contracts are supported by algorithms for verification, these are not necessarily efficient. Moreover, even though we can design an implementation for a given behavioural contract, the procedure does not lend itself to other design problems, e.g., controller synthesis. Motivated by this, we take a slightly different approach and we introduce simulation contracts for linear dynamical input-state-output systems with a driving variable. Like for behavioural contracts, we develop notions of implementation and refinement, this time characterized in terms of simulation. Since simulation can be verified efficiently using the (controlled) invariant subspace algorithm [68], refinement and implementation can also be verified efficiently. Then, using the connection between simulation and geometric control theory [67], we solve two problems related to contract-based design, namely, the construction of an implementation of a given contract, and the construction of a controller that turns a given plant system into an implementation of a given contract. In addition to implementation and refinement, we introduce a notion of series composition for simulation contracts, which allows us to reason about the series interconnection based on the contracts for its components. This presents a first step towards enabling the use of simulation-based contracts for independent design.

1.3 Outline

The outline of this thesis is as follows. Chapter 2 contains a summary of the meta-theory of contracts with a brief discussion of the main ideas behind contract-based design. Then, Chapter 3 introduces behavioural contracts together with the notions of implementation, refinement and conjunction. This continues with Chapter 4, which introduces notions of series and feedback composition for behavioural contracts. Next, Chapter 5 introduces simulation contracts together with notions of implementation, refinement and series composition. Finally, we end with concluding remarks in Chapter 6.

Chapter 2

Meta-theory of contracts

In this chapter, we will discuss the main ideas behind contract-based design. As mentioned in the introduction, these ideas are elegantly encapsulated in the mathematical meta-theory of contracts presented in [46]. The purpose of this meta-theory is to be a formal theory of contracts that focuses on the main aspects of the notions of contract, refinement, conjunction and composition. In the following, we will discuss the meta-theoretic definitions of these notions and their relevance in expressing specifications for components and enabling the independent design of components within interconnected systems. We will split the discussion into two parts. First, we will discuss the notions of contract, refinement and conjunction, which allow us to express, compare and combine specifications for components. Second, we will discuss the notion of composition, which, together with the notion of refinement, enables the independent design of components within interconnected systems. Although we will attempt to be as formal as possible, the main purpose of the following discussion is to convey the basic ideas.

2.1 Contracts as specifications

We begin with a universe of *components* $\mathbb{U}$ for which we want to express specifications using contracts. In this thesis, the universe $\mathbb{U}$ will be the class of linear time-invariant dynamical systems. We treat the components in $\mathbb{U}$ as open systems, that is, each component $\Sigma \in \mathbb{U}$ has external variables that interact with its environment, see Figure 2.1. A key feature of using contracts as specifications is that the environment of a component is taken explicitly into account. We model the environment of a component as another component, and we represent a component operating in a particular environment by an appropriate notion of component *interconnection* $\times$. Then, a component $\mathrm{E} \in \mathbb{U}$ is an *environment* for another component $\Sigma \in \mathbb{U}$ if their interconnection $\mathrm{E} \times \Sigma$

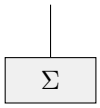

Figure 2.1: A component $\Sigma \in \mathbb{U}$.

is defined and is itself a component in $\mathbb{U}$, see Figure 2.2.

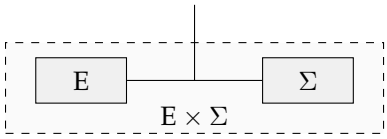

Figure 2.2: A component $\Sigma \in \mathbb{U}$ operating in an environment $E \in \mathbb{U}$.

The specification expressed by a contract needs to be satisfied only when the component operates in a relevant environment. This means that, on an abstract level, a contract must indicate which environments are relevant and which components satisfy the specification expressed by the contract. In other words, the semantics of a *contract* $\mathcal{C}$ is a pair $(\mathbb{E}_\mathcal{C}, \mathbb{I}_\mathcal{C})$ of subclasses of the universe of components $\mathbb{U}$, where $\mathbb{E}_\mathcal{C} \subset \mathbb{U}$ is the class of *compatible environments* and $\mathbb{I}_\mathcal{C} \subset \mathbb{U}$ is the class of *implementations*. We say that $\mathcal{C}$ is *compatible* if $\mathbb{E}_\mathcal{C}$ is non-empty and *consistent* if $\mathbb{I}_\mathcal{C}$ is non-empty. Naturally, we require that E is an environment for Σ for all $E \in \mathbb{E}_\mathcal{C}$ and all $\Sigma \in \mathbb{I}_\mathcal{C}$.

The precise way in which the subclasses of compatible environments and implementations are obtained depends on the context. A common approach, which will also be taken in this thesis, is to define a contract as a pair of components called assumptions and guarantees. Such contracts are referred to as *assume-guarantee* contracts. More precisely, we can define a contract $\mathcal{C} = (A, \Gamma)$ as a pair of *assumptions* $A \in \mathbb{U}$ and *guarantees* $\Gamma \in \mathbb{U}$. Then, the classes of compatible environments and implementations are defined through comparison with the assumptions A and guarantees Γ. Namely, given a relation $\preccurlyeq$ on the universe of components $\mathbb{U}$, we have that $E \in \mathbb{E}_\mathcal{C}$ if $E \preccurlyeq A$, and $\Sigma \in \mathbb{I}_\mathcal{C}$ if $E \times \Sigma \preccurlyeq \Gamma$ for all $E \in \mathbb{E}_\mathcal{C}$. Here, we have implicitly assumed that $E \times \Sigma$ is defined, that is, E is an environment for Σ. This will not be an issue in this thesis because we will define environments in such a way that the interconnection $E \times \Sigma$ is always defined.

Assume-guarantee contracts provide an intuitive interpretation of a contract as a specification for a component through the following two aspects. First, the assumptions A capture the known properties of the environment in which the component Σ is expected to operate. Second, the guarantees capture the properties that we require the component to exhibit when operating in interconnection with a relevant environment. Naturally, the properties

that the assumptions and guarantees capture depend on the definition of the relation $\preccurlyeq$ and the universe of components $\mathbb{U}$.

We want to use contracts not only to express specifications but also to enable the independent design of components within interconnected systems. An essential aspect of the latter is the ability to determine if satisfaction of one specification implies satisfaction of another. This motivates the notion of contract *refinement*. Refinement is used to compare contracts and, in particular, to determine if one contract expresses a stricter specification than another contract. To this end, refinement must ensure the following: if a contract $\mathcal{C}'$ refines another contract $\mathcal{C}$, then any implementation of $\mathcal{C}'$ should be an implementation of $\mathcal{C}$ and should be able to operate in interconnection with any compatible environment of $\mathcal{C}$. Therefore, $\mathcal{C}'$ *refines* $\mathcal{C}$ if

$$\mathbb{E}_{\mathcal{C}'} \supset \mathbb{E}_{\mathcal{C}} \quad \text{and} \quad \mathbb{I}_{\mathcal{C}'} \subset \mathbb{I}_{\mathcal{C}}, \tag{2.1}$$

that is, any compatible environment of $\mathcal{C}$ is a compatible environment of $\mathcal{C}'$, and any implementation of $\mathcal{C}'$ is an implementation of $\mathcal{C}$.

It is easily seen that refinement defines a preorder. Indeed, $\mathcal{C}$ refines itself, hence refinement is reflexive. Furthermore, if $\mathcal{C}''$ refines $\mathcal{C}'$ and $\mathcal{C}'$ refines $\mathcal{C}$, then

$$\mathbb{E}_{\mathcal{C}''} \supset \mathbb{E}_{\mathcal{C}'} \supset \mathbb{E}_{\mathcal{C}} \quad \text{and} \quad \mathbb{I}_{\mathcal{C}''} \subset \mathbb{I}_{\mathcal{C}'} \subset \mathbb{I}_{\mathcal{C}}, \tag{2.2}$$

hence $\mathcal{C}''$ refines $\mathcal{C}$ and, thus, refinement is transitive. Generally, refinement is not antisymmetric, hence it does not define a partial order. For example, given assume-guarantee contracts $\mathcal{C}' = (\mathrm{A}', \Gamma')$ and $\mathcal{C} = (\mathrm{A}, \Gamma)$, we might have that $\mathcal{C}'$ refines $\mathcal{C}$ and $\mathcal{C}$ refines $\mathcal{C}'$ even if $\mathcal{C}'$ and $\mathcal{C}$ are not identical, that is, A' is not identical to A or Γ' is not identical to Γ. Nevertheless, in this case, $\mathcal{C}'_1$ and $\mathcal{C}'_2$ define the same classes of compatible environments and implementations, hence we consider them to be *equivalent*.

Finally, we might have multiple specifications for the same component, perhaps capturing different viewpoints. In such a case, we would like to be able to fuse these specifications into one. This motivates the notion of contract *conjunction*. Suppose that we have two contracts $\mathcal{C}_1$ and $\mathcal{C}_2$ that express specifications for a single component. This means that the component should be an implementation of both $\mathcal{C}_1$ and $\mathcal{C}_2$, and should be able to operate in interconnection with any compatible environment of $\mathcal{C}_1$ or $\mathcal{C}_2$. In other words, the component must belong to $\mathbb{I}_{\mathcal{C}_1} \cap \mathbb{I}_{\mathcal{C}_2}$ and must be able to operate in interconnection with any environment belonging to $\mathbb{E}_{\mathcal{C}_1} \cup \mathbb{E}_{\mathcal{C}_2}$. Ideally, this specification would be expressed by a contract $\mathcal{C}$ such that

$$\mathbb{E}_{\mathcal{C}} = \mathbb{E}_{\mathcal{C}_1} \cup \mathbb{E}_{\mathcal{C}_2} \quad \text{and} \quad \mathbb{I}_{\mathcal{C}} = \mathbb{I}_{\mathcal{C}_1} \cap \mathbb{I}_{\mathcal{C}_2}. \tag{2.3}$$

However, it is not always possible to define such a contract $\mathcal{C}$. Because of this, we only require that

$$\mathbb{E}_{\mathcal{C}} \supset \mathbb{E}_{\mathcal{C}_1} \cup \mathbb{E}_{\mathcal{C}_2} \quad \text{and} \quad \mathbb{I}_{\mathcal{C}} \subset \mathbb{I}_{\mathcal{C}_1} \cap \mathbb{I}_{\mathcal{C}_2}. \tag{2.4}$$

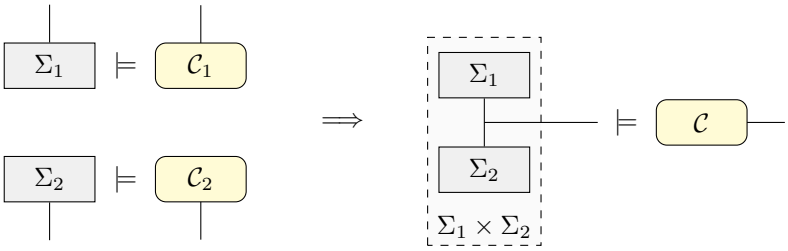

Figure 2.3: Independent design.

Then, any implementation of $\mathcal{C}$ is an implementation of both $\mathcal{C}_1$ and $\mathcal{C}_2$, and can operate in interconnection with any compatible environment of $\mathcal{C}_1$ or $\mathcal{C}_2$. By definition of refinement, the latter holds if and only if $\mathcal{C}$ refines both $\mathcal{C}_1$ and $\mathcal{C}_2$. With this in mind, the *conjunction* of $\mathcal{C}_1$ and $\mathcal{C}_2$, denoted by $\mathcal{C}_1 \wedge \mathcal{C}_2$, is defined as the largest (with respect to refinement) contract that refines both $\mathcal{C}_1$ and $\mathcal{C}_2$. This means that $\mathbb{I}_{\mathcal{C}_1 \wedge \mathcal{C}_2}$ is as large as possible but not larger than $\mathbb{I}_{\mathcal{C}_1} \cap \mathbb{I}_{\mathcal{C}_2}$, whereas $\mathbb{E}_{\mathcal{C}_1 \wedge \mathcal{C}_2}$ is as small as possible but not smaller than $\mathbb{E}_{\mathcal{C}_1} \cup \mathbb{E}_{\mathcal{C}_2}$. In other words, $\mathcal{C}_1 \wedge \mathcal{C}_2$ is the greatest lower bound of the set $\{\mathcal{C}_1, \mathcal{C}_2\}$ with respect to the preorder defined by refinement. Note that the conjunction does not necessarily exist for arbitrary contracts $\mathcal{C}_1$ and $\mathcal{C}_2$.

2.2 Independent design

As already mentioned, we want to use contracts to enable the independent design of components within interconnected systems. We will make this more concrete by considering a simple example. Suppose that we want to design an interconnected system $\Sigma_1 \times \Sigma_2$ that satisfies a global specification expressed by a contract $\mathcal{C}$. Our goal is to assign local 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 is an implementation of $\mathcal{C}_1$ and Σ_2 is an implementation of $\mathcal{C}_2$, then the interconnection $\Sigma_1 \times \Sigma_2$ is an implementation of $\mathcal{C}$. In other words, we would like the implication in Figure 2.3 to hold. This offers the following advantages in the design of interconnected systems:

- *Independent design.* The designer of each component is only concerned with designing an implementation of their assigned local contract and need not concern themselves with the design of the other component, or the integration of the components into the interconnected system. This is especially relevant for the design of complex engineering systems, where the design of components requires specialized expertise and is, thus, usually handled by different (independent) teams.

- *Component substitution.* A component can be substituted for another without compromising the behaviour of the interconnected system as long as the new component is an implementation of the same local contract. In particular, it is not necessary to verify that the new component integrates properly into the interconnected system, and it is not necessary to verify that the resulting interconnected system implements the global contract. This makes upgrading components much simpler.

- *Component reusability.* The same component can be used in different interconnected systems as long as the corresponding local contracts are equivalent. This can potentially allow a variety of interconnected systems to be designed with mostly off-the-shelf components.

With this in mind, to enable independent design, we will introduce a notion of contract *composition*. We want the composition of two contracts $\mathcal{C}_1$ and $\mathcal{C}_2$, denoted by $\mathcal{C}_1 \otimes \mathcal{C}_2$, to be a contract that satisfies the following *composition property*: if Σ_1 and Σ_2 are implementations of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and E is a compatible environment of $\mathcal{C}_1 \otimes \mathcal{C}_2$, then the environment of Σ_1 in $\mathrm{E} \times (\Sigma_1 \times \Sigma_2)$ is a compatible environment of $\mathcal{C}_1$, the environment of Σ_2 in $\mathrm{E} \times (\Sigma_1 \times \Sigma_2)$ is a compatible environment of $\mathcal{C}_2$, and $\Sigma_1 \times \Sigma_2$ is an implementation of $\mathcal{C}_1 \otimes \mathcal{C}_2$. Here, we assume that the interconnection $\mathrm{E} \times (\Sigma_1 \times \Sigma_2)$ can be interpreted as an interconnection $\mathrm{E}_1 \times \Sigma_1$ for some E_1, such that E_1 is the environment of Σ_1 in $\mathrm{E} \times (\Sigma_1 \times \Sigma_2)$. In particular, if $\times$ is both commutative and associative, then $\mathrm{E} \times (\Sigma_1 \times \Sigma_2)$ can be interpreted as $(\mathrm{E} \times \Sigma_2) \times \Sigma_1$, hence the environment of Σ_1 in $\mathrm{E} \times (\Sigma_1 \times \Sigma_2)$ is $\mathrm{E} \times \Sigma_2$. Similarly, the environment of Σ_2 in $\mathrm{E} \times (\Sigma_1 \times \Sigma_2)$ is $\mathrm{E} \times \Sigma_1$. We require these to be compatible environments of the respective contracts because the respective implementations are designed to operate correctly only in interconnection with compatible environments.

There might be none or multiple contracts that satisfy the composition property. Therefore, we say that $\mathcal{C}_1$ and $\mathcal{C}_2$ are *composable* if there exists at least one contract that satisfies the composition property. Then, if $\mathcal{C}_1$ and $\mathcal{C}_2$ are composable, their *composition* $\mathcal{C}_1 \otimes \mathcal{C}_2$ is defined as the smallest (with respect to refinement) contract that satisfies the composition property. In other words, $\mathcal{C}_1 \otimes \mathcal{C}_2$ expresses the strictest specification while still ensuring the satisfaction of the composition property. Note that the composition $\mathcal{C}_1 \otimes \mathcal{C}_2$ does not necessarily exist for arbitrary contracts $\mathcal{C}_1$ and $\mathcal{C}_2$, even if they are composable.

Now, suppose that $\mathcal{C}_1$ and $\mathcal{C}_2$ are such that $\mathcal{C}_1 \otimes \mathcal{C}_2$ refines $\mathcal{C}$. Let Σ_1 and Σ_2 be implementations of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Then, $\Sigma_1 \times \Sigma_2$ is an implementation of $\mathcal{C}_1 \otimes \mathcal{C}_2$ due to the composition property, hence $\Sigma_1 \times \Sigma_2$ is an implementation of $\mathcal{C}$ by definition of refinement. In other words, the definitions of refinement and composition enable the independent design of components within interconnected systems by the following reasoning:

$$\left.\begin{array}{c} \mathcal{C}_1 \otimes \mathcal{C}_2 \text{ refines } \mathcal{C} \\ \textbf{and} \\ \Sigma_1 \text{ implements } \mathcal{C}_1 \\ \Sigma_2 \text{ implements } \mathcal{C}_2 \end{array}\right\} \quad \textbf{imply} \quad \Sigma_1 \times \Sigma_2 \text{ implements } \mathcal{C}$$

The above reasoning can easily be extended to interconnected systems that comprise more than two components by suitably defining composition and, thus, enabling the following reasoning:

$$\left.\begin{array}{c} \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_n \text{ refines } \mathcal{C} \\ \textbf{and} \\ \Sigma_1 \text{ implements } \mathcal{C}_1 \\ \vdots \\ \Sigma_n \text{ implements } \mathcal{C}_n \end{array}\right\} \quad \textbf{imply} \quad \Sigma_1 \times \cdots \times \Sigma_n \text{ implements } \mathcal{C}$$

However, such complex interconnections can also be conveniently handled by applying the above ideas in a hierarchical manner. To this end, in addition to independent design, we would also like to enable independent refinement. This refers to the ability to independently design interconnected systems as components of an interconnected system. To make this concrete, suppose that the designer of the first component wants to design an interconnected system $\Sigma_{11} \times \Sigma_{12}$ instead of a single component Σ_1. To do this independently, we want to be able to assign local contracts $\mathcal{C}_{11}$ and $\mathcal{C}_{12}$ for Σ_{11} and Σ_{12} such that, if Σ_{11} and Σ_{12} are implementations of $\mathcal{C}_{11}$ and $\mathcal{C}_{12}$, respectively, the interconnection $\Sigma_{11} \times \Sigma_{12}$ is an implementation of the local contract $\mathcal{C}_1$. In the context of independent refinement, we also want the interconnection $(\Sigma_{11} \times \Sigma_{12}) \times \Sigma_2$ to be an implementation of the global contract $\mathcal{C}$. In other words, independent refinement allows us to independently design complex interconnected systems in hierarchical stages, starting with a simple interconnection which is refined until the desired interconnected system is obtained, see Figure 2.4.

Note that independent refinement is enabled if the composition $\otimes$ satisfies the following property: if $\mathcal{C}_1'$ refines $\mathcal{C}_1$ and $\mathcal{C}_2'$ refines $\mathcal{C}_2$, then $\mathcal{C}_1' \otimes \mathcal{C}_2'$ refines $\mathcal{C}_1 \otimes \mathcal{C}_2$. Indeed, if $\otimes$ satisfies the independent refinement property, then the designer of the first component can assign local contracts $\mathcal{C}_{11}$ and $\mathcal{C}_{12}$ such that $\mathcal{C}_{11} \otimes \mathcal{C}_{12}$ refines $\mathcal{C}_1$. 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 $\mathcal{C}$, see Figure 2.5. Therefore, instead of designing an implementation Σ_1 of $\mathcal{C}_1$, the designer of the first component can design implementations Σ_{11} and Σ_{12} of $\mathcal{C}_{11}$ and $\mathcal{C}_{12}$, respectively, and the interconnection $(\Sigma_{11} \times \Sigma_{12}) \times \Sigma_2$ would be an implementation of the global contract $\mathcal{C}$.

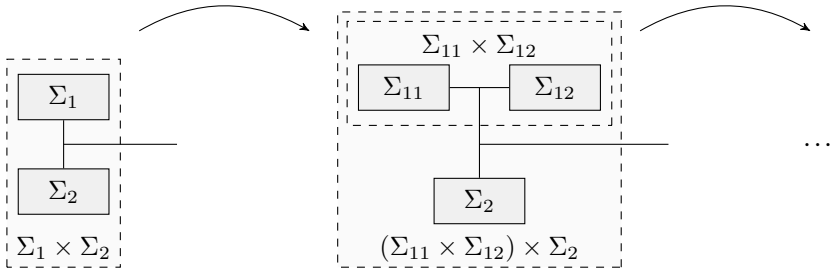

Figure 2.4: Independent refinement.

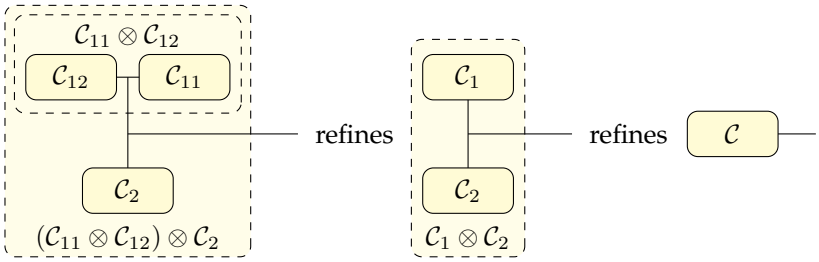

Figure 2.5: Independent refinement using contracts.

We conclude this chapter with a short summary of the relevant notions.

- *Component.* There is an underlying universe of components $\mathbb{U}$.
- *Environment.* An environment for a component $\Sigma \in \mathbb{U}$ is another component $\mathrm{E} \in \mathbb{U}$ such that the interconnection $\mathrm{E} \times \Sigma$ is defined.
- *Contract.* A contract $\mathcal{C}$ defines a pair $(\mathbb{E}_\mathcal{C}, \mathbb{I}_\mathcal{C})$, where $\mathbb{E}_\mathcal{C} \subset \mathbb{U}$ is the class of compatible environments and $\mathbb{I}_\mathcal{C} \subset \mathbb{U}$ is the class of implementations. If $\mathcal{C} = (\mathrm{A}, \Gamma)$ is an assume-guarantee contract, then $\mathrm{E} \in \mathbb{E}_\mathcal{C}$ if $\mathrm{E} \preccurlyeq \mathrm{A}$, and $\Sigma \in \mathbb{I}_\mathcal{C}$ if $\mathrm{E} \times \Sigma \preccurlyeq \Gamma$ for all $\mathrm{E} \in \mathbb{E}_\mathcal{C}$.
- *Refinement.* A contract $\mathcal{C}'$ refines $\mathcal{C}$ if $\mathbb{E}_{\mathcal{C}'} \supset \mathbb{E}_\mathcal{C}$ and $\mathbb{I}_{\mathcal{C}'} \subset \mathbb{I}_\mathcal{C}$.
- *Conjunction.* The conjunction $\mathcal{C}_1 \wedge \mathcal{C}_2$ is the largest contract that refines both $\mathcal{C}_1$ and $\mathcal{C}_2$.
- *Composition.* The composition $\mathcal{C}_1 \otimes \mathcal{C}_2$ is the smallest contract that satisfies the composition property.

Chapter 3

Behavioural contracts

In this chapter, we introduce assume-guarantee contracts as specifications for linear dynamical systems with inputs and outputs.[1] In particular, we define a contract as a pair of linear dynamical systems called *assumptions* and *guarantees*. The assumptions capture the available information about the dynamics of the environment, which provides inputs for the system, thus leading to a class of compatible environments. The guarantees capture the desired dynamics of the system when interconnected with a compatible environment, thus leading to a class of implementations.

We use a notion of system comparison to explicitly relate compatible environments and implementations to assumptions and guarantees. In particular, we make use of the notion of behaviour of a system, defined as the set of trajectories that satisfy the system's equations. In the behavioural approach to systems theory [63], pioneered by Jan C. Willems [71–73], a dynamical system is identified by its behaviour, which is also the vantage point from which other system theoretic concepts are introduced. We can use behaviours to compare systems in the following sense: if the behaviour of a system is contained in the behaviour of another system, then the latter can produce a larger variety of trajectories and, thus, has richer dynamics. In the context of this chapter, we can more appropriately view the latter system as defining a set of permissible trajectories. Then, the behaviour of the former system being contained in the behaviour of the latter means that the former produces only permissible trajectories.

With this interpretation in mind, the assumptions define a set of permissible input trajectories, whereas the guarantees define a set of permissible input-output trajectories. The class of compatible environments consists of all environments that produce only permissible input trajectories, i.e., whose behaviour is contained in the behaviour of the assumptions. On the other

[1] Parts of this chapter have appeared in [69,70].

hand, the class of implementations consists of all systems that produce only permissible input-output trajectories when interconnected with a compatible environment, i.e., whose behaviour when interconnected with a compatible environment is contained in the behaviour of the guarantees. Therefore, as it specifies desired trajectories, a contract expresses a specification on the *dynamics* of a system.

We make the following contributions in this chapter. To begin with, 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 given contract expresses. The condition for implementation takes the form of a behavioural inclusion, which, as we show, can be verified algorithmically, thus allowing contract implementation to be verified algorithmically. We then turn to the characterizing contract *consistency*, which has to do with the existence of an implementation for a given contract. We show that not every contract is consistent, and we obtain necessary and sufficient conditions for consistency that can be verified algorithmically. In the process, we also obtain a procedure for constructing an implementation of a given contract, thus allowing contracts to be used for design, not only verification.

Lastly, we treat the notions of contract refinement and contract conjunction, both defined following the meta-theoretic definitions outlined in Chapter 2. In particular, we obtain necessary and sufficient conditions for refinement that take the form of a pair of behavioural inclusions, thus allowing refinement to be verified algorithmically. On the other hand, we show that the conjunction of two arbitrary contracts does not necessarily exist. Nevertheless, we discuss two special cases where the conjunction does exist, and we provide an explicit expression for it in these cases.

This chapter is structured as follows. In Section 3.1, we review polynomial and rational matrices, as well as some related notions that will be used throughout this and the next chapter. Then, in Section 3.2, we discuss the classes of systems that will be considered throughout this and next chapter, as well as the notion of behaviour and some related results. Our first contribution is in Section 3.3, where we define contracts and characterize contract implementation. Afterwards, in Section 3.4, we characterize contract consistency and provide a procedure for constructing an implementation of a given contract. Lastly, in Section 3.5 and Section 3.6, we treat the notions of refinement and conjunction, respectively, after which we end this chapter with a short discussion in Section 3.7.

3.1 Polynomial and rational matrices

In this section, we will review some definitions and results on polynomial and rational matrices that will be used throughout the rest of this and the next

chapter. For a comprehensive treatment of polynomial and rational matrices, we refer to [74]. Some relevant results can also be found in [63,68,75]. To begin with, we denote the set of polynomials with real coefficients by $\mathbb{R}[s]$ and the set of rational functions with real coefficients by $\mathbb{R}(s)$. A *polynomial matrix* is a matrix whose entries are polynomials, and a *rational matrix* is a matrix whose entries are rational functions. The set of $n \times m$ polynomial matrices is denoted by $\mathbb{R}[s]^{n\times m}$ and the set of $n \times m$ rational matrices is denoted by $\mathbb{R}(s)^{n\times m}$. In particular, the set of polynomial vectors with n entries is denoted by $\mathbb{R}[s]^n$, and the set of rational vectors with n entries is denoted by $\mathbb{R}(s)^n$. Note that a polynomial is also a rational function, hence $\mathbb{R}[s]^{n\times m} \subset \mathbb{R}(s)^{n\times m}$.

The degree of a polynomial $p(s) \in \mathbb{R}[s]$, denoted by $\deg p(s)$, is the degree of its highest-order term. The degree of a rational function $r(s) \in \mathbb{R}(s)$, denoted by $\deg r(s)$, is the difference between the degrees of its numerator and denominator. In other words, given a rational function

$$r(s) = \frac{p(s)}{q(s)}, \tag{3.1}$$

where $p(s), q(s) \in \mathbb{R}[s]$, we have that

$$\deg r(s) = \deg p(s) - \deg q(s). \tag{3.2}$$

Note that the degree of a polynomial coincides with its degree when treated as a rational function. We say that $r(s)$ is *proper* if $\deg p(s) \leq \deg q(s)$ or, equivalently, $\deg r(s) \leq 0$. We say that $r(s)$ is *strictly proper* if $\deg r(s) < 0$. It is easily seen that the product of two (strictly) proper rational functions is also (strictly) proper. Note that every rational function can be written as the sum of a polynomial and a strictly proper rational function. Indeed, we can divide $p(s)$ by $q(s)$ to obtain

$$p(s) = a(s)q(s) + b(s) \tag{3.3}$$

for some polynomials $a(s), b(s) \in \mathbb{R}[s]$ such that $\deg b(s) < \deg q(s)$, and, thus,

$$r(s) = a(s) + \frac{b(s)}{q(s)}. \tag{3.4}$$

We will refer to $a(s)$ as the *polynomial part* of $r(s)$.

In the same vein, the degree of a rational matrix $R(s) \in \mathbb{R}(s)^{n\times m}$ is equal to the maximum of the degrees of its entries, that is,

$$\deg R(s) = \max_{i,j} \deg R_{ij}(s), \tag{3.5}$$

where $R_{ij}(s)$ is the entry on the i'th row and j'th column of $R_(s)$. We say that $R(s)$ is (strictly) proper if all of its entries are (strictly) proper. Therefore,

$R(s)$ is proper if and only if $\deg R(s) \leq 0$, and strictly proper if and only if $\deg R(s) < 0$. Like with rational functions, the product of two (strictly) proper rational matrices is also a (strictly) proper rational matrix. Furthermore, we can write $R(s)$ as the sum of a polynomial matrix and a strictly proper rational matrix by writing each of its entries as the sum of a polynomial and a strictly proper rational function. In other words, we can write

$$R(s) = A(s) + B(s), \tag{3.6}$$

for some polynomial matrix $A(s) \in \mathbb{R}[s]^{n\times m}$ and a strictly proper rational matrix $B(s) \in \mathbb{R}(s)^{n\times m}$. We will refer to $A(s)$ as the polynomial part of $R(s)$. The following result regarding (strictly) proper rational matrices is well-known.

Proposition 3.1. *A rational matrix $R(s) \in \mathbb{R}(s)^{n\times m}$ is proper if and only if*

$$\lim_{s\to\infty} R(s) = R_\infty \tag{3.7}$$

for some real matrix $R_\infty \in \mathbb{R}^{n\times m}$, and strictly proper if and only if $R_\infty = 0$.

Rational functions with real coefficients form a field, just like real numbers. This means that $\mathbb{R}(s)^n$ is a vector space over the field $\mathbb{R}(s)$, just like $\mathbb{R}^n$ is a vector space over the field $\mathbb{R}$. Because of this, rational matrices share many of the properties that real matrices have. We will review some of these properties now. First, a square rational matrix $R(s) \in \mathbb{R}(s)^{n\times n}$ is *invertible* if there exists a rational matrix $T(s) \in \mathbb{R}(s)^{n\times n}$ such that

$$R(s)T(s) = T(s)R(s) = I. \tag{3.8}$$

We refer to $T(s)$ as the *inverse* of $R(s)$, and we denote it by $R(s)^{-1}$. It is well known that a real matrix is invertible if and only if its determinant is nonzero. Similarly, a rational matrix is invertible if and only if its determinant is a nonzero rational function. From the fundamental theorem of algebra, we know that a rational function $r(s) \in \mathbb{R}(s)$ is nonzero if and only if $r(\lambda)$ is nonzero for all but finitely many $\lambda \in \mathbb{C}$, namely, the roots of the nonzero denominator of $r(s)$. With this in mind, the following proposition provides a number of equivalent conditions for invertibility.

Proposition 3.2. *Given a square rational matrix $R(s) \in \mathbb{R}(s)^{n\times n}$, the following statements are equivalent:*

1. *$R(s)$ is invertible;*
2. *$R(\lambda)$ is invertible for all but finitely many $\lambda \in \mathbb{C}$;*
3. *$R(\lambda)$ is invertible for some $\lambda \in \mathbb{C}$;*
4. *$\det R(s)$ is a nonzero rational function;*

5. $\det R(\lambda)$ *is nonzero for all but finitely many* $\lambda \in \mathbb{C}$*;*

6. $\det R(\lambda)$ *is nonzero for some* $\lambda \in \mathbb{C}$*;*

7. $x(s)^\top R(s) = 0$ *implies* $x(s) = 0$ *for all* $x(s) \in \mathbb{R}(s)^n$*.*

The following proposition provides a condition under which the inverse of an invertible proper rational matrix is also proper.

Proposition 3.3. *Suppose that* $R(s) \in \mathbb{R}(s)^{m\times m}$ *is proper. Then*

$$R_\infty = \lim_{s\to\infty} R(s) \tag{3.9}$$

is invertible if and only if $R(s)$ *is invertible and* $R(s)^{-1}$ *is proper.*

Proof. We begin by proving necessity. Suppose that R_∞ is invertible. We will prove that $R(s)$ is invertible by contradiction. Let $x(s) \in \mathbb{R}(s)^m$ be a nonzero rational vector such that

$$x(s)^\top R(s) = 0. \tag{3.10}$$

Without loss of generality, we can assume that $x(s)$ is actually a polynomial vector. Otherwise, we can premultiply $x(s)$ by s^k, where the integer k is large enough, to obtain a polynomial vector $x(s)$ that satisfies (3.10). Now, since $x(s)$ is a nonzero polynomial vector, it follows that $k = \deg x(s)$ is such that $s^{-k}x(s)$ is proper but not strictly proper, hence

$$\lim_{s\to\infty} s^{-k}x(s) = x_\infty \neq 0. \tag{3.11}$$

In view of (3.10), we have that

$$\lim_{s\to\infty} s^{-k}x(s)^\top R(s) = x_\infty^\top R_\infty = 0, \tag{3.12}$$

which implies that $x_\infty = 0$ because R_∞ is invertible. This is a contradiction, which shows that $R(s)$ is invertible. Note that $R(\frac{1}{s})$ is a rational matrix. Since

$$\lim_{s\to 0} R(\tfrac{1}{s}) = R_\infty \tag{3.13}$$

is invertible, it follows by continuity that $R(\frac{1}{s})$ is invertible in a neighbourhood around $s = 0$. Therefore, we have that

$$\lim_{s\to\infty} R(s)^{-1} = \lim_{s\to 0} R(\tfrac{1}{s})^{-1} = \Big(\lim_{s\to 0} R(\tfrac{1}{s})\Big)^{-1} = R_\infty^{-1} \tag{3.14}$$

hence $R(s)^{-1}$ is proper.

We proceed by proving sufficiency. Suppose that $R(s)$ is invertible and $R(s)^{-1}$ is proper. This means that

$$\lim_{s\to\infty} R(s)^{-1} = \bar{R}_\infty, \tag{3.15}$$

for some $\bar{R}_\infty \in \mathbb{R}^{m\times m}$. Consequently,

$$R(s)R(s)^{-1} = I \tag{3.16}$$

implies that

$$\lim_{s\to\infty} R(s)R(s)^{-1} = R_\infty \bar{R}_\infty = I, \tag{3.17}$$

which shows that R_∞ is invertible. □

The *row (column) rank* of a rational matrix is given by the number of its linearly independent (over the field $\mathbb{R}(s)$) rows (columns). A rational matrix has *full row (column) rank* if all of its rows (columns) are linearly independent. In other words, the rational matrix $R(s) \in \mathbb{R}(s)^{n\times m}$ has full row rank if $x(s)^\top R(s) = 0$ implies $x(s) = 0$ for all $x(s) \in \mathbb{R}(s)^n$. Due to the last statement in Proposition 3.2, a square rational matrix is invertible if and only if it has full row rank. On the other hand, it is well-known that a real matrix $R \in \mathbb{R}^{n\times m}$ has full row rank if and only if $RR^\top$ is invertible. Similarly, a rational matrix $R(s) \in \mathbb{R}(s)^{n\times m}$ has full row rank if and only if $R(s)R(s)^\top$ is invertible. Consequently, in the spirit of Proposition 3.2, we obtain the following proposition.

Proposition 3.4. *Given a rational matrix $R(s) \in \mathbb{R}(s)^{n\times m}$, the following statements are equivalent:*

1. *$R(s)$ has full row rank;*
2. *$R(\lambda)$ has full row rank for all but finitely many $\lambda \in \mathbb{R}$;*
3. *$R(\lambda)$ has full row rank for some $\lambda \in \mathbb{R}$;*
4. *$R(s)R(s)^\top$ is invertible;*
5. *$R(s)T(s) = I$ for some rational matrix $T(s) \in \mathbb{R}(s)^{m\times n}$.*

The following proposition follows almost immediately from Proposition 3.2 and Proposition 3.4.

Proposition 3.5. *If the rational matrix $R(s) \in \mathbb{R}(s)^{n\times m}$ has full row rank, then there exists a matrix $R' \in \mathbb{R}^{(n-m)\times m}$ such that the rational matrix*

$$\begin{bmatrix} R(s) \\ R' \end{bmatrix} \tag{3.18}$$

is square and invertible.

Proof. Due to Proposition 3.4, since $R(s)$ has full row rank, there exists $\lambda \in \mathbb{R}$ such that $R(\lambda) \in \mathbb{R}^{n\times m}$ has full row rank. Consequently, there exists a matrix $R' \in \mathbb{R}^{(n-m)\times m}$ such that

$$\begin{bmatrix} R(\lambda) \\ R' \end{bmatrix} \tag{3.19}$$

is square and invertible. Then, (3.18) is invertible due to Proposition 3.2. □

Since polynomial matrices are also rational matrices, the definitions of invertibility and full row (column) rank are also applicable to polynomial matrices. However, there is a stronger notion of invertibility for polynomial matrices, where the inverse is required to also be a polynomial matrix. In particular, a square polynomial matrix $P(s) \in \mathbb{R}[s]^{n\times n}$ is *unimodular* if there exists a *polynomial matrix* $Q(s) \in \mathbb{R}[s]^{n\times n}$ such that

$$P(s)Q(s) = Q(s)P(s) = I. \tag{3.20}$$

Note that $Q(s)$ is the inverse of $P(s)$ when treated as a rational matrix, hence we will denote it by $P(s)^{-1}$. As the determinant of a polynomial matrix is a polynomial, and $P(s)Q(s) = I$ only if $\det P(s) \det Q(s) = 1$, it follows that a polynomial matrix is unimodular only if its determinant is a nonzero constant. The converse is also true [68, Corollary 7.4], hence the following proposition.

Proposition 3.6. *Given a square polynomial matrix $P(s) \in \mathbb{R}[s]^{n\times n}$, the following statements are equivalent:*

1. *$P(s)$ is unimodular;*
2. *$P(\lambda)$ is invertible for all $\lambda \in \mathbb{R}$;*
3. *$\det P(s)$ is a nonzero constant;*
4. *$\det P(\lambda)$ is nonzero for all $\lambda \in \mathbb{R}$.*

For the remainder of this section, we will focus on a particular type of polynomial matrix that has full row rank, namely, a row-reduced polynomial matrix. Suppose that the polynomial matrix $G(s) \in \mathbb{R}[s]^{n\times m}$ has full row rank. Let d_i be the degree of the i'th row of $G(s)$, that is, $d_i = \deg G_i(s)$, where $G_i(s)$ is the i'th row of $G(s)$. We will refer to d_i as the i'th row degree of $G(s)$. Note that, by definition of d_i, there exists a unique nonzero $G_i^h \in \mathbb{R}^{1\times m}$ and a unique $G_i^l(s) \in \mathbb{R}[s]^{1\times m}$ such that

$$G_i(s) = s^{d_i} G_i^h + G_i^l(s), \tag{3.21}$$

and $\deg G_i^l(s) < d_i$, that is, $s^{-d_i} G_i^l(s)$ is strictly proper. Consequently, if we define the *row degree matrix* of $G(s)$ as

$$D(s) = \begin{bmatrix} s^{d_1} & 0 & \cdots & 0 \\ 0 & s^{d_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & s^{d_n} \end{bmatrix}, \tag{3.22}$$

then there exist unique $G^h \in \mathbb{R}^{n\times m}$ and $G^l(s) \in \mathbb{R}[s]^{n\times m}$ such that

$$G(s) = D(s)G^h + G^l(s), \tag{3.23}$$

each row of G^h is nonzero and $D(s)^{-1}G^l(s)$ is strictly proper. With this in mind, consider the following definition.

Definition 3.1. Consider a polynomial matrix $G(s) \in \mathbb{R}[s]^{n\times m}$ and write

$$G(s) = D(s)G^h + G^l(s), \tag{3.24}$$

where $D(s) \in \mathbb{R}[s]^{n\times n}$ is the row degree matrix of $G(s)$, $G^h \in \mathbb{R}^{n\times m}$ has no zero rows, and $G^l(s) \in \mathbb{R}[s]^{n\times m}$ is such that $D(s)^{-1}G^l(s)$ is strictly proper. We say that $G(s)$ is *row-reduced* if G^h has full row rank.

Row-reduced polynomial matrices play an important role in the following sections due to their favourable properties, which we will explore now. To begin with, we can show that a row-reduced polynomial matrix must have full row rank. However, not every polynomial matrix that has full row rank is row-reduced. Indeed, the polynomial matrix

$$G(s) = \begin{bmatrix} s & 1 \\ s & 2 \end{bmatrix} \tag{3.25}$$

clearly has full row rank, but writing it in the form (3.23) yields

$$D(s) = \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix}, \quad G^h = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \quad G^l(s) = \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix}, \tag{3.26}$$

and G^h does not have full row rank. Nevertheless, we can always transform $G(s)$ into a row-reduced polynomial matrix by a series of row operations. To show this, we need the following intermediate result.

Lemma 3.7. *Suppose that $G(s) \in \mathbb{R}[s]^{n\times m}$ has full row rank but is not row-reduced. Then, there exists a unimodular matrix $U(s)$ such that the sum of the row degrees of $U(s)G(s)$ is smaller than the sum of the row degrees of $G(s)$.*

Proof. To begin with, write

$$G(s) = D(s)G^h + G^l(s), \tag{3.27}$$

where $D(s) \in \mathbb{R}[s]^{n\times n}$ is the row degree matrix of $G(s)$, $G^h \in \mathbb{R}^{m\times n}$ has no zero rows, and $G^l(s) \in \mathbb{R}[s]^{n\times m}$ is such that $D(s)^{-1}G^l(s)$ is strictly proper. The assumption that $G(s)$ is not row-reduced implies that G^h does not have full row rank. Therefore, there exists a nonzero $x \in \mathbb{R}^n$ such that $x^\top G^h = 0$. Let d_i indicate the i'th row degree of $G(s)$ and note that $\deg D(s)x = d_j$ for some $j \in \{1, \dots, n\}$. This implies that

$$z(s) = s^{d_j} D(s)^{-1} x \tag{3.28}$$

is a polynomial vector whose j'th entry is a nonzero constant, i.e.,

$$z(s)^\top = \begin{bmatrix} z_{1j}(s)^\top & z_j & z_{jn}(s)^\top \end{bmatrix}, \tag{3.29}$$

where $z_{1j} \in \mathbb{R}[s]^{j-1}$, $z_{jn} \in \mathbb{R}[s]^{n-j}$ and $z_j \in \mathbb{R} \setminus \{0\}$. With this in mind, consider the polynomial matrix

$$U(s) = \begin{bmatrix} I & 0 & 0 \\ z_{1j}(s)^\top & z_j & z_{jn}(s)^\top \\ 0 & 0 & I \end{bmatrix}. \tag{3.30}$$

and note that $\det U(s) = z_j$, that is, $U(s)$ is unimodular. Furthermore, the i'th row of $U(s)G(s)$ is equal to the i'th row of $G(s)$ for $i \neq j$, hence the i'th row degree of $U(s)G(s)$ is equal to the i'th row degree of $G(s)$ for $i \neq j$. On the other hand, the j'th row of $U(s)G(s)$ is given by

$$z(s)^\top G(s) = s^{d_j} x^\top D(s)^{-1} \left(D(s)G^h + G^l(s) \right) = s^{d_j} x^\top D(s)^{-1} G^l(s), \tag{3.31}$$

where we used the assumption that $x^\top G^h = 0$. Since $D(s)^{-1}G^l(s)$ is strictly proper and x is constant, it follows that $\deg z(s)^\top G(s) < d_j$, hence the j'th row degree of $U(s)G(s)$ is smaller than the j'th row degree of $G(s)$. Finally, this implies that the sum of the row degrees of $U(s)G(s)$ is smaller than the sum of the row degrees of $G(s)$, as desired. □

The following proposition shows that any row-reduced polynomial matrix has full row rank and any polynomial matrix that has full row rank can be transformed into a row-reduced polynomial matrix by left multiplication with an appropriately chosen unimodular matrix.

Proposition 3.8. *The polynomial matrix $G(s) \in \mathbb{R}[s]^{n\times m}$ has full row rank if and only if there exists a unimodular matrix $U(s) \in \mathbb{R}[s]^{n\times n}$ such that $U(s)G(s)$ is row-reduced.*

Proof. We begin by proving sufficiency. Suppose that there exists a unimodular matrix $U(s)$ such that $U(s)G(s)$ is row-reduced, that is,

$$U(s)G(s) = D(s)G^h + G^l(s), \tag{3.32}$$

where $D(s) \in \mathbb{R}[s]^{n\times n}$ is the row degree matrix of $U(s)G(s)$, $G^h \in \mathbb{R}^{n\times m}$ has full row rank and $G^l(s) \in \mathbb{R}[s]^{n\times m}$ is such that $D(s)^{-1}G^l(s)$ is strictly proper. Since $U(s)$ is unimodular, $G(s)$ has full row rank if and only if $U(s)G(s)$ has full row rank. Similarly, since $D(s)$ is invertible, $U(s)G(s)$ has full row rank if and only if $G^h + D(s)^{-1}G^l(s)$ has full row rank. We will prove that the latter has full row rank by contradiction. To this end, let $x(s) \in \mathbb{R}(s)^n$ be a nonzero rational vector such that

$$x(s)^\top \left(G^h + D(s)^{-1}G^l(s) \right) = 0. \tag{3.33}$$

Without loss of generality, we can assume that $x(s)$ is actually a polynomial vector. Otherwise, we can premultiply $x(s)$ with s^k, where the integer k is

large enough, to obtain a polynomial vector $x(s)$ that satisfies (3.33). With this in mind, let $k = \deg x(s)$ and note that $s^{-k}x(s)$ is proper but not strictly proper. In other words, there exists a nonzero vector $x_\infty \in \mathbb{R}^n$ such that

$$\lim_{s\to\infty} s^{-k}x(s) = x_\infty. \tag{3.34}$$

Note that (3.33) holds if and only if

$$s^{-k}x(s)^\top \left(G^h + D(s)^{-1}G^l(s)\right) = 0. \tag{3.35}$$

Taking the limit of the latter as $s \to \infty$ yields

$$x_\infty^\top G^h = 0, \tag{3.36}$$

where we used the assumption that $D(s)^{-1}G^l(s)$ is strictly proper, hence it converges to 0 as $s \to \infty$. Since G^h has full row rank, it follows that $x_\infty = 0$, which is a contradiction. Therefore, due to Proposition 3.4, $G^h + D(s)^{-1}G^l(s)$ has full row rank and, thus, $G(s)$ has full row rank.

We proceed by proving necessity. Suppose that $G(s)$ has full row rank. If $G(s)$ is already row-reduced, then we can take $U(s) = I$. Otherwise, due to Lemma 3.7, there exists a unimodular matrix $U_1(s)$ such that the sum of the row degrees of $G_1(s) = U_1(s)G(s)$ is smaller than the sum of the row degrees of $G(s)$. If $G_1(s)$ is row-reduced, then we can take $U(s) = U_1(s)$. Otherwise, we can repeat this to obtain a sequence of polynomial matrices $G_1(s)$, $G_2(s)$, $\ldots$, where $G_{k+1}(s) = U_{k+1}(s)G_k(s)$ for some unimodular matrix $U_{k+1}(s)$, and the sum of the row degrees of $G_{k+1}(s)$ is smaller that the sum of the row degrees of $G_k(s)$. Since the sum of the row degrees of any polynomial matrix is nonnegative, it follows that the sequence $G_1(s)$, $G_2(s)$, $\ldots$, terminates at some step K. But the only way this can happen is if $G_K(s)$ is row-reduced, hence

$$U(s) = U_K(s)\cdots U_1(s) \tag{3.37}$$

is such that $U(s)G(s)$ is row-reduced, as desired. □

The following result is the main motivation for considering row-reduced polynomial matrices.

Proposition 3.9. *Suppose that the polynomial matrix $G(s) \in \mathbb{R}[s]^{n\times m}$ is row-reduced and consider the polynomial matrix $H(s) \in \mathbb{R}[s]^{n\times p}$. Let $D(s) \in \mathbb{R}[s]^{n\times n}$ be the row degree matrix of $G(s)$. Then, there exists a proper rational matrix $R(s) \in \mathbb{R}(s)^{m\times p}$ such that*

$$G(s)R(s) = H(s) \tag{3.38}$$

if and only if $D(s)^{-1}H(s)$ is proper, that is, the i'th row degree of $H(s)$ is less than or equal to the i'th row degree of $G(s)$.

Proof. We begin by proving necessity. Suppose that (3.38) holds for some proper $R(s) \in \mathbb{R}(s)^{m\times p}$. Since $G(s)$ is row-reduced, we can write

$$G(s) = D(s)G^h + G^l(s), \tag{3.39}$$

where $D(s) \in \mathbb{R}[s]^{n\times n}$ is the row degree matrix of $G(s)$, $G^h \in \mathbb{R}^{n\times m}$ has full row rank and $G^l(s) \in \mathbb{R}[s]^{n\times m}$ is such that $D(s)^{-1}G^l(s)$ is strictly proper. In particular, we have that $D(s)^{-1}G(s)$ is proper and thus

$$D(s)^{-1}H(s) = D(s)^{-1}G(s)R(s) \tag{3.40}$$

is proper as a product of proper rational matrices.

We proceed by proving sufficiency. Suppose that $D(s)^{-1}H(s)$ is proper. Since G^h has full row rank, there exists $\bar{G}^h \in \mathbb{R}^{m\times n}$ such that $G^h\bar{G}^h = I$. Furthermore, the polynomial matrix

$$G(s)\bar{G}^h = D(s) + G^l(s)\bar{G}^h \tag{3.41}$$

is square and in row-reduced form, hence, due to Proposition 3.8, $G(s)\bar{G}^h$ has full row rank and is, thus, invertible. Therefore, the rational matrix

$$R(s) = \bar{G}^h \left(G(s)\bar{G}^h\right)^{-1} H(s) \tag{3.42}$$

is such that (3.38) holds. It remains to show that $R(s)$ is proper. We can insert the product $D(s)D(s)^{-1} = I$ to the left of $H(s)$ in (3.42) to obtain

$$R(s) = \bar{G}^h \left(D(s)^{-1}G(s)\bar{G}^h\right)^{-1} D(s)^{-1}H(s), \tag{3.43}$$

where we note that

$$\lim_{s\to\infty} D(s)^{-1}G(s)\bar{G}^h = \lim_{s\to\infty} \left(I + D(s)^{-1}G^l(s)\bar{G}^h\right) = I, \tag{3.44}$$

because $D(s)^{-1}G^l(s)$ is strictly proper. In view of Proposition 3.3, it follows that

$$\left(D(s)^{-1}G(s)\bar{G}^h\right)^{-1} \tag{3.45}$$

is proper, and since $D(s)^{-1}H(s)$ is proper, we conclude that $R(s)$ in (3.42) is proper as a product of proper rational matrices. □

We can see Proposition 3.9 as generalizing the requirement that $G(s)^{-1}H(s)$ is proper to the case where $G(s)$ is not square. Indeed, the following corollary follows almost immediately.

Corollary 3.10. *Suppose that the polynomial matrix $G(s) \in \mathbb{R}[s]^{n\times n}$ is invertible and row-reduced. Then the polynomial matrix $H(s) \in \mathbb{R}[s]^{n\times p}$ is such that $G(s)^{-1}H(s)$ is proper if and only if $D(s)^{-1}H(s)$ is proper, where $D(s) \in \mathbb{R}[s]^{n\times n}$ is the row degree matrix of $G(s)$.*

Proof. The proof follows from Proposition 3.9 after noting that (3.38) holds if and only if $R(s) = G(s)^{-1}H(s)$. □

Another useful property of row-reduced polynomial matrices is concerned with how their row degrees change after left multiplication with a polynomial row vector, referred to as the "predictable degree" property [76, Main Theorem, 4(b)], see also [75, Theorem 6.3-13]. Here, we extend this property to left multiplication with a rational row vector.

Proposition 3.11. *Suppose that the polynomial matrix $G(s) \in \mathbb{R}[s]^{n\times m}$ is row-reduced, and consider the nonzero rational row vector $T(s) \in \mathbb{R}(s)^{1\times n}$. Then*

$$\deg T(s)G(s) = \max_{i:T_i(s)\neq 0} \deg T_i(s) + d_i, \tag{3.46}$$

where d_i is the i'th row degree of $G(s)$.

Proof. There exists an integer k such that $s^kT(s)$ is a polynomial row vector. Let $\hat{T}(s) = s^kT(s)$ and note that

$$\deg T(s)G(s) = \deg \hat{T}(s)G(s) - k \tag{3.47}$$

By transposing the statement in [75, Theorem 6.3-13], we obtain

$$\deg \hat{T}(s)G(s) = \max_{i:\hat{T}_i(s)\neq 0} \deg \hat{T}_i(s) + d_i. \tag{3.48}$$

Note that $\hat{T}_i(s) = 0$ if and only if $T_i(s) = 0$, and $\deg \hat{T}_i(s) = \deg T_i(s) + k$, hence (3.46) follows from (3.47) and (3.48). □

We conclude this section with a result concerning full row rank polynomial matrices.

Proposition 3.12. *Suppose that the polynomial matrix $A(s) \in \mathbb{R}[s]^{n\times m}$ has full row rank. Then, there exists a permutation matrix $P \in \mathbb{R}^{m\times m}$ such that*

$$A(s)P = \begin{bmatrix} A_1(s) & A_2(s) \end{bmatrix}, \tag{3.49}$$

where the polynomial matrix $A_1(s) \in \mathbb{R}[s]^{n\times n}$ is invertible and the polynomial matrix $A_2(s) \in \mathbb{R}[s]^{n\times(m-n)}$ is such that $A_1(s)^{-1}A_2(s)$ is proper.

Proof. In view of Lemma 3.8 and the assumption that $A(s)$ has full row rank, it follows that there exists a unimodular matrix $U(s)$ such that $U(s)A(s)$ is in row-reduced form, i.e.,

$$U(s)A(s) = D(s)A^h + A^l(s), \tag{3.50}$$

where $D(s) \in \mathbb{R}[s]^{n\times m}$ is the row degree matrix of $U(s)A(s)$, $A^h \in \mathbb{R}^{n\times m}$ has full row rank and $A^l(s) \in \mathbb{R}[s]^{n\times m}$ is such that $D(s)^{-1}A^l(s)$ is strictly proper.

Since A^h has full row rank, there exists a permutation matrix $P \in \mathbb{R}^{m\times m}$ such that

$$A^h P = \begin{bmatrix} A_1^h & A_2^h \end{bmatrix}, \tag{3.51}$$

where $A_1^h \in \mathbb{R}^{n\times n}$ is invertible and $A_2^h \in \mathbb{R}^{n\times(m-n)}$. Let

$$A^l(s)P = \begin{bmatrix} A_1^l(s) & A_2^l(s) \end{bmatrix}, \tag{3.52}$$

where $A_1^l(s) \in \mathbb{R}[s]^{n\times n}$ and $A_2^l(s) \in \mathbb{R}[s]^{n\times(m-n)}$, and

$$A(s)P = \begin{bmatrix} A_1(s) & A_2(s) \end{bmatrix}, \tag{3.53}$$

where $A_1(s) \in \mathbb{R}[s]^{n\times n}$ and $A_2(s) \in \mathbb{R}[s]^{n\times(m-n)}$. Note that

$$U(s)A_1(s) = D(s)A_1^h + A_1^l(s), \tag{3.54}$$

where A_1^h is invertible and $D(s)^{-1}A_1^l(s)$ is strictly proper because $D(s)^{-1}A^l(s)$ is strictly proper. This means that $U(s)A_1(s)$ is in row-reduced form and, thus, invertible. On the other hand, we have that

$$U(s)A_2(s) = D(s)A_2^h + A_2^l(s) \tag{3.55}$$

where $D(s)^{-1}A_2^l(s)$ is strictly proper because $D(s)^{-1}A^l(s)$ is strictly proper. This means that $D(s)^{-1}U(s)A_2(s)$ is proper hence, due to Corollary 3.10, the rational matrix

$$\left(U(s)A_1(s)\right)^{-1} U(s)A_2(s) = A_1(s)^{-1}A_2(s) \tag{3.56}$$

is proper, as desired. □

3.2 System classes and behaviours

In this section, we will introduce the class of systems that will be considered throughout this and next chapter. Along the way, we will review some definitions and results from the behavioural approach to systems theory [63, 73]. In the following, as well as throughout this thesis, we denote the space of smooth functions from $\mathbb{R}$ to $\mathbb{R}^k$ by $\mathscr{C}_k^\infty$.

Consider a system of the form

$$\Sigma : \begin{cases} \dot{x} = Ax + Bu, \\ y = Cx + Du, \end{cases} \tag{3.57}$$

where $x \in \mathscr{C}_n^\infty$ is the state trajectory, $u \in \mathscr{C}_m^\infty$ is the input trajectory, and $y \in \mathscr{C}_p^\infty$ is the output trajectory. We refer to Σ as an *input-state-output* system. We regard the input u and the output y as external variables that can interact with

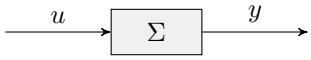

Figure 3.1: The system Σ.

the environment, but the state x as an internal variable that cannot interact with the environment, as illustrated in Figure 3.1.

Our goal is to develop a formal method for expressing specifications on the dynamic behaviour of such systems, which is part of a framework that facilitates the independent design of components within interconnected systems, as discussed in Chapter 1. We will do this by introducing contracts as specifications and developing appropriate notions of contract refinement and contract composition, as outlined in Chapter 2. Recall that a distinguishing feature of contracts is that they take the environment of a system explicitly into account. In particular, a contract specifies a desired behaviour of the system only when it is interconnected with a relevant environment. As the environment of the system has access only to its external variables, this means that we are only interested in the behaviour of the external variables u and y, whereas the behaviour of the internal variable x can be disregarded. To formalize this, we will utilize the behavioural approach to systems theory.

The *external behaviour* of Σ is defined as

$$\mathfrak{B}(\Sigma) = \left\{ (u,y) \in \mathscr{C}^{\infty}_{m+p} \;\middle|\; \exists x \in \mathscr{C}^{\infty}_{n} \text{ s.t. (3.57) holds} \right\}. \tag{3.58}$$

In the behavioural approach to systems theory, the system Σ is seen as a representation of its external behaviour $\mathfrak{B}(\Sigma)$. The same external behaviour can be represented by different systems. For example, it is well-known that the external behaviour is invariant under state-space transformation, that is, if Σ' is obtained from Σ by a state-space transformation, then $\mathfrak{B}(\Sigma') = \mathfrak{B}(\Sigma)$. On the other hand, the same external behaviour can be represented by a system belonging to a completely different class.

In particular, consider a system of the form

$$\Sigma : P\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = Q\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u, \tag{3.59}$$

where $u \in \mathscr{C}^{\infty}_{m}$, $y \in \mathscr{C}^{\infty}_{p}$, and $P(s)$ and $Q(s)$ are polynomial matrices. Here, $P\left(\frac{\mathrm{d}}{\mathrm{d}t}\right)$ and $Q\left(\frac{\mathrm{d}}{\mathrm{d}t}\right)$ are linear differential operators obtained after substituting the indeterminate s for the differential operator $\frac{\mathrm{d}}{\mathrm{d}t}$ in $P(s)$ and $Q(s)$. If $P(s)$ is invertible and $P(s)^{-1}Q(s)$ is proper, then we say that Σ is in *input-output form* [63, Section 3.3], and refer to Σ as an *input-output* system. The external behaviour of Σ of the form (3.59) is defined in the obvious way, namely,

$$\mathfrak{B}(\Sigma) = \left\{ (u,y) \in \mathscr{C}^{\infty}_{m+p} \;\middle|\; \text{(3.59) holds} \right\}. \tag{3.60}$$

In view of [77, Theorem 6.2], the external behaviour of any input-state-output system is equal to the external behaviour of an appropriately chosen

input-output system, and vice versa. For example, the external behaviour of a single-input single-output input-state-output system of the form (3.57), where $D = 0$ and (A, C) is observable, is equal to the external behaviour of an input-output system of the form (3.59) with

$$P(s) = \det(sI - A), \qquad Q(s) = \det(sI - A)^{-1}C(sI - A)^{-1}B, \tag{3.61}$$

where we note that $P(s)$ is indeed square and invertible, and $P(s)^{-1}Q(s)$ is proper. More generally, we can *eliminate* [63, Section 6.2] the state from the equations of a given input-state-output system to obtain an input-output system with the same external behaviour, see [63, Section 6.3] for a treatment of this in the single-input single-output case. Conversely, we can obtain an input-state-output system with the same external behaviour as the one of a given input-output system. The procedure for this is similar to the procedure for obtaining a state-space realization of a given transfer function ($P(s)^{-1}Q(s)$ is the transfer function of a system of the form (3.59)). We refer the reader to [63, Section 6.4] for a treatment of the single-input single-output case.

Input-output systems are more convenient for analysis involving external behaviours since they involve only the external variables u and y. Therefore, throughout the rest of this chapter, we will consider input-output systems instead of input-state-output systems, Nevertheless, we stress that the two classes are completely interchangeable due to [77, Theorem 6.2].

Remark 3.1. *The conditions on $P(s)$ and $Q(s)$ in the input-output system Σ given by* (3.59) *can be interpreted as follows. First, the condition that $P(s)$ is square and invertible guarantees that u is free in $\mathfrak{B}(\Sigma)$, that is, for all $u \in \mathscr{C}_m^\infty$, there exists $y \in \mathscr{C}_p^\infty$ such that $(u, y) \in \mathfrak{B}(\Sigma)$. Furthermore, for a fixed u, none of the components of y are free in $\mathfrak{B}(\Sigma)$, that is, u is* maximally free*. Second, the condition that $P(s)^{-1}Q(s)$ is proper guarantees that Σ is* non-anticipating*, that is, y does not depend on the derivatives of u. Note that $P(s)^{-1}Q(s)$ is, in fact, the transfer function from u to y in Σ. See [63, Section 3.3] for details.*

The concept of behaviour allows one to compare the (external) dynamics of different systems. In particular, if $\mathfrak{B}(\Sigma_1) \subset \mathfrak{B}(\Sigma_2)$, then, for a given input trajectory, 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 (external) dynamics than Σ_1. Alternatively, we can view Σ_2 as defining a set of permissible input-output trajectories, namely, the external behaviour $\mathfrak{B}(\Sigma_2)$. Then, the inclusion $\mathfrak{B}(\Sigma_1) \subset \mathfrak{B}(\Sigma_2)$ holds if and only if Σ_1 produces only permissible input-output trajectories. In other words, we can interpret Σ_2 as expressing a specification on the dynamics of Σ_1 via behavioural inclusion. This interpretation is at the core of our definition of a contract.

Behavioural inclusion plays a major role in the contract theory that will be developed in this and the next chapter. The following proposition pro-

vides an algebraic characterization of behavioural inclusion that will be used regularly.

Proposition 3.13. *The behaviours*

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

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

Proof. Suppose that $R_2(s) = M(s)R_1(s)$ for some polynomial matrix $M(s)$. If $w \in \mathfrak{B}_1$, then $R_1(\frac{\mathrm{d}}{\mathrm{d}t})w = 0$ and

$$R_2\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) w = M\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) R_1\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) w = 0,$$

hence $w \in \mathfrak{B}_2$, which shows that $\mathfrak{B}_1 \subset \mathfrak{B}_2$. To show the converse, suppose that $\mathfrak{B}_1 \subset \mathfrak{B}_2$, that is, $R_1(\frac{\mathrm{d}}{\mathrm{d}t})w = 0$ implies $R_2(\frac{\mathrm{d}}{\mathrm{d}t})w = 0$. Due to [78, Lemma 2.1], it follows that there exists a polynomial matrix $M(s)$ such that $R_2(s) = M(s)R_1(s)$. □

In particular, given two input-output systems

$$\Sigma_j : P_j\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = Q_j\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u, \quad j \in \{1, 2\}, \tag{3.62}$$

we have that

$$\mathfrak{B}(\Sigma_j) = \left\{ (u, y) \in \mathscr{C}_{m+p}^\infty \;\middle|\; \left[P_j\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) - Q_j\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) \right] \begin{bmatrix} u \\ y \end{bmatrix} = 0 \right\}, \quad j \in \{1, 2\}, \tag{3.63}$$

hence, due to Proposition 3.13, $\mathfrak{B}(\Sigma_1) \subset \mathfrak{B}(\Sigma_2)$ if and only if there exists a polynomial matrix $M(s)$ such that

$$\begin{bmatrix} P_2(s) & -Q_2(s) \end{bmatrix} = M(s) \begin{bmatrix} P_1(s) & -Q_1(s) \end{bmatrix}. \tag{3.64}$$

The following proposition utilizes the Smith canonical form [74, Section 1.8] to produce a condition for the existence of such a polynomial matrix $M(s)$.

Proposition 3.14. *Let $R_1(s)$ and $R_2(s)$ be polynomial matrices and assume that $R_1(s)$ has full row rank. Let $U_1(s)$ and $V_1(s)$ be unimodular matrices that bring $R_1(s)$ to its Smith canonical form, that is,*

$$R_1(s) = U_1(s) \begin{bmatrix} D_1(s) & 0 \end{bmatrix} V_1(s) \tag{3.65}$$

where $D_1(s)$ is an invertible diagonal polynomial matrix. Then there exists a polynomial matrix $M(s)$ such that $R_2(s) = M(s)R_1(s)$ if and only if the following conditions hold:

1. $R_2(s)V_1(s)^{-1} \begin{bmatrix} 0 \\ I \end{bmatrix} = 0$;

2. $R_2(s)V_1(s)^{-1}\begin{bmatrix} D_1(s)^{-1} \\ 0 \end{bmatrix}$ *is a polynomial matrix.*

Proof. We begin by proving necessity. Suppose that there exists a polynomial matrix $M(s)$ such that $R_2(s) = M(s)R_1(s)$. Then we obtain

$$R_2(s)V_1(s)^{-1} = \begin{bmatrix} M(s)U_1(s)D_1(s) & 0 \end{bmatrix},$$

hence conditions 1 and 2 hold, the latter because $M(s)U_1(s)$ is a polynomial matrix.

We proceed by proving sufficiency. Suppose that conditions 1 and 2 hold. In view of condition 2, we have that

$$M(s) = R_2(s)V_1(s)^{-1}\begin{bmatrix} D_1(s)^{-1} \\ 0 \end{bmatrix}U_1(s)^{-1}$$

is a polynomial matrix. Then, we can use condition 1 to obtain

$$\begin{aligned} M(s)R_1(s) &= R_2(s)V_1(s)\begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}V_1(s)^{-1} \\ &= R_2(s)V_1(s)\begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}V_1(s)^{-1} = R_2(s), \end{aligned}$$

which concludes the proof. □

Note that the assumption on $R_1(s)$ in Proposition 3.14 is met for any input-output system. In particular, we have that $\begin{bmatrix} P_1(s) & -Q_1(s) \end{bmatrix}$ has full row rank because $P_1(s)$ is invertible, hence we can use Proposition 3.14 to check whether (3.64) holds and, thus, whether $\mathfrak{B}(\Sigma_1) \subset \mathfrak{B}(\Sigma_2)$. In other words, Proposition 3.13 and Proposition 3.14 provide us with an algorithmic procedure for verifying behavioural inclusion.

Remark 3.2. *More generally, as shown in [63, Theorem 2.5.23], given a behaviour*

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

we can always find a polynomial matrix $R'(s)$ such that

$$\mathfrak{B} = \left\{ w \in \mathscr{C}_k^\infty \;\middle|\; R'\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right)w = 0 \right\}$$

and $R'(s)$ has full row rank. The latter is called a minimal representation *of the behaviour $\mathfrak{B}$. This means that the assumption on $R_1(s)$ in Proposition 3.14 is not restrictive since we can always obtain a minimal representation of $\mathfrak{B}_1$ before checking whether $\mathfrak{B}_1 \subset \mathfrak{B}_2$.*

We conclude this section with the following corollary of Proposition 3.13 regarding equality of behaviours.

Corollary 3.15. *The behaviours*

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

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

Proof. Since $U(s)$ is a polynomial matrix and $R_2(s) = U(s)R_1(s)$, Proposition 3.13 yields $\mathfrak{B}_1 \subset \mathfrak{B}_2$. Similarly, since $U(s)^{-1}$ is a polynomial matrix and $R_1(s) = U(s)^{-1}R_2(s)$, Proposition 3.13 yields $\mathfrak{B}_2 \subset \mathfrak{B}_1$, hence $\mathfrak{B}_1 = \mathfrak{B}_2$. □

Remark 3.3. *The converse of Corollary 3.15 is true when the polynomial matrices $R_1(s)$ and $R_2(s)$ have full row rank. Indeed, if $\mathfrak{B}_1 = \mathfrak{B}_2$, then, due to Proposition 3.13, there exist polynomial matrices $M_1(s)$ and $M_2(s)$ such that*

$$R_2(s) = M_2(s)R_1(s) \quad \textit{and} \quad R_1(s) = M_1(s)R_2(s). \tag{3.66}$$

Consequently, we obtain

$$R_2(s) = M_2(s)M_1(s)R_2(s) \quad \textit{and} \quad R_1(s) = M_1(s)M_2(s)R_1(s). \tag{3.67}$$

Since $R_1(s)$ and $R_2(s)$ have full row rank, we must have that

$$I = M_2(s)M_1(s) \quad \textit{and} \quad I = M_1(s)M_2(s), \tag{3.68}$$

which is the case if and only if $M_1(s)$ and $M_2(s)$ are square and inverses of each other, that is, $M_1(s)$ and $M_2(s)$ are unimodular.

3.3 Contracts

In this section, we define contracts and introduce the notion of contract implementation, which shows how a contract serves as a formal specification for the external behaviour of a system. We also establish a necessary and sufficient condition for contract implementation, and we show how it can be verified.

Consider the input-output system Σ given by (3.59). As an open system, Σ operates in interconnection with its environment, which is responsible for providing it with input trajectories. Therefore, we define an *environment* E as a system of the form

$$\mathrm{E} : 0 = E\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u, \tag{3.69}$$

where $u \in \mathscr{C}_m^\infty$ and $E(s)$ is a polynomial matrix. The environment E defines the behaviour

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{E}) = \{ u \in \mathscr{C}_m^\infty \mid (3.69) \text{ holds} \}. \tag{3.70}$$

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

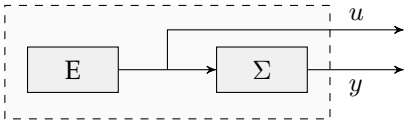

Figure 3.2: The interconnection $\mathrm{E} \wedge \Sigma$.

interconnection of Σ with E is obtained by setting the input generated by E as input of Σ. This yields the system

$$\mathrm{E} \wedge \Sigma : \begin{bmatrix} P\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \\ 0 \end{bmatrix} y = \begin{bmatrix} Q\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \\ E\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \end{bmatrix} u, \tag{3.71}$$

which is represented graphically in Figure 3.2. As a design goal, we are interested in guaranteeing properties of the external behaviour

$$\mathfrak{B}(\mathrm{E} \wedge \Sigma) = \left\{ (u, y) \in \mathscr{C}^{\infty}_{m+p} \;\middle|\; (3.71) \text{ holds} \right\} \tag{3.72}$$

Since this is partially determined by the environment E, any available information about E can ease the design burden on the system Σ and should thus be taken into account. To formalize this, we will introduce two more systems. First, the assumptions A are a system of the form

$$\mathrm{A} : 0 = A\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) u, \tag{3.73}$$

where $u \in \mathscr{C}^{\infty}_{m}$ and $A(s)$ is a polynomial matrix. Just like an environment, the assumptions A represent the input behaviour

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) = \left\{ u \in \mathscr{C}^{\infty}_{m} \mid (3.69) \text{ holds} \right\}. \tag{3.74}$$

Second, the guarantees Γ are a system of the form

$$\Gamma : G\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) y = H\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) u, \tag{3.75}$$

where $u \in \mathscr{C}^{\infty}_{m}$, $y \in \mathscr{C}^{\infty}_{p}$, and $G(s)$ and $H(s)$ are polynomial matrices. The guarantees Γ represent the external behaviour

$$\mathfrak{B}(\Gamma) = \left\{ (u, y) \in \mathscr{C}^{\infty}_{m+p} \;\middle|\; (3.75) \text{ holds} \right\}, \tag{3.76}$$

just like the interconnection $\mathrm{E} \wedge \Sigma$ of a system with its environment. With this in mind, we define a contract as follows.

Definition 3.2. A *contract* $\mathcal{C} = (\mathrm{A}, \Gamma)$ is a pair of assumptions and guarantees.

The interpretation of a contract as a specification is given in the following definition.

Definition 3.3. An environment E is *compatible* with $\mathcal{C} = (\mathrm{A}, \Gamma)$ if

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{E}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}). \tag{3.77}$$

An input-output system Σ *implements* $\mathcal{C}$ if

$$\mathfrak{B}(\mathrm{E} \wedge \Sigma) \subset \mathfrak{B}(\Gamma) \tag{3.78}$$

for all environments E compatible with $\mathcal{C}$.

Definition 3.3 has the following aspects. First, the assumptions capture the available information about the environment, thus leading to a class of compatible environments. Second, the guarantees represent the desired behaviour of the system when interconnected with any compatible environment, thus leading to a class of implementations. These two aspects of a contract constitute a formal specification for the external behaviour of a system.

We identify a contract with the classes of compatible environments and implementations that it defines. Therefore, we consider two contracts equivalent if they define the same classes of compatible environments and implementations.

Definition 3.4. The contracts $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent if:

1. an environment is compatible with $\mathcal{C}_1$ if and only if it is compatible with $\mathcal{C}_2$;

2. an input-output system implements $\mathcal{C}_1$ if and only if it implements $\mathcal{C}_2$.

Remark 3.4. *The classes of compatible environments and implementations of a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ are determined by the behaviours $\mathfrak{B}_{\mathrm{i}}(\mathrm{A})$ and $\mathfrak{B}(\Gamma)$ rather than A and Γ themselves. Therefore, another contract $\mathcal{C}' = (\mathrm{A}', \Gamma')$ is equivalent to $\mathcal{C}$ if $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}')$ and $\mathfrak{B}(\Gamma) = \mathfrak{B}(\Gamma')$, even if $\mathrm{A} \neq \mathrm{A}'$ or $\Gamma \neq \Gamma'$. 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 $\mathfrak{B}(\Gamma)$, that is, they are given by* (3.73) *and* (3.75)*, where the polynomial matrices $A(s)$ and $\begin{bmatrix} G(s) & -H(s) \end{bmatrix}$ have full row rank. As mentioned in Remark 3.2, such representations can always be obtained.*

Definition 3.3 suggests that checking contract implementation requires the construction of all compatible environments. The following theorem shows that this is not necessary and contract implementation can be verified directly from the assumptions and guarantees.

Theorem 3.1. *An input-output system Σ implements $\mathcal{C} = (\mathrm{A}, \Gamma)$ if and only if*

$$\mathfrak{B}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}(\Gamma). \tag{3.79}$$

Proof. Suppose that $\mathfrak{B}(\mathrm{A}\wedge\Sigma) \subset \mathfrak{B}(\Gamma)$ and let E be an environment compatible with $\mathcal{C}$. If $(u, y) \in \mathfrak{B}(\mathrm{E} \wedge \Sigma)$ then $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{E}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$ and $(u, y) \in \mathfrak{B}(\Sigma)$, hence $(u, y) \in \mathfrak{B}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}(\Gamma)$. This shows that $\mathfrak{B}(\mathrm{E} \wedge \Sigma) \subset \mathfrak{B}(\Gamma)$ for all compatible environments E, thus Σ implements $\mathcal{C}$. Conversely, suppose that Σ is an implementation of $\mathcal{C}$. Then $\mathfrak{B}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}(\Gamma)$ because A is compatible with $\mathcal{C}$. □

Remark 3.5. *Note that $\mathfrak{B}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}(\Gamma)$ if and only if $\mathfrak{B}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}(\mathrm{A} \wedge \Gamma)$, hence the class of implementations of $\mathcal{C} = (\mathrm{A}, \Gamma)$ is determined by $\mathfrak{B}(\mathrm{A} \wedge \Gamma)$ rather than $\mathfrak{B}(\Gamma)$ alone. Therefore, we can replace Γ by Γ' without changing the class of implementations as long as $\mathfrak{B}(\mathrm{A} \wedge \Gamma) = \mathfrak{B}(\mathrm{A} \wedge \Gamma')$. In particular, this means that $\mathcal{C}$ is equivalent to $\mathcal{C}' = (\mathrm{A}, \mathrm{A} \wedge \Gamma)$.*

Theorem 3.1 tells us that implementation can be verified by checking a behavioural inclusion condition. For this, we can first make use of Proposition 3.13 first to obtain the following corollary of Theorem 3.1.

Corollary 3.16. *Consider the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$, where the assumptions* A *are given by* (3.73) *and the guarantees* Γ *are given by* (3.75)*. Then, an input-output system Σ of the form* (3.59) *implements $\mathcal{C}$ if and only if there exist polynomial matrices $T(s)$ and $M(s)$ such that*

$$\begin{bmatrix} G(s) & -H(s) \end{bmatrix} = \begin{bmatrix} T(s) & M(s) \end{bmatrix} \begin{bmatrix} P(s) & -Q(s) \\ 0 & -A(s) \end{bmatrix}. \tag{3.80}$$

The existence of the polynomial matrices $T(s)$ and $M(s)$ in Corollary 3.16 can be verified using Proposition 3.14. However, to do that, we need the polynomial matrix

$$\begin{bmatrix} P(s) & -Q(s) \\ 0 & -A(s) \end{bmatrix} \tag{3.81}$$

to have full row rank. Since $P(s)$ is square and invertible, this is the case if and only if $A(s)$ has full row rank, which, due to Remark 3.4, can be assumed without loss of generality. In other words, Corollary 3.16 and Proposition 3.14 provide us with an algorithmic procedure for verifying that a given input-output system implements a given contract.

Remark 3.6. *Even though the results in this chapter are stated for input-output systems, they remain true when input-state-output systems are considered instead, as explained in Section 3.2. Nevertheless, some additional effort is required when verifying that a given system implements a given contract. In particular, due to Theorem 3.1, an input-state-output system Σ of the form* (3.57) *implements the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ if and only if $\mathfrak{B}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}(\Gamma)$. However, as Σ involves the state x, we cannot directly use Proposition 3.13 and Proposition 3.14 to verify this. Instead, we can do the following. Define the full behaviour of Σ as*

$$\mathfrak{B}_f(\Sigma) = \left\{ (u, y, x) \in \mathscr{C}^{\infty}_{m+p+n} \;\middle|\; \text{(3.57) } \textit{holds} \right\}, \tag{3.82}$$

and note that the full behaviour of $\mathrm{A} \wedge \Sigma$ *is given by*

$$\mathfrak{B}_f(\mathrm{A}\wedge\Sigma) = \left\{(u,y,x) \in \mathscr{C}^\infty_{m+p+n} \;\middle|\; u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \text{ and } (u,y,x) \in \mathfrak{B}_f(\Sigma)\right\}. \quad (3.83)$$

It is easily seen that $\mathfrak{B}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}(\Gamma)$ *if and only if* $\mathfrak{B}_f(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}(\Gamma) \times \mathscr{C}^\infty_n$. *Due to Proposition 3.13, if* A *and* Γ *are given by* (3.73) *and* (3.75), *respectively, the latter holds if and only if there exist polynomial matrices* $T(s)$, $M(s)$ *and* $R(s)$ *such that*

$$\begin{bmatrix} G(s) & -H(s) & 0 \end{bmatrix} = \begin{bmatrix} T(s) & M(s) & R(s) \end{bmatrix} \begin{bmatrix} 0 & -B & sI-A \\ I & -D & -C \\ 0 & A(s) & 0 \end{bmatrix}. \quad (3.84)$$

As explained in Remark 3.4, without loss of generality, we can assume that $A(s)$ *has full row rank. Since* I *and* $sI - A$ *also have full row rank, we can use Proposition 3.14 to verify that* (3.84) *holds and, thus, that* Σ *implements* $\mathcal{C}$.

Remark 3.7. *A special class of guarantees is obtained when* $H(s) = 0$ *in* (3.75). *In such a case, the guarantees* Γ *given by* (3.75) *represent the behaviour*

$$\mathfrak{B}_{\mathrm{o}}(\Gamma) = \left\{y \in \mathscr{C}^\infty_p \;\middle|\; G\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right)y = 0\right\} \quad (3.85)$$

where the subscript o indicates that $\mathfrak{B}_{\mathrm{o}}(\Gamma)$ *is in terms of* y, *which is the output of an input-output system* Σ. *We refer to* $\mathfrak{B}_{\mathrm{o}}(\Gamma)$ *as an* output behaviour *and we refer to* Γ *as* output guarantees. *Note that* $\mathfrak{B}(\Gamma) = \mathscr{C}^\infty_m \times \mathfrak{B}_{\mathrm{o}}(\Gamma)$. *Therefore, due to Theorem 3.1, an input-output system* Σ *implements a contract* $\mathcal{C} = (\mathrm{A}, \Gamma)$ *with output guarantees* Γ *if and only if* $\mathfrak{B}_{\mathrm{o}}(\mathrm{A}\wedge\Sigma) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma)$, *where* $\mathfrak{B}_{\mathrm{o}}(\mathrm{A}\wedge\Sigma)$ *is obtained by projecting the external behaviour* $\mathfrak{B}(\mathrm{A} \wedge \Sigma)$ *onto* y, *that is,*

$$\mathfrak{B}_{\mathrm{o}}(\mathrm{A} \wedge \Sigma) = \left\{y \in \mathscr{C}^\infty_p \;\middle|\; \exists u \in \mathscr{C}^\infty_m \text{ s.t. } (u,y) \in \mathfrak{B}(\mathrm{A} \wedge \Sigma)\right\} \quad (3.86)$$

Contracts with output guarantees have properties that make characterizing contract-related concepts simpler, as will become apparent in the following sections.

We conclude this section with a simple practical example that illustrates how contracts can be used to express specifications.

Example 3.1. Suppose that we have two ships on the open sea, one much bigger than the other. The large ship has a crane which moves cargo to the smaller ship. We want the crane to be such that the cargo descends to the smaller ship at a given constant 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 modelled simply as

$$\tau_l \dot{q}_l = -q_l + d, \quad \tau_s \dot{q}_s = -q_s + d, \quad (3.87)$$

where d is the water surface displacement caused by waves, while τ_l and τ_s are constants that represent how much the vertical displacement changes

due to 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

$$\dot{q}_c - \dot{q}_s = -k(q_c - q_s), \tag{3.88}$$

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. To begin with, the input and output of the crane are given by

$$u = \begin{bmatrix} q_s \\ q_l \\ \dot{q}_l \end{bmatrix} \quad \text{and} \quad y = q_c. \tag{3.89}$$

Note that $\dot{u}_2 = u_3$, and, thus, subtracting the two equations in (3.87) yields

$$\tau_s \dot{u}_1 + u_1 - u_2 - \tau_l u_3 = 0. \tag{3.90}$$

Therefore, the assumptions A are given by (3.73) with

$$A(s) = \begin{bmatrix} 0 & s & -1 \\ \tau_s s + 1 & -1 & -\tau_l \end{bmatrix}. \tag{3.91}$$

Note that the assumptions are on the relative motion of the two ships, that is, there are no assumptions on the water surface displacement d. Meanwhile, in view of (3.88), the guarantees Γ are given by (3.75) with

$$G(s) = s + k \quad \text{and} \quad H(s) = \begin{bmatrix} s + k & 0 & 0 \end{bmatrix}. \tag{3.92}$$

Now, the specification on the crane is captured by the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$, that is, the crane is an input-output system Σ that needs to implement $\mathcal{C}$.

We claim that the crane satisfies this specification if it is designed to lower the cargo according to

$$\dot{q}_c = -kq_c + \left(k - \frac{1}{\tau_s}\right) q_s + \frac{1}{\tau_s} q_l + \frac{\tau_l}{\tau_s} \dot{q}_l. \tag{3.93}$$

To show this, note that the latter is equal to

$$\dot{y} + ky = \left(k - \frac{1}{\tau_s}\right) u_1 + \frac{1}{\tau_s} u_2 + \frac{\tau_l}{\tau_s} u_3, \tag{3.94}$$

hence the claim is that the system Σ given by (3.59) with

$$P(s) = s + k, \quad Q(s) = \begin{bmatrix} k - \dfrac{1}{\tau_s} & \dfrac{1}{\tau_s} & \dfrac{\tau_l}{\tau_s} \end{bmatrix} \tag{3.95}$$

implements $\mathcal{C}$. Note that Σ is in input-output form because $P(s)$ is a nonzero polynomial and $P(s)^{-1}Q(s)$ is proper. Furthermore, the polynomial matrix

$$M(s) = \begin{bmatrix} 0 & \dfrac{1}{\tau_s} \end{bmatrix} \tag{3.96}$$

is such that $H(s) = Q(s) + M(s)A(s)$, hence

$$\begin{bmatrix} G(s) & -H(s) \end{bmatrix} = \begin{bmatrix} 1 & M(s) \end{bmatrix} \begin{bmatrix} P(s) & -Q(s) \\ 0 & -A(s) \end{bmatrix} \tag{3.97}$$

which, due to Corollary 3.16, implies that Σ implements $\mathcal{C}$.

Note that we can relax the assumptions A while keeping Σ as an implementation. Indeed, since the first component of $M(s)$ is 0, it is straightforward to show that Σ implements $\mathcal{C}' = (\mathrm{A}', \Gamma)$, where

$$\mathrm{A}' : 0 = \begin{bmatrix} \tau_s \frac{\mathrm{d}}{\mathrm{d}t} + 1 & -1 & -\tau_l \end{bmatrix} u. \tag{3.98}$$

Since $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}')$, A' represents weaker assumptions than A.

On the other hand, note that $\mathfrak{B}(\Sigma) \not\subset \mathfrak{B}(\Gamma)$. Therefore, without assumptions, even if the crane were to lower the cargo according to (3.93), the cargo would not be guaranteed to descend according to (3.88). This illustrates the benefit of explicitly including assumptions about the environment when using contracts to express specifications.

Finally, note that the guarantees Γ themselves are an input-output system, and they obviously implement $\mathcal{C}$. In fact, since $\mathfrak{B}(\mathrm{A}' \wedge \Gamma) \subset \mathfrak{B}(\Gamma)$, Γ implements $\mathcal{C}' = (\mathrm{A}', \Gamma)$ for any assumptions A'.

3.4 Consistency

In this section, we will turn our attention to system design. As explained in the last section, Corollary 3.16 and Proposition 3.14 provide us with an algorithmic procedure for verifying whether a given input-output system implements a given contract. However, in the context of system design, we would like to *construct* an implementation for a given contract. Before we attempt to do that, we should know whether an implementation exists. This is the issue of contract consistency, defined below.

Definition 3.5. A contract $\mathcal{C}$ is *consistent* if it has an implementation.

In what follows, we will provide necessary and sufficient conditions for consistency of a given contract and, in the process, we will obtain a particular implementation of the contract. To begin with, we note that not every contract is consistent. One reason is that u is free in $\mathfrak{B}(\Sigma)$ when Σ is an input-output system, see Remark 3.1, hence any restrictions on u imposed by the

guarantees must already be present in the assumptions. We can formalize this observation as a behavioural inclusion. To this end, the input behaviour of a system that involves both u and y is given by projecting the external behaviour onto u. For guarantees Γ, this yields

$$\mathfrak{B}_{\mathrm{i}}(\Gamma) = \left\{ u \in \mathscr{C}_m^\infty \;\middle|\; \exists y \in \mathscr{C}_p^\infty \text{ s.t. } (u,y) \in \mathfrak{B}(\Gamma) \right\}. \tag{3.99}$$

Consequently, we obtain the following necessary condition for consistency.

Lemma 3.17. *The contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ is consistent only if $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\Gamma)$.*

Proof. Since $\mathcal{C}$ is consistent, there exists an input-output system Σ such that $\mathfrak{B}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}(\Gamma)$. In view of Remark 3.1, we have that u is free in $\mathfrak{B}(\Sigma)$, that is, for all $u \in \mathscr{C}_m^\infty$, there exists $y \in \mathscr{C}_p^\infty$ such that $(u,y) \in \mathfrak{B}(\Sigma)$. This means that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A} \wedge \Sigma) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$, hence $\mathfrak{B}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}(\Gamma)$ only if $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\Gamma)$. □

Remark 3.8. *If Γ are output guarantees, then the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ is consistent for any assumptions* A*. Indeed, recall from Remark 3.7 that an input-output system Σ implements $\mathcal{C}$ if and only if $\mathfrak{B}_{\mathrm{o}}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma)$. Note that*

$$\Sigma : y = 0 \tag{3.100}$$

is an input-output system such that $\mathfrak{B}_{\mathrm{o}}(\Sigma) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma)$. Consequently, we have that $\mathfrak{B}_{\mathrm{o}}(\mathrm{A} \wedge \Sigma) = \mathfrak{B}_{\mathrm{o}}(\Sigma) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma)$, hence Σ implements $\mathcal{C}$ and, thus, $\mathcal{C}$ is consistent.

Unfortunately, the inclusion $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\Gamma)$ is generally not sufficient for the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ to be consistent. This is demonstrated by the following example.

Example 3.2. Consider the assumptions A given by (3.73) with $A(s) = 0$, and the guarantees Γ given by (3.75) with $G(s) = 1$ and $H(s) = s$. It is easy to see that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) = \mathfrak{B}_{\mathrm{i}}(\Gamma) = \mathscr{C}_1^\infty$, and in particular, that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\Gamma)$. Nevertheless, we will show that $\mathcal{C} = (\mathrm{A}, \Gamma)$ is not consistent. Consider an input-output system Σ given by (3.59). Note that $\mathfrak{B}(\mathrm{A} \wedge \Sigma) = \mathfrak{B}(\Sigma)$, hence Σ implements $\mathcal{C} = (\mathrm{A}, \Gamma)$ if and only if $\mathfrak{B}(\Sigma) \subset \mathfrak{B}(\Gamma)$. From Proposition 3.13, we know that $\mathfrak{B}(\Sigma) \subset \mathfrak{B}(\Gamma)$ if and only if there exists a polynomial $M(s)$ such that

$$\begin{bmatrix} 1 & s \end{bmatrix} = M(s) \begin{bmatrix} P(s) & Q(s) \end{bmatrix}. \tag{3.101}$$

But this implies that $M(s) \neq 0$ and $P(s)^{-1}Q(s) = s$, which contradicts the assumption that Σ is an input-output system and shows that $\mathcal{C}$ is not consistent.

Example 3.2 shows that u being free in $\mathfrak{B}(\Sigma)$ for an input-output system Σ is not the only reason why some contracts are not consistent. Indeed, as explained in Remark 3.1, if Σ is given by (3.59), then u being free in $\mathfrak{B}(\Sigma)$ follows solely from the condition that $P(s)$ is invertible, and is unrelated to the condition that $P(s)^{-1}Q(s)$ is proper. In order to understand the role of the latter in contract consistency, we will first define a type of contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ where the condition that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\Gamma)$ is vacuously satisfied.

Definition 3.6. A contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ is *row-reduced* if A and Γ are given by (3.73) and (3.75), respectively, where $A(s)$ and $G(s)$ are row-reduced.

As shown in the proof of [63, Theorem 6.2.6], if Γ is given by (3.75), where $G(s)$ has full row rank, then u is free in $\mathfrak{B}(\Gamma)$, that is, $\mathfrak{B}_{\mathrm{i}}(\Gamma) = \mathscr{C}_m^\infty$. Therefore, $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\Gamma)$ for any assumptions A. On the other hand, in view of Remark 3.4, without loss of generality, we can assume that A is given by (3.73), where $A(s)$ has full row rank. In other words, requiring that $A(s)$ and $G(s)$ have full row rank is quite natural, and not restrictive when considering consistent contracts. However, the definition of a row-reduced contract requires something extra, namely, that $A(s)$ and $G(s)$ are row-reduced. The relevance of this requirement will become apparent later in this section. In the meantime, we have the following result, which shows that requiring a contract to be row-reduced is also not restrictive when considering consistent contracts.

Lemma 3.18. *The contract $\mathcal{C}$ is consistent only if it is equivalent to a row-reduced contract.*

Proof. We will show that there exists a row-reduced contract $\mathcal{C}' = (\mathrm{A}', \Gamma')$ such that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}') = \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$ and $\mathfrak{B}(\mathrm{A} \wedge \Gamma') = \mathfrak{B}(\mathrm{A} \wedge \Gamma)$. In view of Remark 3.4 and Remark 3.5, this would imply that $\mathcal{C}'$ is equivalent to $\mathcal{C}$. With this in mind, let A and Γ be given by (3.73) and (3.75), respectively. As mentioned in Remark 3.4, we can assume that $A(s)$ and $\begin{bmatrix} G(s) & -H(s) \end{bmatrix}$ have full row rank. Then, due to Proposition 3.8, there exists a unimodular matrix $U(s)$ such that

$$A'(s) = U(s)A(s) \tag{3.102}$$

is row-reduced. Moreover, due to Corollary 3.15, the assumptions

$$\mathrm{A}' : 0 = A'\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u \tag{3.103}$$

are such that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}') = \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$, as desired.

For the construction of Γ', we will consider two cases depending on whether $G(s)$ has full row rank or not. First, suppose that $G(s)$ has full row rank. In view of Proposition 3.8, there exists a unimodular matrix $V(s)$ such that

$$G'(s) = V(s)G(s) \tag{3.104}$$

is row-reduced. Then, taking $H'(s) = V(s)H(s)$ yields the guarantees

$$\Gamma' : G'\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y = H'\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u, \tag{3.105}$$

which, due to Corollary 3.15, are such that $\mathfrak{B}(\Gamma') = \mathfrak{B}(\Gamma)$. This also means that $\mathfrak{B}(\mathrm{A} \wedge \Gamma') = \mathfrak{B}(\mathrm{A} \wedge \Gamma)$, as desired.

Second, suppose that $G(s)$ does not have full row rank. In view of [63, Theorem 6.2.6], there exists a unimodular matrix $V(s)$ such that

$$V(s)G(s) = \begin{bmatrix} G''(s) \\ 0 \end{bmatrix}, \quad V(s)H(s) = \begin{bmatrix} H''(s) \\ H_u(s) \end{bmatrix}, \tag{3.106}$$

where $G''(s)$, $H'(s)$ and $H_u(s)$ are polynomial matrices, and $G''(s)$ has full row rank. Furthermore, from the same theorem, we have that

$$\mathfrak{B}_{\mathrm{i}}(\Gamma) = \left\{ u \in \mathscr{C}_m^\infty \;\middle|\; 0 = H_u\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u \right\}. \tag{3.107}$$

Since $\mathcal{C}$ is consistent, it follows from Lemma 3.17 that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\Gamma)$, hence, due to Proposition 3.13, there exists a polynomial matrix $M(s)$ such that

$$H_u(s) = M(s)A(s). \tag{3.108}$$

Consider the guarantees

$$\Gamma'' : G''\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = H''\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right). \tag{3.109}$$

Note that $(u, y) \in \mathfrak{B}(\mathrm{A} \wedge \Gamma'')$ if and only if

$$\begin{bmatrix} G''\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) & -H''\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \\ 0 & -A\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \end{bmatrix} \begin{bmatrix} y \\ u \end{bmatrix} = 0. \tag{3.110}$$

Using (3.108), the latter holds if and only if

$$\begin{bmatrix} G''\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) & -H''\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \\ 0 & -H_u\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \\ 0 & -A\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \end{bmatrix} \begin{bmatrix} y \\ u \end{bmatrix} = 0. \tag{3.111}$$

Since (3.106) holds and $V(s)$ is unimodular, the latter holds if and only if

$$\begin{bmatrix} G\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) & -H\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \\ 0 & -A\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \end{bmatrix} \begin{bmatrix} y \\ u \end{bmatrix} = 0, \tag{3.112}$$

that is, $(u, y) \in \mathfrak{B}(\mathrm{A} \wedge \Gamma')$. This shows that $\mathfrak{B}(\mathrm{A} \wedge \Gamma'') = \mathfrak{B}(\mathrm{A} \wedge \Gamma)$. Since $G''(s)$ has full row rank, as already shown, there exist guarantees Γ' as in (3.105), where $G'(s)$ is row-reduced, such that $\mathfrak{B}(\mathrm{A} \wedge \Gamma') = \mathfrak{B}(\mathrm{A} \wedge \Gamma'')$. In particular, this implies that $\mathfrak{B}(\mathrm{A} \wedge \Gamma') = \mathfrak{B}(\mathrm{A} \wedge \Gamma)$, as desired.

In conclusion, we have found A' and Γ' such that the contract $\mathcal{C}' = (\mathrm{A}', \Gamma')$ is row-reduced, $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}') = \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$ and $\mathfrak{B}(\mathrm{A} \wedge \Gamma') = \mathfrak{B}(\mathrm{A} \wedge \Gamma)$. This means that $\mathcal{C}'$ is equivalent to $\mathcal{C}$, which concludes the proof. □

For the remainder of this section, we will consider row-reduced contracts. We stress, however, that any consistent contract can be transformed into an equivalent row-reduced contract, as shown in Lemma 3.18. With this in mind, the following lemma captures the requirement that $P(s)^{-1}Q(s)$ must be proper for any implementation Σ given by (3.59).

Lemma 3.19. *Suppose that the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ is row-reduced, where A and Γ are given by* (3.73) *and* (3.75)*, respectively. Then, $\mathcal{C}$ is consistent if and only if there exists a polynomial matrix $M(s)$ such that the rational matrix*

$$D(s)^{-1}\left(H(s) - M(s)A(s)\right) \tag{3.113}$$

is proper, where $D(s)$ is the row degree matrix of $G(s)$.

Proof. We begin by proving necessity. Suppose that $\mathcal{C}$ is consistent, Then, there exists an input-output system Σ of the form (3.59) that implements $\mathcal{C}$. Due to Corollary 3.16, there exist polynomial matrices $T(s)$ and $M(s)$ such that

$$\begin{bmatrix} G(s) & -H(s) \end{bmatrix} = \begin{bmatrix} T(s) & M(s) \end{bmatrix} \begin{bmatrix} P(s) & -Q(s) \\ 0 & -A(s) \end{bmatrix}. \tag{3.114}$$

From the latter we obtain

$$G(s) = T(s)P(s) \quad \text{and} \quad H(s) - M(s)A(s) = T(s)Q(s), \tag{3.115}$$

which implies that

$$G(s)P(s)^{-1}Q(s) = H(s) - M(s)A(s). \tag{3.116}$$

Note that $G(s)$ is row-reduced and $P(s)^{-1}Q(s)$ is proper. Therefore, due to Proposition 3.9, it follows that (3.113) is proper, as desired.

We proceed by proving sufficiency. Suppose that there exists a polynomial matrix $M(s)$ such that (3.113) is proper. As $G(s)$ is row-reduced, we can write

$$G(s) = D(s)G^h + G^l(s), \tag{3.117}$$

where G^h is a real matrix that has full row rank and $G^l(s)$ is a polynomial matrix such that $D(s)^{-1}G^l(s)$ is strictly proper. Since G^h has full row rank, there exists a real matrix $\bar{G}^h$ such that

$$\begin{bmatrix} G^h \\ \bar{G}^h \end{bmatrix} \tag{3.118}$$

is invertible. With this in mind, define

$$P(s) = \begin{bmatrix} D(s) & 0 \\ 0 & I \end{bmatrix} \begin{bmatrix} G^h \\ \bar{G}^h \end{bmatrix} + \begin{bmatrix} G^l(s) \\ 0 \end{bmatrix}. \tag{3.119}$$

and note that $P(s)$ is row-reduced and, thus, invertible. Next, define

$$Q(s) = \begin{bmatrix} H(s) - M(s)A(s) \\ 0 \end{bmatrix}, \tag{3.120}$$

and note that

$$\begin{bmatrix} D(s) & 0 \\ 0 & I \end{bmatrix}^{-1} Q(s) = \begin{bmatrix} D(s)^{-1}\left(H(s) - M(s)A(s)\right) \\ 0 \end{bmatrix} \tag{3.121}$$

is proper. Therefore, due to Corollary 3.10, it follows that $P(s)^{-1}Q(s)$ is proper, hence the system Σ given by (3.59) is in input-output form. Furthermore, we have that (3.115) and, thus, (3.114) hold with

$$T(s) = \begin{bmatrix} I & 0 \end{bmatrix}. \tag{3.122}$$

In view of Corollary 3.16, this shows that Σ implements $\mathcal{C}$, hence $\mathcal{C}$ is consistent. □

Lemma 3.19 translates the problem of verifying the consistency of a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ to the problem of verifying the existence of a polynomial matrix $M(s)$ such that (3.113) is proper. At the same time, the proof of Lemma 3.19 tells us how to construct an implementation from a polynomial matrix $M(s)$ such that (3.113) is proper. Therefore, the natural next step is to find conditions under which such a polynomial matrix $M(s)$ exists and to provide a method for its construction if it exists. To this end, note that (3.113) is proper if and only if i'th row degree of $H(s) + M(s)A(s)$ is less than or equal to the i'th row degree of $G(s)$. Therefore, a good candidate for a polynomial matrix $M(s)$ such that (3.113) is proper is the one that minimizes the row degrees of $H(s) + M(s)A(s)$. The following lemma shows how to find such an $M(s)$ in the special case where $H(s)$ has only one row and $A(s)$ is square, invertible and row-reduced.

Lemma 3.20. *Suppose that $H(s)$ is a polynomial row vector, and the polynomial matrix $A(s)$ is square, invertible and row-reduced. Let $\bar{M}(s)$ be the polynomial part of the rational row vector $H(s)A(s)^{-1}$. Then,*

$$\deg H(s) - \bar{M}(s)A(s) \leq \deg H(s) - M(s)A(s) \tag{3.123}$$

for any polynomial row vector $M(s)$.

Proof. To begin with, we can write

$$H(s)A(s)^{-1} = \bar{M}(s) + \bar{R}(s), \tag{3.124}$$

for some strictly proper rational row vector $\bar{R}(s)$, and, thus,

$$H(s) - \bar{M}(s)A(s) = \bar{R}(s)A(s). \tag{3.125}$$

Let $M(s)$ be a polynomial row vector and note that

$$H(s) - M(s)A(s) = H(s) - \bar{M}(s)A(s) + \bar{M}(s)A(s) - M(s)A(s), \tag{3.126}$$

hence we can write

$$H(s) - M(s)A(s) = T(s)A(s), \tag{3.127}$$

where

$$T(s) = \bar{M}(s) - M(s) + \bar{R}(s). \tag{3.128}$$

We can compare the degrees of $\bar{R}(s)A(s)$ and $T(s)A(s)$ using Proposition 3.11. Since the entries of $\bar{M}(s)$ and $M(s)$ are polynomials, but the entries of $\bar{R}(s)$ are strictly proper rational functions, it follows that $T_i(s) = 0$ if and only if $\bar{M}_i(s) = M_i(s)$ and $\bar{R}_i(s) = 0$, where $T_i(s)$, $\bar{M}_i(s)$, $M_i(s)$ and $\bar{R}_i(s)$ denote the i'th entries of $T(s)$, $\bar{M}(s)$, $M(s)$ and $\bar{R}(s)$, respectively. In particular, $R_i(s) \neq 0$ implies that $T_i(s) \neq 0$, hence

$$\max_{i:\bar{R}_i(s)\neq 0} \deg T_i(s) + d_i \leq \max_{i:T_i(s)\neq 0} \deg T_i(s) + d_i, \tag{3.129}$$

where d_i is the degree of the i'th row of $A(s)$. Furthermore, since adding a polynomial to a strictly proper rational function cannot decrease its degree, it follows that $\deg \bar{R}_i(s) \leq \deg T_i(s)$ and thus

$$\max_{i:\bar{R}_i(s)\neq 0} \deg \bar{R}_i(s) + d_i \leq \max_{i:R_i(s)\neq 0} \deg T_i(s) + d_i. \tag{3.130}$$

Now, (3.129) and (3.130) imply that

$$\max_{i:\bar{R}_i(s)\neq 0} \deg \bar{R}_i(s) + d_i \leq \max_{i:T_i(s)\neq 0} \deg T_i(s) + d_i, \tag{3.131}$$

which, due to Proposition 3.11, implies that

$$\deg R(s)A(s) \leq \deg T(s)A(s) \tag{3.132}$$

and we conclude that (3.123) holds, as desired. □

Remark 3.9. *Lemma 3.20 can be extended to the case where $H(s)$ has multiple rows by noting that the i'th row of $H(s) - M(s)A(s)$ is $H_i(s) - M_i(s)A(s)$, where $H_i(s)$ and $M_i(s)$ indicate the i'th rows of $H(s)$ and $M(s)$, respectively. Then, due to Lemma 3.20, the degree of $H_i(s) - M_i(s)A(s)$ is minimized when $M_i(s)$ is the polynomial part of $H_i(s)A(s)^{-1}$, hence the row degrees of $H(s) - M(s)A(s)$ are minimized when $M(s)$ is the polynomial part of $H(s)A(s)^{-1}$.*

In general, we do not expect $A(s)$ to be square. But, due to Lemma 3.18, we can assume that $A(s)$ is row-reduced. This turns out to be enough, and we obtain the following characterization of contract consistency for row-reduced contracts.

Theorem 3.2. *Suppose that the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ is row-reduced, where* A *and* Γ *are given by* (3.73) *and* (3.75)*, respectively. According to Proposition 3.12, let P be a permutation matrix such that*

$$A(s)P = \begin{bmatrix} A_1(s) & A_2(s) \end{bmatrix}, \tag{3.133}$$

where $A_1(s)$ is square, invertible and row-reduced, and $A_1(s)^{-1}A_2(s)$ is proper. Furthermore, let $D(s)$ be the row-degree matrix of $G(s)$, let $H_1(s)$ and $H_2(s)$ be such that

$$H(s)P = \begin{bmatrix} H_1(s) & H_2(s) \end{bmatrix}, \tag{3.134}$$

and let $\bar{M}(s)$ be the polynomial part of $H_1(s)A_1(s)^{-1}$. Then, the contract $\mathcal{C}$ is consistent if and only if the rational matrix

$$D(s)^{-1} \begin{bmatrix} H_1(s) - \bar{M}(s)A_1(s) & H_1(s)A_1(s)^{-1}A_2(s) - H_2(s) \end{bmatrix} \tag{3.135}$$

is proper.

Proof. From Lemma 3.19, we know that $\mathcal{C}$ is consistent if and only if there exists a polynomial matrix $M(s)$ such that the rational matrix

$$D(s)^{-1}\left(H(s) - M(s)A(s)\right) \tag{3.136}$$

is proper. Note that multiplying the latter with P from the right yields

$$D(s)^{-1}\begin{bmatrix} H_1(s) - M(s)A_1(s) & H_2(s) - M(s)A_2(s)\end{bmatrix}. \tag{3.137}$$

Since $A_1(s)^{-1}A_2(s)$ is proper, we have that

$$T(s) = \begin{bmatrix} I & -A_1(s)^{-1}A_2(s) \\ 0 & I \end{bmatrix} \tag{3.138}$$

is proper. Furthermore, it is easily seen that

$$T(s)^{-1} = \begin{bmatrix} I & A_1(s)^{-1}A_2(s) \\ 0 & I \end{bmatrix} \tag{3.139}$$

is proper as well. This means that (3.137) is proper if and only if multiplying it with $T(s)$ from the right yields a proper rational matrix. In other words, (3.137) and, thus, (3.136) are proper if and only if

$$D(s)^{-1}\begin{bmatrix} H_1(s) - M(s)A_1(s) & H_1(s)A_1(s)^{-1}A_2(s) - H_2(s)\end{bmatrix}. \tag{3.140}$$

is proper. Due to Lemma 3.20 and Remark 3.9, there exists $M(s)$ such that

$$D(s)^{-1}\left(H_1(s) - M(s)A_1(s)\right) \tag{3.141}$$

is proper if and only if

$$D(s)^{-1}\left(H_1(s) - \bar{M}(s)A_1(s)\right) \tag{3.142}$$

is proper, hence $\mathcal{C}$ is consistent if and only if (3.135) is proper. □

Note that each matrix in the statement Theorem 3.2 can be computed, hence we can verify the consistency of a row-reduced contract. Now, consider verifying the consistency of a general contract $\mathcal{C} = (\mathrm{A}, \Gamma)$. In view of Lemma 3.17, we first need to verify that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\Gamma)$. To this end, we can use [63, Theorem 6.2.6] to obtain a polynomial matrix $H_u(s)$ such that

$$\mathfrak{B}_{\mathrm{i}}(\Gamma) = \left\{ u \in \mathscr{C}_m^\infty \;\middle|\; 0 = H_u\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right)u \right\}, \tag{3.143}$$

after which we can use Proposition 3.13 and Proposition 3.14 to verify that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\Gamma)$. If $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \not\subset \mathfrak{B}_{\mathrm{i}}(\Gamma)$, then $\mathcal{C}$ is not consistent. Otherwise, using Lemma 3.18, we can obtain a row-reduced contract $\mathcal{C}'$ that is equivalent to $\mathcal{C}$. As such, $\mathcal{C}'$ is consistent if and only if $\mathcal{C}$ is consistent, hence we can use Theorem 3.2 and $\mathcal{C}'$ to verify the consistency of $\mathcal{C}$.

Remark 3.10. *Theorem 3.2 only tells us how to verify contract consistency but it does not tell us how to construct an implementation for a consistent contract. For that, we can look at the proof of Lemma 3.19. In particular, given a consistent row-reduced contract $\mathcal{C} = (\mathrm{A}, \Gamma)$, where A and Γ are given by* (3.73) *and* (3.75)*, respectively, we can write*

$$G(s) = D(s)G^h + G^l(s), \tag{3.144}$$

where $D(s)$ is the row degree matrix of $G(s)$, the real matrix G^h has full row rank and the polynomial matrix $G^l(s)$ is such that $D(s)^{-1}G^l(s)$ is strictly proper. Then, the system Σ in (3.59) *is in input-output form and implements $\mathcal{C}$ if*

$$P(s) = \begin{bmatrix} D(s) & 0 \\ 0 & I \end{bmatrix} \begin{bmatrix} G^h \\ \bar{G}^h \end{bmatrix} + \begin{bmatrix} G^l(s) \\ 0 \end{bmatrix}, \quad Q(s) = \begin{bmatrix} H(s) - \bar{M}(s)A(s) \\ 0 \end{bmatrix}, \tag{3.145}$$

where $\bar{M}(s)$ is defined as in Theorem 3.2 and $\bar{G}^h \in \mathbb{R}^{(p-g)\times p}$ is such that

$$\begin{bmatrix} G^h \\ \bar{G}^h \end{bmatrix} \tag{3.146}$$

is invertible. In fact, an implementation is also obtained by taking

$$P(s) = \begin{bmatrix} D(s) & 0 \\ 0 & \bar{D}(s) \end{bmatrix} \begin{bmatrix} G^h \\ \bar{G}^h \end{bmatrix} + \begin{bmatrix} G^l(s) \\ \bar{G}^l(s) \end{bmatrix}, \quad Q(s) = \begin{bmatrix} H(s) - \bar{M}(s)A(s) \\ \bar{H}(s) \end{bmatrix} \tag{3.147}$$

for any nonsingular diagonal polynomial matrix $\bar{D}(s)$, and polynomial matrices $\bar{G}^l(s)$ and $\bar{H}(s)$ such that $\bar{D}(s)^{-1}\bar{G}^l(s)$ and $\bar{D}(s)^{-1}\bar{H}(s)$ are proper. Indeed, the latter ensures that the resulting system Σ is in input-output form, while the top block rows of $P(s)$ and $Q(s)$ ensure that Σ implements $\mathcal{C}$.

Remark 3.11. *Given an input-output system Σ that implements a given contract $\mathcal{C}$, we can use the results from [77] to obtain an input-state-output system that implements $\mathcal{C}$. More precisely, we can construct an input-state-output system Σ' such that $\mathfrak{B}(\Sigma') = \mathfrak{B}(\Sigma)$, which would imply that Σ' implements $\mathcal{C}$ because Σ implements $\mathcal{C}$. Although it is possible to construct such a system Σ', the procedure is not trivial.*

Remark 3.12. *On a technical level, the problem of designing an implementation for a given contract closely resembles the problems of control by interconnection [12, 14] and, in particular, (regular) implementability in the behavioural setting [16, 79–81]. To see this, consider a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$. We can view the assumptions A as a plant system, the guarantees Γ as the desired system (or specification), and an implementation Σ as a controller. In this context, designing an implementation can be interpreted as the design of a controller Σ such that the behaviour of the controlled plant $\mathrm{A} \wedge \Sigma$ is a subset of the behaviour of the desired system Γ. The problem of control by interconnection is very similar. The main difference is that the latter requires the behaviour of the controlled plant $\mathrm{A} \wedge \Sigma$ to be exactly equal to the behaviour of the desired system Γ. Furthermore, the system classes to which A, Γ and Σ belong in the literature are different from the ones in this chapter. Nevertheless, some of the results in the literature can be useful in tackling problems related to contract-based design.*

We conclude this section by revisiting Example 3.1 to illustrate how Theorem 3.2 and Remark 3.10 can be used in practice.

Example 3.3. Consider the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ from Example 3.1. Note that $\mathcal{C}$ is already row-reduced. Indeed, we have that

$$A(s) = \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ \tau_s & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & -1 \\ 1 & -1 & -\tau_l \end{bmatrix}, \tag{3.148}$$

which is clearly row-reduced, and $G(s)$ in (3.92) is a nonzero polynomial, which is also clearly row-reduced. Furthermore, the polynomial matrices

$$A_1(s) = \begin{bmatrix} 0 & s \\ \tau_s s + 1 & -1 \end{bmatrix} \quad \text{and} \quad A_2(s) = \begin{bmatrix} -1 \\ -\tau_l \end{bmatrix} \tag{3.149}$$

are such that $A_1(s)$ is square, invertible and row-reduced, $A_1(s)^{-1}A_2(s)$ is proper, and $A(s) = \begin{bmatrix} A_1(s) & A_2(s) \end{bmatrix}$. With this in mind, partition $H(s)$ in (3.92) as $H(s) = \begin{bmatrix} H_1(s) & H_2(s) \end{bmatrix}$ with

$$H_1(s) = \begin{bmatrix} s + k & 0 \end{bmatrix} \quad \text{and} \quad H_2(s) = 0, \tag{3.150}$$

and note that

$$H(s) = \begin{bmatrix} H_1(s) & H_2(s) \end{bmatrix} \tag{3.151}$$

Then, according to Theorem 3.2, $\mathcal{C}$ is consistent if and only if (3.135) holds, where $D(s)$ is the row-degree matrix of $G(s)$ and $\bar{M}(s)$ is the polynomial part of $H_1(s)A_1(s)^{-1}$. Note that $D(s) = s$ and

$$H_1(s)A_1(s)^{-1} = \frac{1}{\tau_s s^2 + s} \begin{bmatrix} s + k & s^2 + ks \end{bmatrix}, \tag{3.152}$$

which implies that

$$\bar{M}(s) = \begin{bmatrix} 0 & \dfrac{1}{\tau_s} \end{bmatrix}. \tag{3.153}$$

Consequently, (3.135) reduces to

$$\frac{1}{s} \begin{bmatrix} k - \dfrac{1}{\tau_s} & \dfrac{1}{\tau_s} & \dfrac{\tau_l s^2 + (1 + \tau_l k)s + k}{\tau_s s^2 + s} \end{bmatrix}, \tag{3.154}$$

which is clearly proper. Finally, in view Remark 3.10, the system Σ given by (3.59), where $P(s) = G(s)$ and $Q(s) = H(s) - \bar{M}(s)A(s)$ implements $\mathcal{C}$. This is the same Σ as in Example 3.1, which was already shown to implement $\mathcal{C}$.

3.5 Refinement

In this section, we will consider the notion of contract refinement. Contract refinement allows one to compare contracts, which has an essential role in enabling the independent design of components within interconnected systems, as explained in Chapter 2. In what follows, we will define contract refinement and will find necessary and sufficient conditions under which a contract refines another contract. These conditions will take the form of a pair of behavioural inclusions, which can be verified algorithmically, thus allowing contract refinement to be verified algorithmically. Then, using our results on contract refinement, we will find necessary and sufficient conditions for contract equivalence.

To begin with, following the meta-theoretic definition outlined in Chapter 2, we define contract refinement as follows.

Definition 3.7. The contract $\mathcal{C}_1$ *refines* the contract $\mathcal{C}_2$ if:

1. all environments compatible with $\mathcal{C}_2$ are compatible with $\mathcal{C}_1$;
2. all implementations of $\mathcal{C}_1$ are implementations of $\mathcal{C}_2$.

Said differently, $\mathcal{C}_1$ refines $\mathcal{C}_2$ if it has a larger class of compatible environments but a smaller class of implementations. Intuitively, this means that $\mathcal{C}_1$ imposes stricter guarantees that have to be satisfied under weaker assumptions, hence $\mathcal{C}_1$ can be seen as expressing a stricter specification than $\mathcal{C}_2$.

Just like implementation, we can characterize refinement based on assumptions and guarantees alone. If $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$, then it is not difficult to see that the first condition in Definition 3.7 holds if and only if $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$. For the second condition, we need to consider two cases depending on whether $\mathcal{C}_1$ is consistent or not. If $\mathcal{C}_1$ is not consistent, then the second condition is vacuously satisfied, hence $\mathcal{C}_1$ refines $\mathcal{C}_2$ if and only if $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$. If $\mathcal{C}_1$ is consistent, then we have the following theorem.

Theorem 3.3. *Consider the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$, where $\mathcal{C}_1$ is consistent. Then, $\mathcal{C}_1$ refines $\mathcal{C}_2$ if and only if*

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \quad \textit{and} \quad \mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_1) \subset \mathfrak{B}(\Gamma_2). \tag{3.155}$$

In this case, $\mathcal{C}_2$ is guaranteed to be consistent.

Proof. We begin by proving sufficiency. Suppose that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ and $\mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_1) \subset \mathfrak{B}(\Gamma_2)$. Clearly, the inclusion $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ implies that every environment compatible with $\mathcal{C}_2$ is also compatible with $\mathcal{C}_1$, such that the first condition in Definition 3.7 holds. To show that the second condition

also holds, let Σ be an implementation of $\mathcal{C}_1$. Since A_2 is compatible with $\mathcal{C}_1$, this implies that $\mathfrak{B}(\mathrm{A}_2 \wedge \Sigma) \subset \mathfrak{B}(\Gamma_1)$. Note that $\mathfrak{B}(\mathrm{A}_2 \wedge \Sigma) \subset \mathfrak{B}(\Gamma_1)$ only if $\mathfrak{B}(\mathrm{A}_2 \wedge \Sigma) \subset \mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_1)$, and $\mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_1) \subset \mathfrak{B}(\Gamma_2)$ by assumption, hence $\mathfrak{B}(\mathrm{A}_2 \wedge \Sigma) \subset \mathfrak{B}(\Gamma_2)$. From Theorem 3.1 it follows that Σ implements $\mathcal{C}_2$, which shows that every implementation of $\mathcal{C}_1$ is also an implementation of $\mathcal{C}_2$, i.e., the second condition in Definition 3.7 holds as well.

We proceed by proving necessity. Suppose that $\mathcal{C}_1$ refines $\mathcal{C}_2$, and let

$$\mathrm{A}_j : 0 = A_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u \quad \text{and} \quad \Gamma_j : G_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y = H_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u, \quad j \in \{1, 2\}. \tag{3.156}$$

Since A_2 is an environment compatible with $\mathcal{C}_2$, it also needs to be compatible with $\mathcal{C}_1$, hence $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$. We will now show that $\mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_1) \subset \mathfrak{B}(\Gamma_2)$. In view of Theorem 3.1 and the assumption that $\mathcal{C}_1$ is consistent, there exists an input-output system Σ such that $\mathfrak{B}(\mathrm{A}_1 \wedge \Sigma) \subset \mathfrak{B}(\Gamma_1)$, which holds if and only if $\mathfrak{B}(\mathrm{A}_1 \wedge \Sigma) \subset \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1)$. Let Σ be given by (3.59). From the proof of Lemma 3.18, we know that there exist guarantees

$$\Gamma_1 : G_1'\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y = H_1'\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u \tag{3.157}$$

where $G_1'(s)$ is row-reduced and $\mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1) = \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1')$, thus, also,

$$\mathfrak{B}(\mathrm{A}_1 \wedge \Sigma) \subset \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1') \subset \mathfrak{B}(\Gamma_1').$$

Now, due to Proposition 3.13, $\mathfrak{B}(\mathrm{A}_1 \wedge \Sigma) \subset \mathfrak{B}(\Gamma_1')$ if and only if there exist polynomial matrices $T(s)$ and $M(s)$ satisfying

$$\begin{bmatrix} G_1'(s) & -H_1'(s) \end{bmatrix} = \begin{bmatrix} T(s) & M(s) \end{bmatrix} \begin{bmatrix} P(s) & -Q(s) \\ 0 & -A_1(s) \end{bmatrix}.$$

Note that $T(s)$ has full row rank because $G_1'(s)$ has full row rank and $P(s)$ is invertible. This implies that there exists a polynomial matrix $T'(s)$ such that

$$\begin{bmatrix} T(s) \\ T'(s) \end{bmatrix} \tag{3.158}$$

is square and invertible. Let k be a positive integer and define

$$P_k(s) = \begin{bmatrix} T(s) \\ s^k T'(s) \end{bmatrix} P(s), \quad Q_k(s) = \begin{bmatrix} T(s) \\ s^k T'(s) \end{bmatrix} Q(s).$$

We will show that the system

$$\Sigma_k : P_k\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y = Q_k\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u$$

implements $\mathcal{C}_1$ for any positive integer k. To this end, note that $P_k(s)$ is invertible and $P_k(s)^{-1}Q_k(s) = P(s)^{-1}Q(s)$ is proper, hence Σ_k is in input-output form. Furthermore, we have that

$$\begin{bmatrix} G_1'(s) & -H_1'(s) \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} I & 0 \end{bmatrix} & M(s) \end{bmatrix} \begin{bmatrix} P_k(s) & -Q_k(s) \\ 0 & -A_1(s) \end{bmatrix},$$

hence $\mathfrak{B}(\mathrm{A}_1 \wedge \Sigma_k) \subset \mathfrak{B}(\Gamma_1')$, which holds only if $\mathfrak{B}(\mathrm{A}_1 \wedge \Sigma_k) \subset \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1')$. Since $\mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1') = \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1)$, it follows that

$$\mathfrak{B}(\mathrm{A}_1 \wedge \Sigma_k) \subset \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1) \subset \mathfrak{B}(\Gamma_1),$$

hence Σ_k implements $\mathcal{C}_1$ due to Theorem 3.1. But then Σ_k must also implement $\mathcal{C}_2$, which is the case if and only if $\mathfrak{B}(\mathrm{A}_2 \wedge \Sigma_k) \subset \mathfrak{B}(\Gamma_2)$. The latter holds if and only if there exist polynomial matrices $T_k(s)$ and $M_k(s)$ such that

$$\begin{bmatrix} G_2(s) & -H_2(s) \end{bmatrix} = \begin{bmatrix} T_k(s) & M_k(s) \end{bmatrix} \begin{bmatrix} P_k(s) & -Q_k(s) \\ 0 & -A_2(s) \end{bmatrix}.$$

In particular, we have that

$$G_2(s) = T_k(s)P_k(s) = T_k(s) \begin{bmatrix} T(s) \\ s^k T'(s) \end{bmatrix} P(s).$$

which implies that

$$G_2(s)P(s)^{-1} \begin{bmatrix} T(s) \\ T'(s) \end{bmatrix}^{-1} = T_k(s) \begin{bmatrix} I & 0 \\ 0 & s^k I \end{bmatrix}, \tag{3.159}$$

As the left-hand side of (3.159) is independent of k, we must have that the right-hand side is also independent of k. This is possible only if

$$T_k(s) = \begin{bmatrix} T_1(s) & 0 \end{bmatrix} \tag{3.160}$$

for some polynomial matrix $T_1(s)$. Consequently, we have that

$$G_2(s) = T_k(s)P_k(s) = T_1(s)T(s)P(s) = T_1(s)G_1'(s),$$

and, similarly, that

$$\begin{aligned} H_2(s) &= T_1(s)T(s)Q(s) + M_k(s)A_2(s) \\ &= T_1(s)(H_1'(s) - M(s)A_1(s)) + M_k(s)A_2(s). \end{aligned}$$

Since $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$, we have that $A_1(s) = R(s)A_2(s)$ for some polynomial matrix $R(s)$, and, thus,

$$\begin{bmatrix} G_2(s) & -H_2(s) \end{bmatrix} = \begin{bmatrix} T_1(s) & T_1(s)M(s)R(s) - M_k(s) \end{bmatrix} \begin{bmatrix} G_1'(s) & -H_1'(s) \\ 0 & -A_2(s) \end{bmatrix},$$

which implies that $\mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_1') \subset \mathfrak{B}(\Gamma_2)$. On the other hand, $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ and $\mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1') = \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1)$ imply that $\mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_1') = \mathfrak{B}(\mathrm{A}_2 \wedge \Gamma)$, hence we conclude that $\mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_1) \subset \mathfrak{B}(\Gamma_2)$, as desired. □

Theorem 3.3 tells us that refinement can be verified by verifying that a pair of behavioural inclusions hold. We can do the latter by using Proposition 3.13 and Proposition 3.14. In particular, if

$$\mathrm{A}_j : 0 = A_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u \quad \text{and} \quad \Gamma_j : G_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y = H_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u, \quad j \in \{1,2\}, \tag{3.161}$$

then, due to Proposition 3.13, (3.155) holds if and only if there exist polynomial matrices $R(s)$, $T(s)$ and $M(s)$ such that $A_1(s) = R(s)A_2(s)$ and

$$\begin{bmatrix} G_2(s) & -H_2(s) \end{bmatrix} = \begin{bmatrix} T(s) & M(s) \end{bmatrix} \begin{bmatrix} G_1(s) & -H_1(s) \\ 0 & -A_2(s) \end{bmatrix}. \tag{3.162}$$

Proposition 3.14 can be used to verify the existence of these polynomial matrices, but only if $A_2(s)$ and $G_1(s)$ have full row rank. Because of Remark 3.4, we can assume that $A_2(s)$ has full row rank without loss of generality. On the other hand, since $\mathcal{C}_1$ is consistent, Lemma 3.18 tells us that $\mathcal{C}_1$ is equivalent to a row-reduced contract, which can be computed explicitly. Therefore, we can also assume that $G_1(s)$ is row-reduced and, thus, that it has full row rank.

We conclude this section with a brief discussion of the notion of contract equivalence. Recall from Definition 3.4 that two contracts $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent if they define the same classes of compatible environments and implementations. It is easily seen that this is the case if and only if $\mathcal{C}_1$ refines $\mathcal{C}_2$ and $\mathcal{C}_2$ refines $\mathcal{C}_1$. Therefore, as an immediate corollary of Theorem 3.3, we obtain the following necessary and sufficient conditions for contract equivalence of consistent contracts.

Corollary 3.21. *Consider the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$, where at least one is consistent. Then, $\mathcal{C}_1$ is equivalent to $\mathcal{C}_2$ if and only if*

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \quad \textit{and} \quad \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1) = \mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_2). \tag{3.163}$$

In this case, the other contract is guaranteed to be consistent.

Remark 3.13. *If Γ_1 and Γ_2 are output guarantees, as in Remark 3.7, then the contract $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ refines $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ if and only if*

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \quad \textit{and} \quad \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma_2). \tag{3.164}$$

To see this, note that, since Γ_2 are output guarantees, $\mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_1) \subset \mathfrak{B}(\Gamma_2)$ if and only if $\mathfrak{B}_{\mathrm{o}}(\mathrm{A}_2 \wedge \Gamma_1) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma_2)$. Furthermore, since Γ_1 are output guarantees, we have that $\mathfrak{B}_{\mathrm{o}}(\mathrm{A}_2 \wedge \Gamma_1) = \mathfrak{B}_{\mathrm{o}}(\Gamma_1)$, and, due to Remark 3.8, that $\mathcal{C}_1$ is consistent. Therefore, due to Theorem 3.3, $\mathcal{C}_1$ refines $\mathcal{C}_2$ if and only if (3.164) *holds. Similarly, we also have that $\mathcal{C}_1$ is equivalent to $\mathcal{C}_2$ if and only if*

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \quad \textit{and} \quad \mathfrak{B}_{\mathrm{o}}(\Gamma_1) = \mathfrak{B}_{\mathrm{o}}(\Gamma_2). \tag{3.165}$$

Remark 3.14. *As already explained in Chapter 2, refinement defines a preorder. Indeed, it is easily seen that $\mathcal{C}$ refines $\mathcal{C}$ for any contract $\mathcal{C}$. On the other hand, if $\mathcal{C}_1$ refines $\mathcal{C}_2$, and $\mathcal{C}_2$ refines $\mathcal{C}_3$, then $\mathcal{C}_1$ refines $\mathcal{C}_3$. With this in mind, given a set of contracts $\mathfrak{C}$, a* smallest *contract in $\mathfrak{C}$ is a contract $\mathcal{C}_s \in \mathfrak{C}$ such that $\mathcal{C}_s$ is refined by $\mathcal{C}$ for all $\mathcal{C} \in \mathfrak{C}$. Similarly, a* largest *contract in $\mathfrak{C}$ is a contract $\mathcal{C}_l \in \mathfrak{C}$ such that $\mathcal{C}_l$ refines $\mathcal{C}$ for all $\mathcal{C} \in \mathfrak{C}$. Such a contract does not necessarily exist and is not necessarily unique if it does exist. Nevertheless, since all such contracts are equivalent by definition, we will refer to* the *smallest and* the *largest contract in a given set $\mathfrak{C}$ and will use a convenient representative of the sets of smallest and largest contracts in $\mathfrak{C}$, respectively.*

3.6 Conjunction

In this section, we will discuss the notion of contract conjunction, which allows us to combine the specifications that two contracts express. We will define contract conjunction as in Chapter 2, and we will show that the conjunction of two arbitrary contracts does not necessarily exist. Nevertheless, we will present two special cases where the conjunction does exist, and we will provide an explicit expression for it in these cases.

To begin with, if a contract $\mathcal{C}_1$ refines another contract $\mathcal{C}_2$, then $\mathcal{C}_1$ can be interpreted as enforcing the specification expressed by $\mathcal{C}_2$, and potentially more. Consequently, if a contract $\mathcal{C}$ refines another two contracts $\mathcal{C}_1$ and $\mathcal{C}_2$, then $\mathcal{C}$ can be interpreted as enforcing both the specification expressed by $\mathcal{C}_1$ and the specification expressed by $\mathcal{C}_2$. This motivates the following definition.

Definition 3.8. The *conjunction* of contracts $\mathcal{C}_1$ and $\mathcal{C}_2$, denoted by $\mathcal{C}_1 \wedge \mathcal{C}_2$, is the largest contract that refines both $\mathcal{C}_1$ and $\mathcal{C}_2$.

The definition of the conjunction $\mathcal{C}_1 \wedge \mathcal{C}_2$ has two aspects. On the one hand, $\mathcal{C}_1 \wedge \mathcal{C}_2$ is a contract that refines both $\mathcal{C}_1$ and $\mathcal{C}_2$, hence it expresses a fusion of the specifications that $\mathcal{C}_1$ and $\mathcal{C}_2$ express. On the other hand, $\mathcal{C}_1 \wedge \mathcal{C}_2$ is the *largest* such contract, that is, it is refined by any contract that refines both $\mathcal{C}_1$ and $\mathcal{C}_2$. This means that $\mathcal{C}_1 \wedge \mathcal{C}_2$ expresses the least restrictive fusion of the specifications that $\mathcal{C}_1$ and $\mathcal{C}_2$ express. Considering the first aspect, we can always find a contract that refines both $\mathcal{C}_1$ and $\mathcal{C}_2$.

Lemma 3.22. *If $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$, then*

$$\mathcal{C} = (\mathrm{A}_1 \vee \mathrm{A}_2, \Gamma_1 \wedge \Gamma_2) \tag{3.166}$$

refines both $\mathcal{C}_1$ and $\mathcal{C}_2$, where

$$\mathrm{A}_1 \vee \mathrm{A}_2 : \begin{bmatrix} I & I \\ A_1\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) & 0 \\ 0 & A_2\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \end{bmatrix} \begin{bmatrix} l_1 \\ l_2 \end{bmatrix} = \begin{bmatrix} I \\ 0 \\ 0 \end{bmatrix} u, \tag{3.167}$$

is the join *of* A_1 *and* A_2*, and*

$$\Gamma_1 \wedge \Gamma_2 : \begin{bmatrix} G_1\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) \\ G_2\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) \end{bmatrix} y = \begin{bmatrix} H_1\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) \\ H_2\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) \end{bmatrix} u \tag{3.168}$$

is the meet *of* Γ_1 *and* Γ_2*.*

Proof. The join $\mathrm{A}_1 \vee \mathrm{A}_2$ is such that $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \vee \mathrm{A}_2)$ if and only if $u = l_1 + l_2$ for some $l_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ and $l_2 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$, while the meet $\Gamma_1 \wedge \Gamma_2$ is such that $(u, y) \in \mathfrak{B}(\Gamma_1 \wedge \Gamma_2)$ if and only if $(u, y) \in \mathfrak{B}(\Gamma_1)$ and $(u, y) \in \mathfrak{B}(\Gamma_2)$. Therefore, we have that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \vee \mathrm{A}_2) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) + \mathfrak{B}(\mathrm{A}_2)$ and $\mathfrak{B}(\Gamma_1 \wedge \Gamma_2) = \mathfrak{B}(\Gamma_1) \cap \mathfrak{B}(\Gamma_2)$. The former immediately implies that every environment compatible with $\mathcal{C}_1$ or $\mathcal{C}_2$ is also compatible with $\mathcal{C}$, hence the first condition for refinement is satisfied. If $\mathcal{C}$ is not consistent, then the second condition for refinement is vacuously satisfied and, thus, $\mathcal{C}$ refines both $\mathcal{C}_1$ and $\mathcal{C}_2$. With this in mind, suppose that $\mathcal{C}$ is consistent. Let Σ be an implementation of $\mathcal{C}$ and note that

$$\mathfrak{B}((\mathrm{A}_1 \vee \mathrm{A}_2) \wedge \Sigma) \subset \mathfrak{B}(\Gamma_1 \wedge \Gamma_2) \tag{3.169}$$

due to Theorem 3.1. Moreover, for each $i \in \{1, 2\}$, we have that

$$\mathfrak{B}(\mathrm{A}_i \wedge \Sigma) \subset \mathfrak{B}((\mathrm{A}_1 \vee \mathrm{A}_2) \wedge \Sigma) \tag{3.170}$$

and $\mathfrak{B}(\Gamma_1 \wedge \Gamma_2) \subset \mathfrak{B}(\Gamma_i)$, hence $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_i \wedge \Sigma) \subset \mathfrak{B}_{\mathrm{i}}(\Gamma_i)$ and, thus, Σ implements $\mathcal{C}_i$ due to Theorem 3.1. This shows that the second condition for refinement is also satisfied and we conclude that $\mathcal{C}$ refines both $\mathcal{C}_1$ and $\mathcal{C}_2$. □

Remark 3.15. *Even though we have defined* $\mathrm{A}_1 \vee \mathrm{A}_2$ *with the help of the* latent variables l_1 *and* l_2*, due to [63, Theorem 6.2.6], we can eliminate these to represent* $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \vee \mathrm{A}_2)$ *by a system of the form* (3.73)*, like any other assumptions.*

Although we can always find a contract that refines two given contracts $\mathcal{C}_1$ and $\mathcal{C}_2$, we cannot necessarily find the largest such contract. To show this, we will first show that, if it exists, the conjunction $\mathcal{C}_1 \wedge \mathcal{C}_2$ must be of the form in Lemma 3.22, but possibly obtained from equivalent contracts $\mathcal{C}_1'$ and $\mathcal{C}_2'$.

Lemma 3.23. *Consider the contracts* $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ *and* $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$*, where*

$$\mathrm{A}_j : 0 = A_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u \quad \textit{and} \quad \Gamma_j : G_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y = H_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u, \quad j \in \{1, 2\}. \tag{3.171}$$

If $\mathcal{C}_1 \wedge \mathcal{C}_2$ *exists, then it must be of the form*

$$\mathcal{C}_1 \wedge \mathcal{C}_2 = (\mathrm{A}_1 \vee \mathrm{A}_2, \Gamma_1' \wedge \Gamma_2'), \tag{3.172}$$

where

$$\Gamma_j' : G_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y = \big(H_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) - M_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)A_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)\big)\, u, \quad j \in \{1, 2\}. \tag{3.173}$$

for some polynomial matrices $M_1(s)$ *and* $M_2(s)$*.*

Proof. To begin with, for each $j \in \{1, 2\}$ and any polynomial matrix $M_j(s)$, we have that $\mathfrak{B}(\mathrm{A}_j \wedge \Gamma'_j) = \mathfrak{B}(\mathrm{A}_j \wedge \Gamma_j)$, hence, due to Remark 3.5, $\mathcal{C}'_j = (\mathrm{A}_j, \Gamma'_j)$ is equivalent to $\mathcal{C}_j$. In view of Lemma 3.22, this means that $\mathcal{C}' = (\mathrm{A}_1 \vee \mathrm{A}_2, \Gamma'_1 \wedge \Gamma'_2)$ refines both $\mathcal{C}'_1$ and $\mathcal{C}'_2$, hence it also refines both $\mathcal{C}_1$ and $\mathcal{C}_2$.

With this in mind, suppose that $\mathcal{C}_1 \wedge \mathcal{C}_2$ exists, and let $\mathcal{C}_1 \wedge \mathcal{C}_2 = (\mathrm{A}, \Gamma)$, where A and Γ be given by (3.73) and (3.75). Since $\mathcal{C}_1 \wedge \mathcal{C}_2$ refines both $\mathcal{C}_1$ and $\mathcal{C}_2$, it follows that

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \quad \text{and} \quad \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}). \tag{3.174}$$

Due to linearity, this implies that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) + \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$, hence

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \vee \mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \tag{3.175}$$

by definition of the join $\mathrm{A}_1 \vee \mathrm{A}_2$. On the other hand, it also follows that

$$\mathfrak{B}(\mathrm{A}_1 \wedge \Gamma) \subset \mathfrak{B}(\Gamma_1) \quad \text{and} \quad \mathfrak{B}(\mathrm{A}_2 \wedge \Gamma) \subset \mathfrak{B}(\Gamma_2), \tag{3.176}$$

which is the case if and only if, for each $j \in \{1, 2\}$, there exist polynomial matrices $T_j(s)$ and $M_j(s)$ such that

$$\begin{bmatrix} G_j(s) & -H_j(s) \end{bmatrix} = \begin{bmatrix} T_j(s) & M_j(s) \end{bmatrix} \begin{bmatrix} G(s) & -H(s) \\ 0 & -A_j(s) \end{bmatrix}. \tag{3.177}$$

In particular, this implies that

$$\begin{bmatrix} G_j(s) & -H_j(s) + M_j(s)A_j(s) \end{bmatrix} = T_j(s) \begin{bmatrix} G(s) & -H(s) \end{bmatrix}, \tag{3.178}$$

hence $\mathfrak{B}(\Gamma) \subset \mathfrak{B}(\Gamma'_j)$, where Γ'_j is given by (3.173). Consequently, we must have that $\mathfrak{B}(\Gamma) \subset \mathfrak{B}(\Gamma'_1) \cap \mathfrak{B}(\Gamma'_2)$, hence

$$\mathfrak{B}(\Gamma) \subset \mathfrak{B}(\Gamma'_1 \wedge \Gamma'_2) \tag{3.179}$$

by definition of the meet $\Gamma'_1 \wedge \Gamma'_2$. In view of Theorem 3.3, (3.175) and (3.179) imply that $\mathcal{C}_1 \wedge \mathcal{C}_2$ refines the contract

$$\mathcal{C}' = (\mathrm{A}_1 \vee \mathrm{A}_2, \Gamma'_1 \wedge \Gamma'_2). \tag{3.180}$$

Now, due to Lemma 3.22, we know that $\mathcal{C}'$ refines both $\mathcal{C}'_1 = (\mathrm{A}_1, \Gamma'_1)$ and $\mathcal{C}'_2 = (\mathrm{A}_2, \Gamma'_2)$. Furthermore, it is easily seen that $\mathfrak{B}(\mathrm{A}_1 \wedge \Gamma'_1) = \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1)$ and $\mathfrak{B}(\mathrm{A}_2 \wedge \Gamma'_2) = \mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_2)$, hence, due to Remark 3.5, $\mathcal{C}'_1$ is equivalent to $\mathcal{C}_1$ and $\mathcal{C}'_2$ is equivalent to $\mathcal{C}_2$. This implies that $\mathcal{C}'$ refines both $\mathcal{C}_1$ and $\mathcal{C}_2$, hence it must also refine their conjunction $\mathcal{C}_1 \wedge \mathcal{C}_2$. As we also have that $\mathcal{C}_1 \wedge \mathcal{C}_2$ refines $\mathcal{C}'$, it follows that $\mathcal{C}_1 \wedge \mathcal{C}_2$ and $\mathcal{C}'$ are equivalent. □

In the following example, we use the result of Lemma 3.23 to show that the conjunction $\mathcal{C}_1 \wedge \mathcal{C}_2$ does not necessarily exist for arbitrary contracts $\mathcal{C}_1$ and $\mathcal{C}_2$.

Example 3.4. Consider the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$, where

$$\mathrm{A}_j : 0 = A_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u \quad \text{and} \quad \Gamma_j : G_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y = H_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u, \quad j \in \{1, 2\}. \tag{3.181}$$

Due to Lemma 3.23, if it exists, the conjunction $\mathcal{C}_1 \wedge \mathcal{C}_2$ is given by

$$\mathcal{C}_1 \wedge \mathcal{C}_2 = (\mathrm{A}_1 \vee \mathrm{A}_2, \Gamma), \tag{3.182}$$

where Γ is given by (3.75) with

$$G(s) = \begin{bmatrix} G_1(s) \\ G_2(s) \end{bmatrix} \quad \text{and} \quad H(s) = \begin{bmatrix} H_1(s) - \bar{M}_1(s)A_1(s) \\ H_2(s) - \bar{M}_2(s)A_2(s) \end{bmatrix} \tag{3.183}$$

for some polynomial matrices $\bar{M}_1(s)$ and $\bar{M}_2(s)$. At the same time, for any polynomial matrices $M_1(s)$ and $M_2(s)$, the guarantees Γ_1' and Γ_2' given by (3.173) are such that $\mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1') = \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1)$ and $\mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_2') = \mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_2)$, hence $\mathcal{C}_1' = (\mathrm{A}_1, \Gamma_1')$ and $\mathcal{C}_2' = (\mathrm{A}_2, \Gamma_2')$ are equivalent to $\mathcal{C}_1$ and $\mathcal{C}_2$. This implies that $\mathcal{C}_1 \wedge \mathcal{C}_2$ is also the conjunction of $\mathcal{C}_1'$ and $\mathcal{C}_2'$. Then, due to Lemma 3.22, the contract

$$\mathcal{C}' = (\mathrm{A}_1 \vee \mathrm{A}_2, \Gamma_1' \wedge \Gamma_2') \tag{3.184}$$

refines both $\mathcal{C}_1'$ and $\mathcal{C}_2'$, hence it must also refine their conjunction $\mathcal{C}_1 \wedge \mathcal{C}_2$. If $\mathcal{C}'$ is consistent, then, due to Theorem 3.3, we must have that

$$\mathfrak{B}((\mathrm{A}_1 \vee \mathrm{A}_2) \wedge (\Gamma_1' \wedge \Gamma_2')) \subset \mathfrak{B}(\Gamma). \tag{3.185}$$

With this in mind, let

$$A_1(s) = \begin{bmatrix} I & 0 \end{bmatrix} \quad \text{and} \quad A_2(s) = \begin{bmatrix} 0 & I \end{bmatrix}, \tag{3.186}$$

and note that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \vee \mathrm{A}_2) = \mathscr{C}_m^\infty$, hence (3.185) holds if and only if

$$\mathfrak{B}(\Gamma_1' \wedge \Gamma_2') \subset \mathfrak{B}(\Gamma). \tag{3.187}$$

Now, let

$$G_1(s) = \begin{bmatrix} sI & 0 \end{bmatrix} \quad \text{and} \quad H_1(s) = \begin{bmatrix} H_{11} & H_{12} \end{bmatrix}, \tag{3.188}$$

$$G_2(s) = \begin{bmatrix} 0 & sI \end{bmatrix} \quad \text{and} \quad H_2(s) = \begin{bmatrix} H_{21} & H_{22} \end{bmatrix}, \tag{3.189}$$

for some real matrices H_{11}, H_{12}, H_{21} and H_{22}. Then, we have that

$$\Gamma_1' \wedge \Gamma_2' : \begin{bmatrix} I\frac{\mathrm{d}}{\mathrm{d}t} & 0 \\ 0 & I\frac{\mathrm{d}}{\mathrm{d}t} \end{bmatrix} y = \begin{bmatrix} H_{11} + M_1\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) & H_{12} \\ H_{21} & H_{21} + M_2\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) \end{bmatrix} u, \tag{3.190}$$

which is clearly in input-output form if $M_1(s)$ and $M_2(s)$ are constant. Consequently, if $M_1(s)$ and $M_2(s)$ are constant, then $\mathcal{C}'$ is consistent and, thus,

(3.187) must hold. In view of Proposition 3.13, (3.187) holds if and only if there exists a polynomial matrix $R(s)$ such that

$$\begin{bmatrix} sI & 0 & -H_{11} - \bar{M}_1(s) & -H_{12} \\ 0 & sI & -H_{21} & -H_{21} - \bar{M}_2(s) \end{bmatrix} = R(s) \begin{bmatrix} sI & 0 & -H_{11} - M_1(s) & -H_{12} \\ 0 & sI & -H_{21} & -H_{21} - M_2\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) \end{bmatrix}. \quad (3.191)$$

The latter implies that

$$sI = R(s)sI \quad (3.192)$$

hence $R(s) = I$ and, thus,

$$\begin{bmatrix} H_{11} + \bar{M}_1(s) & H_{12} \\ H_{21} & H_{21} + \bar{M}_2(s) \end{bmatrix} = \begin{bmatrix} H_{11} + M_1(s) & H_{12} \\ H_{21} & H_{21} + M_2(s) \end{bmatrix}. \quad (3.193)$$

In other words, the latter must hold for all constant matrices $M_1(s)$ and $M_2(s)$, which is obviously impossible. This shows that multiple contracts refine both $\mathcal{C}_1$ and $\mathcal{C}_2$ but do not refine their conjunction $\mathcal{C}_1 \wedge \mathcal{C}_2$, which is a contradiction. Therefore, the conjunction $\mathcal{C}_1 \wedge \mathcal{C}_2$ does not exist in this case.

We conclude this section by showing that, even though the conjunction does not exist in general, there are two special cases where it does. In these cases, the conjunction is given by the contract in Lemma 3.22.

Theorem 3.4. *The conjunction $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ is given by*

$$\mathcal{C}_1 \wedge \mathcal{C}_2 = (\mathrm{A}_1 \vee \mathrm{A}_2, \Gamma_1 \wedge \Gamma_2) \quad (3.194)$$

if at least one of the following conditions holds:

1. $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$*;*
2. $\mathfrak{B}((\mathrm{A}_1 \vee \mathrm{A}_2) \wedge \Gamma_1) = \mathfrak{B}((\mathrm{A}_1 \vee \mathrm{A}_2) \wedge \Gamma_2)$.

Proof. Due to Lemma 3.22, we already know that the proposed contract $\mathcal{C}_1 \wedge \mathcal{C}_2$ refines both $\mathcal{C}_1$ and $\mathcal{C}_2$. Therefore, we only need to show that $\mathcal{C}_1 \wedge \mathcal{C}_2$ is the largest such contract. To this end, let $\mathcal{C} = (\mathrm{A}, \Gamma)$ be a contract that refines both $\mathcal{C}_1$ and $\mathcal{C}_2$. Then, every environment compatible with $\mathcal{C}_1$ or $\mathcal{C}_2$ must also be compatible with $\mathcal{C}$. This is the case if and only if $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$ and $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$, hence $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) + \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$ due to linearity, and, thus, $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \vee \mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$ by definition of the join $\mathrm{A}_1 \vee \mathrm{A}_2$. Therefore, every environment compatible with $\mathcal{C}_1 \wedge \mathcal{C}_2$ is also compatible with $\mathcal{C}$.

Next, we will show that every implementation of $\mathcal{C}$ is also an implementation of $\mathcal{C}_1 \wedge \mathcal{C}_2$. This is vacuously true when $\mathcal{C}$ is not consistent. Now, suppose

that $\mathcal{C}$ is consistent. Since $\mathcal{C}$ refines both $\mathcal{C}_1$ and $\mathcal{C}_2$, from Theorem 3.3 it follows that

$$\mathfrak{B}(\mathrm{A}_1 \wedge \Gamma) \subset \mathfrak{B}(\Gamma_1) \quad \text{and} \quad \mathfrak{B}(\mathrm{A}_2 \wedge \Gamma) \subset \mathfrak{B}(\Gamma_2). \tag{3.195}$$

Furthermore, since $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \vee \mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$, the same theorem tells us that $\mathcal{C}$ refines $\mathcal{C}_1 \wedge \mathcal{C}_2$ if and only if

$$\mathfrak{B}((\mathrm{A}_1 \vee \mathrm{A}_2) \wedge \Gamma) \subset \mathfrak{B}(\Gamma_1 \wedge \Gamma_2). \tag{3.196}$$

With this in mind, we will show that (3.196) holds in the following two cases:

1. Suppose that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$. Then

   $$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \vee \mathrm{A}_2) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2), \tag{3.197}$$

   from which it follows that

   $$\mathfrak{B}(\mathrm{A}_1 \wedge \Gamma) = \mathfrak{B}(\mathrm{A}_2 \wedge \Gamma) = \mathfrak{B}((\mathrm{A}_1 \vee \mathrm{A}_2) \wedge \Gamma),$$

   and thus (3.195) implies (3.196).

2. Suppose that

   $$\mathfrak{B}((\mathrm{A}_1 \vee \mathrm{A}_2) \wedge \Gamma_1) = \mathfrak{B}((\mathrm{A}_1 \vee \mathrm{A}_2) \wedge \Gamma_2). \tag{3.198}$$

   Let $i \in \{1, 2\}$ and note that (3.195) holds only if

   $$\mathfrak{B}(\mathrm{A}_i \wedge \Gamma) \subset \mathfrak{B}(\mathrm{A}_i \wedge \Gamma_i). \tag{3.199}$$

   Since $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_i) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \vee \mathrm{A}_2)$, (3.199) yields

   $$\mathfrak{B}(\mathrm{A}_i \wedge \Gamma) \subset \mathfrak{B}((\mathrm{A}_1 \vee \mathrm{A}_2) \wedge \Gamma_i). \tag{3.200}$$

   Furthermore, from (3.198) it follows that

   $$\mathfrak{B}((\mathrm{A}_1 \vee \mathrm{A}_2) \wedge \Gamma_i) \subset \mathfrak{B}(\Gamma_1 \wedge \Gamma_2), \tag{3.201}$$

   which, together with (3.200), implies that

   $$\mathfrak{B}(\mathrm{A}_i \wedge \Gamma) \subset \mathfrak{B}(\Gamma_1 \wedge \Gamma_2) \tag{3.202}$$

   But $\mathfrak{B}(\Gamma_1 \wedge \Gamma_2)$ is a linear space, hence

   $$\mathfrak{B}(\mathrm{A}_1 \wedge \Gamma) + \mathfrak{B}(\mathrm{A}_2 \wedge \Gamma) \subset \mathfrak{B}(\Gamma_1 \wedge \Gamma_2). \tag{3.203}$$

   Now, note that (3.196) would follow from (3.203) if

   $$\mathfrak{B}((\mathrm{A}_1 \vee \mathrm{A}_2) \wedge \Gamma) \subset \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma) + \mathfrak{B}(\mathrm{A}_2 \wedge \Gamma). \tag{3.204}$$

To show that (3.204) holds, let $(u, y) \in \mathfrak{B}((\mathrm{A}_1 \vee \mathrm{A}_2) \wedge \Gamma)$. It follows that $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \vee \mathrm{A}_2)$ and $(u, y) \in \mathfrak{B}(\Gamma)$, which implies that $u = u_1 + u_2$, where $u_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ and $u_2 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$. Since $\mathcal{C}$ is consistent, we must have that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\Gamma)$. Therefore, for all $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$, there exists y such that $(u, y) \in \mathfrak{B}_{\mathrm{i}}(\Gamma)$. Given that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$, this means that there exist y_1 such that $(u_1, y_1) \in \mathfrak{B}(\Gamma)$. Since $\mathfrak{B}(\Gamma)$ is a linear space and $(u, y) \in \mathfrak{B}(\Gamma)$, we get $(u_2, y - y_2) \in \mathfrak{B}(\Gamma)$. But then $(u_1, y_1) \in \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma)$ and $(u_2, y - y_1) \in \mathfrak{B}(\mathrm{A}_2 \wedge \Gamma)$, hence $(u, y) \in \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma) + \mathfrak{B}(\mathrm{A}_2 \wedge \Gamma)$, which shows that (3.204) holds, as desired.

In both cases, we have seen that (3.196) holds, hence $\mathcal{C}$ refines $\mathcal{C}_1 \wedge \mathcal{C}_2$. Since this is the case for any $\mathcal{C}$ that refines both $\mathcal{C}_1$ and $\mathcal{C}_2$, we conclude that the contract $\mathcal{C}_1 \wedge \mathcal{C}_2$ given in (3.166) is indeed the largest contract that refines both $\mathcal{C}_1$ and $\mathcal{C}_2$. □

Remark 3.16. *If we restrict the class of contracts to ones with output guarantees, then the conjunction of two contracts always exists. In particular, if Γ_1 and Γ_2 are output guarantees, then $\Gamma_1 \wedge \Gamma_2$ are also output guarantees, and the contract $\mathcal{C}_1 \wedge \mathcal{C}_2$ defined in Theorem 3.4 is the largest contract with output guarantees that refines $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$. To show this, suppose that there is another contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ with output guarantees Γ that refines both $\mathcal{C}_1$ and $\mathcal{C}_2$. In view of Remark 3.13, this is the case if and only if*

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_j) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \quad \textit{and} \quad \mathfrak{B}_{\mathrm{o}}(\Gamma) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma_j), \quad j \in \{1, 2\}, \tag{3.205}$$

which is equivalent to

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \vee \mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \quad \textit{and} \quad \mathfrak{B}_{\mathrm{o}}(\Gamma) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma_1 \wedge \Gamma_2). \tag{3.206}$$

This implies that $\mathcal{C}$ refines $\mathcal{C}_1 \wedge \mathcal{C}_2$.

Note that the first condition in Theorem 3.4 states that $\mathcal{C}_1$ and $\mathcal{C}_2$ have the same assumptions, which implies that

$$\mathcal{C}_1 \wedge \mathcal{C}_2 = (\mathrm{A}_1, \Gamma_1 \wedge \Gamma_2) = (\mathrm{A}_2, \Gamma_1 \wedge \Gamma_2).$$

On the other hand, the second condition states that $\mathcal{C}_1$ and $\mathcal{C}_2$ have the same guarantees when restricted to the assumptions of $\mathcal{C}_1 \wedge \mathcal{C}_2$, hence

$$\mathcal{C}_1 \wedge \mathcal{C}_2 = (\mathrm{A}_1 \vee \mathrm{A}_2, \Gamma_1) = (\mathrm{A}_1 \vee \mathrm{A}_2, \Gamma_2).$$

Clearly, these are very special cases. The reason why the the conjunction does not exist in general lies in the fact that the class of input-output systems that simultaneously implement $\mathcal{C}_1$ and $\mathcal{C}_2$ cannot necessarily be expressed as the class of implementations of a single contract. On a high level, part of the problem is that the union of two linear spaces is generally not a linear space.

To see this, consider an input-output system Σ that implements both contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$. Since Σ implements $\mathcal{C}_1$, we know how it behaves when its input belongs to $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$, namely, we know that the corresponding input-output trajectories belong to $\mathfrak{B}(\Gamma_1)$. Similarly, since Σ implements $\mathcal{C}_2$, we know how it behaves when its input belongs to $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$. Therefore, we know how Σ behaves when its input belongs to the union $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \cup \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$. However, in view of Lemma 3.23, to obtain the conjunction $\mathcal{C}_1 \wedge \mathcal{C}_2$, we need to know how Σ behaves when its input belongs to the sum $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) + \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$, i.e., the smallest linear space that contains $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \cup \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$. This is because the input behaviour of any assumptions is a linear space, not merely a set.

With this in mind, we can intuitively interpret the result of Theorem 3.4 as follows. If the first condition of Theorem 3.4 holds, then it follows that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) + \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$, hence we know how Σ behaves when its input belongs to $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) + \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ and we can obtain the conjunction. On the other hand, if the second condition of Theorem 3.4 holds, then we know that Σ behaves the same whether its input belongs to $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ or $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$. Therefore, by linearity of the external behaviour of Σ, we know that Σ behaves the same when its input belongs to $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) + \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$, and we can obtain the conjunction.

3.7 Discussion

In this chapter, we introduced assume-guarantee contracts as specifications for linear dynamical input-output systems. These contracts were defined as a pair of linear systems called assumptions and guarantees. The assumptions captured available knowledge about the dynamics of the environment in which a system is expected to operate, while the guarantees captured the desired dynamics of the system when interconnected with a relevant environment. This was formalized with the notion of behaviour and behavioural inclusion. Then, following the meta-theory outlined in Chapter 2, we defined and characterized notions of implementation, consistency, refinement, and conjunction.

First, we showed that a given system implements a given contract if and only if a single behavioural inclusion holds. Since behavioural inclusion can be verified algorithmically, this allows implementation to be verified algorithmically. Then, we turned to the problem of constructing an implementation of a given contract. To solve this problem, we first obtained necessary and sufficient conditions for contract consistency, i.e., the existence of an implementation of a given contract. In the process, we also obtained a procedure for constructing an implementation of a consistent contract.

Next, we discussed the notion of refinement, which allowed us to determine if one contract expresses a stricter specification than another contract.

Moreover, as explained in Chapter 2, refinement has an essential role in enabling the independent design of components within interconnected systems. We obtained necessary and sufficient conditions for refinement that take the form of a pair of behavioural inclusions involving only assumptions and guarantees. As such, these conditions can be verified algorithmically.

Lastly, we discussed the notion of conjunction, which allowed us to fuse the specifications that two contracts express. We showed that the conjunction of two arbitrary contracts does not necessarily exists. Nevertheless, we presented two cases where the conjunction does exist, and we provided an explicit expression for the conjunction in these cases.

In conclusion, the results in this chapter allow us to use contracts to express, compare and combine specifications on the external dynamics of a component. Furthermore, they allow us to algorithmically *verify* that a given component satisfies a given specification, and to algorithmically *design* a component that satisfies a given specification. Nevertheless, there are a couple of limitations to our approach. First, computing the Smith canonical form is computationally heavy as it generally requires a very large number of polynomial divisions [74, Section 1.8], or the computation of a number of greatest common divisors and Bezout coefficients [82]. Therefore, although we have algorithmic procedures for verification and design, they are not necessarily efficient. Second, we currently do not know how to tackle problems related to control design, e.g., how to design a feedback controller for a given plant system such that the controlled plant satisfies a given specification expressed by a contract. These limitations are addressed in Chapter 5, where we define contracts using simulation instead of behavioural inclusion as a means of comparing system behaviour.

Chapter 4

Composition of behavioural contracts

In this chapter, we will further develop the contract theory introduced in the last chapter by introducing notions of contract composition.[1] As discussed in Chapter 2, the notion of contract composition, together with the notion of contract refinement introduced in the last chapter, enables the independent design of components within interconnected systems. Loosely speaking, the notion of contract composition aims 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 chapter, we will consider two types of interconnection, namely, the series interconnection and the feedback interconnection. We will define these interconnections fairly generally, which will ultimately allow us to analyse a large class of interconnected systems by decomposing them into a sequence of series and feedback interconnections.

We make the following contributions in the chapter. To begin with, following the meta-theoretic definition of composition outlined in Chapter 2, we define the series composition of two contracts according to the series interconnection of components. We show that the series composition does not necessarily exist for arbitrary contracts. To understand this better and gain some intuition, we restrict ourselves to the simpler special case where both contracts have output guarantees. With this restriction in place, we obtain a necessary and sufficient condition for the existence of the series composition, and we provide an explicit expression for it when it exists. For this, we make use of the fact that contracts with output guarantees have autonomous implementations.

[1] Part of this chapter has appeared in [83].

Then, we define the feedback composition of two contracts according to the feedback interconnection of components. We do this by following the meta-theoretic definition of composition outlined in Chapter 2 again. Like the series composition, the feedback composition does not necessarily exist for arbitrary contracts, which motivates us to first consider the special case where both contracts have output guarantees. In this special case, we obtain a necessary and sufficient condition for the existence of the feedback composition and we provide an explicit expression for it when it exists.

Finally, we treat the general cases for the feedback and series compositions. First, we obtain a necessary and sufficient condition for the existence of the feedback composition, and we provide an explicit expression for it when it exists. Then, by treating the series interconnection as a special case of the feedback interconnection, we use our results on the feedback composition to obtain a necessary and sufficient condition for the existence of the series composition, and an explicit expression for it when it exists. We also show that both types of composition satisfy the independent refinement property described in Chapter 2. Notably, the condition for the existence of each type of composition takes the form of behavioural inclusion, which can be verified algorithmically. Furthermore, the assumptions and guarantees for the composition can be obtained algorithmically from the assumptions and guarantees of the contracts that are composed.

This chapter is structured as follows. In Section 4.1, we define the two types of system interconnections that will be considered throughout this chapter, namely, the series interconnection and the feedback interconnection. Then, in Section 4.2, we define the series composition of two contracts and treat the special case where both contracts have output guarantees. Similarly, in Section 4.3, we define the feedback composition of two contracts and treat the special case where both contracts have output guarantees. We proceed by treating the general case for the feedback composition in Section 4.4, after which we go back and treat the general case of the series composition in Section 4.5. Finally, we discuss a modification of the series and feedback compositions in Section 4.6, and we end this chapter with a brief discussion in Section 4.7.

4.1 System interconnections

In this section, we will define two types of interconnections for input-output systems, namely, the series interconnection and the feedback interconnection. We will also define the analogous series and feedback interconnections of guarantees. In addition, we will define notions of well-posedness for each feedback interconnection and will provide simple necessary and sufficient conditions for well-posedness of each feedback interconnection. Here, as well as throughout the rest of this chapter, we will consider the input-output sys-

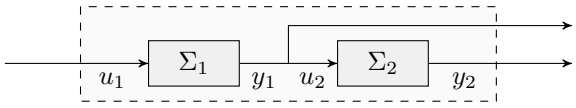

Figure 4.1: The series interconnection $\Sigma_1 \to \Sigma_2$.

tems

$$\Sigma_j : P_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y_j = Q_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u_j, \quad j \in \{1,2\}, \tag{4.1}$$

and the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$, where

$$\mathrm{A}_j : 0 = A_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u_j \quad \text{and} \quad \Gamma_j : G_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y_j = H_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u_j, \quad j \in \{1,2\}. \tag{4.2}$$

4.1.1 Series interconnection

The series interconnection of Σ_1 to Σ_2 is obtained by setting the output of Σ_1 as input of Σ_2, as shown in Figure 4.1. Note that we consider both the output of Σ_1 and the output of Σ_2 as outputs of their series interconnection. Formally, we have the following definition.

Definition 4.1. Consider the input-output systems Σ_1 and Σ_2 given by (4.1). The *series interconnection* of Σ_1 to Σ_2, denoted by $\Sigma_1 \to \Sigma_2$, is obtained by setting $u_2 = y_1$, as shown in Figure 4.1. This results in the system

$$\Sigma_1 \to \Sigma_2 : P\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y = Q\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u, \tag{4.3}$$

where $y = (y_1, y_2)$, $u = u_1$, and

$$P(s) = \begin{bmatrix} P_1(s) & 0 \\ -Q_2(s) & P_2(s) \end{bmatrix} \quad \text{and} \quad Q(s) = \begin{bmatrix} Q_1(s) \\ 0 \end{bmatrix}. \tag{4.4}$$

Note that the series interconnection $\Sigma_1 \to \Sigma_2$ is in input-output form because Σ_1 and Σ_2 are in input-output form. Indeed, $P(s)$ is invertible because $P_1(s)$ and $P_2(s)$ are invertible, and

$$P(s)^{-1}Q(s) = \begin{bmatrix} P_1(s)^{-1}Q_1(s) \\ P_2(s)^{-1}Q_2(s)P_1(s)^{-1}Q_1(s) \end{bmatrix} \tag{4.5}$$

is proper because $P_1(s)^{-1}Q_1(s)$ and $P_2(s)^{-1}Q_2(s)$ are proper.

Analogously to the series interconnection of input-output systems, we can define the series interconnection of guarantees.

Definition 4.2. Consider the guarantees Γ_1 and Γ_2 given by (4.2). The *series interconnection* of Γ_1 to Γ_2, denoted by $\Gamma_1 \to \Gamma_2$, is obtained by setting $u_2 = y_1$, as shown in Figure 4.2. This results in the guarantees

$$\Gamma_1 \to \Gamma_2 : G\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y = H\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u, \tag{4.6}$$

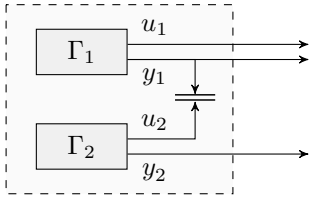

Figure 4.2: The series interconnection $\Gamma_1 \to \Gamma_2$. The long equality sign indicates the constraint $u_2 = y_1$.

where $y = (y_1, y_2)$, $u = u_1$, and

$$G(s) = \begin{bmatrix} G_1(s) & 0 \\ -H_2(s) & G_2(s) \end{bmatrix} \quad \text{and} \quad H(s) = \begin{bmatrix} H_1(s) \\ 0 \end{bmatrix}. \tag{4.7}$$

4.1.2 Feedback interconnection

The feedback interconnection of Σ_1 and Σ_2 is obtained by setting part of the output of Σ_1 as part of the input of Σ_2, and vice versa, as shown in Figure 4.3 To formalize this, we partition the inputs and outputs of Σ_1 and Σ_2 as

$$\begin{aligned} u_j &= (u_{j1}, u_{j2}), \\ y_j &= (y_{j1}, y_{j2}), \end{aligned} \qquad j \in \{1, 2\}, \tag{4.8}$$

and the polynomial matrices

$$\begin{aligned} P_j(s) &= \begin{bmatrix} P_{j1}(s) & P_{j2}(s) \end{bmatrix}, \\ Q_j(s) &= \begin{bmatrix} Q_{j1}(s) & Q_{j2}(s) \end{bmatrix}, \end{aligned} \qquad j \in \{1, 2\}, \tag{4.9}$$

accordingly. The feedback interconnection is defined as follows.

Definition 4.3. Consider the input-output systems Σ_1 and Σ_2 given by (4.1), and the partitions (4.8) and (4.9). The *feedback interconnection* of Σ_1 to Σ_2, denoted by $\Sigma_1 \leftarrow \Sigma_2$, is obtained by setting $y_{12} = u_{21}$ and $y_{21} = u_{12}$, as shown in Figure 4.3. This results in

$$\Sigma_1 \leftarrow \Sigma_2 : \left(P\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) - Q_{\mathrm{i}}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right)\right) y = Q_{\mathrm{e}}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u, \tag{4.10}$$

where $y = (y_{11}, y_{12}, y_{21}, y_{22})$, $u = (u_{11}, u_{22})$, and

$$P(s) = \begin{bmatrix} P_{11}(s) & P_{12}(s) & 0 & 0 \\ 0 & 0 & P_{21}(s) & P_{22}(s) \end{bmatrix}, \tag{4.11}$$

$$Q_{\mathrm{i}}(s) = \begin{bmatrix} 0 & 0 & Q_{12}(s) & 0 \\ 0 & Q_{21}(s) & 0 & 0 \end{bmatrix}, \tag{4.12}$$

$$Q_{\mathrm{e}}(s) = \begin{bmatrix} Q_{11}(s) & 0 \\ 0 & Q_{22}(s) \end{bmatrix}. \tag{4.13}$$

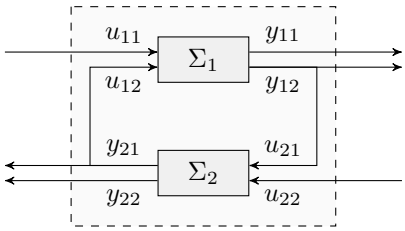

Figure 4.3: The feedback interconnection $\Sigma_1 \hookleftarrow \Sigma_2$.

Here, the subscript i indicates that Q_{i} is related to the internal (or interconnection) inputs u_{12} and u_{21}, whereas the subscript e indicates that Q_{e} is related to the external inputs u_{11} and u_{22}.

The feedback interconnection $\Sigma_1 \hookleftarrow \Sigma_2$ is not guaranteed to be in input-output form, even if Σ_1 and Σ_2 are in input-output form. For that, we need $P(s) - Q_{\mathrm{i}}(s)$ to be invertible and $\left(P(s) - Q_{\mathrm{i}}(s)\right)^{-1} Q_{\mathrm{e}}(s)$ to be proper, where $P(s)$, $Q_{\mathrm{i}}(s)$ and $Q_{\mathrm{e}}(s)$ are defined as in Definition 4.3. Since $P(s)$ is invertible, $P(s) - Q_{\mathrm{i}}(s)$ is invertible if and only if $I - P(s)^{-1}Q_{\mathrm{i}}(s)$ is invertible, and

$$\left(P(s) - Q_{\mathrm{i}}(s)\right)^{-1} Q_{\mathrm{e}}(s) = \left(I - P(s)^{-1}Q_{\mathrm{i}}(s)\right)^{-1} P(s)^{-1}Q_{\mathrm{e}}(s). \tag{4.14}$$

Note that $P(s)^{-1}Q_{\mathrm{e}}(s)$ is proper because Σ_1 and Σ_2 are in input-output form. Therefore, a sufficient condition for $\Sigma_1 \hookleftarrow \Sigma_2$ to be in input-output form is that $I - P(s)^{-1}Q_{\mathrm{i}}(s)$ is invertible and its inverse $(I - P(s)^{-1}Q_{\mathrm{i}}(s))^{-1}$ is proper. In fact, the latter is a necessary condition if we consider a slightly stronger requirement for the feedback interconnection, namely, that it is *well-posed*.

Recall from Remark 3.1 that $P(s) - Q_{\mathrm{i}}(s)$ being invertible implies that u is free in $\mathfrak{B}(\Sigma_1 \hookleftarrow \Sigma_2)$. On the other hand, $\left(P(s) - Q_{\mathrm{i}}(s)\right)^{-1} Q_{\mathrm{e}}(s)$ being proper implies that $\Sigma_1 \hookleftarrow \Sigma_2$ is non-anticipating, that is, y does not depend on the derivatives of u. Therefore, $\Sigma_1 \hookleftarrow \Sigma_2$ being in input-output form implies that the external inputs u_{11} and u_{22} are free, and the outputs y_{11}, y_{12}, y_{21} and y_{22} do not depend on derivatives of these external inputs. For well-posedness, we also require that the external outputs do not depend on derivatives of the *internal* inputs u_{12} and u_{21}. In other words, $\Sigma_1 \hookleftarrow \Sigma_2$ is well-posed if the system obtained by injecting virtual inputs v_{12} and v_{21} to the internal inputs of $\Sigma_1 \hookleftarrow \Sigma_2$, as shown in Figure 4.4, is in input-output form. Formally, we have the following definition.

Definition 4.4. The feedback interconnection $\Sigma_1 \hookleftarrow \Sigma_2$, as defined in Definition 4.3, is *well-posed* if the associated system

$$\Sigma_1 \hookleftarrow_v \Sigma_2 : \left(P\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) - Q_{\mathrm{i}}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right)\right) y = Q_{\mathrm{e}}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u + Q_{\mathrm{v}}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) v, \tag{4.15}$$

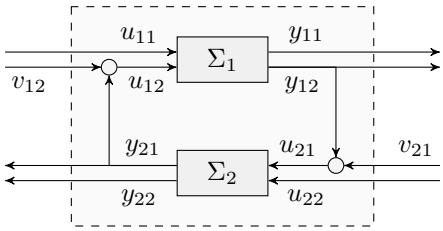

Figure 4.4: The system $\Sigma_1 \leftrightarrow_v \Sigma_2$ associated to $\Sigma_1 \leftarrow\!\!\rightarrow \Sigma_2$.

shown in Figure 4.4, is in input-output form, where $v = (v_{21}, v_{12})$ and

$$Q_{\mathrm{v}}(s) = \begin{bmatrix} 0 & Q_{12}(s) \\ Q_{21}(s) & 0 \end{bmatrix}. \tag{4.16}$$

In other words, $\Sigma_1 \leftarrow\!\!\rightarrow \Sigma_2$ is well-posed if $P(s) - Q_{\mathrm{i}}(s)$ is invertible, and

$$\left(P(s) - Q_{\mathrm{i}}(s)\right)^{-1} Q_{\mathrm{e}}(s) \quad \text{and} \quad \left(P(s) - Q_{\mathrm{i}}(s)\right)^{-1} Q_{\mathrm{v}}(s) \tag{4.17}$$

are proper.

Note that we can rewrite (4.17) as

$$\left(I - P(s)^{-1}Q_{\mathrm{i}}(s)\right)^{-1} P(s)^{-1}Q_{\mathrm{e}}(s), \tag{4.18}$$

$$\left(I - P(s)^{-1}Q_{\mathrm{i}}(s)\right)^{-1} P(s)^{-1}Q_{\mathrm{v}}(s), \tag{4.19}$$

where $P(s)^{-1}Q_{\mathrm{e}}(s)$ and $P(s)^{-1}Q_{\mathrm{v}}(s)$ are proper because Σ_1 and Σ_2 are input-output systems. Therefore, a sufficient condition for well-posedness is that $I - P(s)^{-1}Q_{\mathrm{i}}(s)$ is invertible and $(I - P(s)^{-1}Q_{\mathrm{i}}(s))^{-1}$ is proper. Due to Proposition 3.3, the latter holds if and only if

$$\lim_{s\to\infty} I - P(s)^{-1}Q_{\mathrm{i}}(s) \tag{4.20}$$

is invertible, where we note that the limit exists because $P(s)^{-1}Q_{\mathrm{i}}(s)$ is proper. The following proposition, whose proof can be found in Appendix B.1, shows that this condition is not only sufficient but also necessary for well-posedness.

Proposition 4.1. *The feedback interconnection $\Sigma_1 \leftarrow\!\!\rightarrow \Sigma_2$, as defined in Definition 4.3, is well-posed if and only if*

$$\lim_{s\to\infty} I - P(s)^{-1}Q_{\mathrm{i}}(s) \tag{4.21}$$

is invertible.

Recall that $T_1(s) = P_1(s)^{-1}Q_1(s)$ and $T_2(s) = P_2(s)^{-1}Q_2(s)$ are the transfer functions of Σ_1 and Σ_2, respectively. If we partition

$$T_1(s) = \begin{bmatrix} T_{11}(s) & T_{12}(s) \end{bmatrix} \quad \text{and} \qquad T_2(s) = \begin{bmatrix} T_{21}(s) & T_{22}(s) \end{bmatrix} \tag{4.22}$$

according to the partitions of $Q_1(s)$ and $Q_2(s)$, respectively, then Proposition 4.1 tells us that $\Sigma_1 \leftarrow\!\!\rightarrow \Sigma_2$ is well-posed if and only if

$$\lim_{s\to\infty} \begin{bmatrix} I & \begin{bmatrix} T_{12}(s) & 0 \end{bmatrix} \\ \begin{bmatrix} 0 & T_{21}(s) \end{bmatrix} & I \end{bmatrix} \tag{4.23}$$

is invertible. This coincides with the usual transfer matrix condition for well-posedness of the feedback interconnection, see, e.g., [84, Section 5.2]. Moreover, if Σ_1^s and Σ_2^s are input-state-output systems with the same external behaviour as Σ_1 and Σ_2, respectively, and feedthrough matrices partitioned as

$$D_1 = \begin{bmatrix} D_{11} & D_{12} \end{bmatrix}, \qquad D_2 = \begin{bmatrix} D_{21} & D_{22} \end{bmatrix}, \tag{4.24}$$

according to (4.8), then $\Sigma_1 \leftarrow\!\!\rightarrow \Sigma_2$ is well-posed if and only if

$$\begin{bmatrix} I & \begin{bmatrix} D_{12} & 0 \end{bmatrix} \\ \begin{bmatrix} 0 & D_{21} \end{bmatrix} & I \end{bmatrix} \tag{4.25}$$

is invertible, which is another well-known condition for well-posedness.

Analogously to the feedback interconnection of input-output systems, we can define the feedback interconnection of guarantees. To do this end, we first partition the polynomial matrices

$$\begin{aligned} G_j(s) &= \begin{bmatrix} G_{j1}(s) & G_{j2}(s) \end{bmatrix}, \\ H_j(s) &= \begin{bmatrix} H_{j1}(s) & H_{j2}(s) \end{bmatrix}, \end{aligned} \qquad j \in \{1, 2\}, \tag{4.26}$$

according to (4.8).

Definition 4.5. Consider the guarantees Γ_1 and Γ_2 given by (4.2), and the partitions (4.8) and (4.26). The *feedback interconnection* of Γ_1 to Γ_2, denoted by $\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2$, is obtained by setting $y_{12} = u_{21}$ and $y_{21} = u_{12}$, as shown in Figure 4.5. This results in

$$\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2 : \left(G\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) - H_{\mathrm{i}}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right)\right) y = H_{\mathrm{e}}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u, \tag{4.27}$$

where $y = (y_{11}, y_{12}, y_{21}, y_{22})$, $u = (u_{11}, u_{22})$, and

$$G(s) = \begin{bmatrix} G_{11}(s) & G_{12}(s) & 0 & 0 \\ 0 & 0 & G_{21}(s) & G_{22}(s) \end{bmatrix}, \tag{4.28}$$

$$H_{\mathrm{i}}(s) = \begin{bmatrix} 0 & 0 & H_{12}(s) & 0 \\ 0 & H_{21}(s) & 0 & 0 \end{bmatrix}, \tag{4.29}$$

$$H_{\mathrm{e}}(s) = \begin{bmatrix} H_{11}(s) & 0 \\ 0 & H_{22}(s) \end{bmatrix}. \tag{4.30}$$

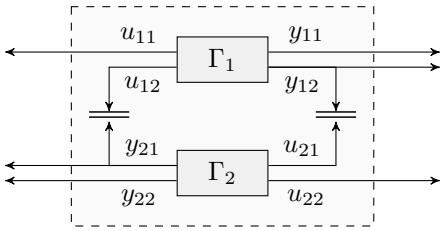

Figure 4.5: The feedback interconnection $\Gamma_1 \leftarrow\!\!\!\rightarrow \Gamma_2$. The long equality signs indicate the constraints $u_{12} = y_{21}$ and $u_{21} = y_{12}$.

The following definition of well-posedness for the feedback interconnection of guarantees can be seen as a generalization of the definition of well-posedness for input-output systems.

Definition 4.6. The feedback interconnection $\Gamma_1 \leftarrow\!\!\!\rightarrow \Gamma_2$ is *well-posed* if there exist input-output systems Σ_1 and Σ_2 such that $\mathfrak{B}(\Sigma_1) \subset \mathfrak{B}(\Gamma_1)$, $\mathfrak{B}(\Sigma_2) \subset \mathfrak{B}(\Gamma_2)$, and the feedback interconnection $\Sigma_1 \leftarrow\!\!\!\rightarrow \Sigma_2$ is well-posed.

The following proposition, whose proof can be found in Appendix B.2, provides a necessary and sufficient condition for well-posedness of $\Gamma_1 \leftarrow\!\!\!\rightarrow \Gamma_2$ that is analogous to the condition for well-posedness of $\Sigma_1 \leftarrow\!\!\!\rightarrow \Sigma_2$ in Proposition 4.1.

Proposition 4.2. *Suppose that the guarantees Γ_1 and Γ_2 given by* (4.2) *are such that $G_1(s)$ and $G_2(s)$ are row-reduced. The feedback interconnection $\Gamma_1 \leftarrow\!\!\!\rightarrow \Gamma_2$, as defined in Definition 4.5, is well-posed if and only if $D(s)^{-1}H_{\mathrm{e}}(s)$ is proper and*

$$\lim_{s\to\infty} D(s)^{-1}\left(G(s) - H_{\mathrm{i}}(s)\right) \tag{4.31}$$

exists and has full row rank, where $D(s)$ is the row-degree matrix of $G(s)$.

Definition 4.6 and Proposition 4.2 can be seen as generalizations of Definition 4.4 and Proposition 4.1 in the following sense. Suppose that Γ_1 and Γ_2 are in input-output form, that is, $G_1(s)$ and $G_2(s)$ are square and invertible, and $G_1(s)^{-1}H_1(s)$ and $G_2(s)H_2(s)$ are proper. This implies that $G(s)$ is square and invertible and $G(s)^{-1}H_{\mathrm{e}}(s)$ is proper. Since $D(s)$ is the row-degree matrix of $G(s)$, it follows that $D(s)^{-1}G(s)$ is proper and, thus,

$$D(s)^{-1}H_{\mathrm{e}}(s) = D(s)^{-1}G(s)G(s)^{-1}H_{\mathrm{e}}(s), \tag{4.32}$$

is also proper. On the other hand, we have that

$$D(s)^{-1}\left(G(s) - H_{\mathrm{i}}(s)\right) = D(s)^{-1}G(s)(I - G(s)^{-1}H_{\mathrm{i}}(s)). \tag{4.33}$$

Since $G_1(s)$ and $G_2(s)$ are row-reduced, $G(s)$ is also row-reduced, hence

$$\lim_{s\to\infty} D(s)^{-1}G(s) \tag{4.34}$$

exists and is invertible. Therefore, (4.31) exists and is invertible if and only if

$$\lim_{s\to\infty} I - G(s)^{-1}H_{\mathrm{i}}(s) \tag{4.35}$$

exists and is invertible, which is precisely the condition in Proposition 4.1. Consequently, if Γ_1 and Γ_2 are in input-output form, then $\Gamma_1 \leftarrow \Gamma_2$ is well-posed as a feedback interconnection of guarantees if and only if it is well-posed as a feedback interconnection of input-output systems. Of course, Γ_1 and Γ_2 are generally not in input-output form, which motivates Definition 4.6.

Remark 4.1. *Proposition 4.2 implies that u is free in $\mathfrak{B}(\Gamma_1 \leftarrow \Gamma_2)$ when $G_1(s)$ and $G_2(s)$ are row-reduced and $\Gamma_1 \leftarrow \Gamma_2$ is well-posed. Indeed,* (B.20) *having full row rank implies that $D(s)^{-1}\left(G(s) - H_{\mathrm{i}}(s)\right)$ and, thus, $G(s) - H_{\mathrm{i}}(s)$ have full row rank. As shown in the proof of [63, Theorem 6.2.6], this implies that u is free in $\mathfrak{B}(\Gamma_1 \leftarrow \Gamma_2)$.*

Remark 4.2. *If u_{12}, y_{11}, u_{22} and y_{21} are void in* (4.8)*, then the feedback interconnection reduces to the series interconnection. This is easily seen from their definitions. Therefore, we can view the series interconnection as a special case of the feedback interconnection. We will make use of this observation to obtain results on the series composition of two contracts from our results on the feedback composition. Note that, by treating the series interconnection as a special case of the feedback interconnection, we obtain notions of well-posedness for $\Sigma_1 \to \Sigma_2$ and $\Gamma_1 \to \Gamma_2$. Then, it is easily seen that $\Sigma_1 \to \Sigma_2$ is well-posed because Σ_1 and Σ_2 are in input-output form. However, $\Gamma_1 \to \Gamma_2$ is not necessarily well-posed. Indeed, in general, there might be no input-output systems Σ_1 and Σ_2 such that $\mathfrak{B}(\Sigma_1) \subset \mathfrak{B}(\Gamma_1)$ and $\mathfrak{B}(\Sigma_2) \subset \mathfrak{B}(\Gamma_2)$.*

We conclude this section with the following proposition, which shows the interplay between behavioural inclusion and the feedback interconnection of guarantees. Note that the same holds if the feedback interconnection is replaced by the series interconnection.

Proposition 4.3. *If $\mathfrak{B}(\Gamma_1') \subset \mathfrak{B}(\Gamma_1)$ and $\mathfrak{B}(\Gamma_2') \subset \mathfrak{B}(\Gamma_2)$, then*

$$\mathfrak{B}(\Gamma_1' \leftarrow \Gamma_2') \subset \mathfrak{B}(\Gamma_1 \leftarrow \Gamma_2) \tag{4.36}$$

Proof. Note that $(u, y) \in \mathfrak{B}(\Gamma_1' \leftarrow \Gamma_2')$ if and only if

$$(u_{11}, y_{21}, y_{11}, y_{12}) \in \mathfrak{B}(\Gamma_1') \quad \text{and} \quad (y_{12}, u_{22}, y_{21}, y_{22}) \in \mathfrak{B}(\Gamma_2'). \tag{4.37}$$

If $\mathfrak{B}(\Gamma_1') \subset \mathfrak{B}(\Gamma_1)$ and $\mathfrak{B}(\Gamma_2') \subset \mathfrak{B}(\Gamma_2)$, the latter implies that

$$(u_{11}, y_{21}, y_{11}, y_{12}) \in \mathfrak{B}(\Gamma_1) \quad \text{and} \quad (y_{12}, u_{22}, y_{21}, y_{22}) \in \mathfrak{B}(\Gamma_2), \tag{4.38}$$

which holds if and only if $(u, y) \in \mathfrak{B}(\Gamma_1' \leftarrow \Gamma_2')$. □

4.2 Series composition with output guarantees

In this section, we will consider the series composition of two contracts in the special case where they have output guarantees, see Remark 3.7. We will begin by defining the series composition of two contracts in the general case. This definition will correspond to the definition of the series interconnection of two input-output systems. To get some intuition behind the properties required by the series composition, we will then restrict ourselves to the case where both contracts have output guarantees. We will see that the series composition does not necessarily exist. Indeed, we will obtain necessary and sufficient conditions for its existence that will not be satisfied for arbitrary contracts. Nevertheless, these conditions will be easily verifiable, and we will provide an explicit expression for the series composition when it exists.

Consider the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ given by (4.2). Following the meta-theoretic definition outlined in Chapter 2, the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ should be a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies the following properties. 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. First, the environments of Σ_1 and Σ_2 in the interconnection $\mathrm{E} \wedge (\Sigma_1 \to \Sigma)$ should be compatible with $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Second, $\Sigma_1 \to \Sigma_2$ should be an implementation of $\mathcal{C}$. Recall Definition 4.1 of the series interconnection and its graphical representation in Figure 4.1. Note that, in the interconnection $\mathrm{E} \wedge (\Sigma_1 \to \Sigma_2)$, the inputs of Σ_1 and Σ_2 are given by u and y_1, respectively. Therefore, the first property holds if and only if

$$(u, y) \in \mathfrak{B}(\mathrm{E} \wedge (\Sigma_1 \to \Sigma_2)) \quad \Longrightarrow \quad \begin{cases} u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1), \\ y_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2). \end{cases} \tag{4.39}$$

It is easily seen that the latter holds for all environments E compatible with $\mathcal{C}$ if and only if it holds for the assumptions A. On the other hand, due to Theorem 3.1, the second property holds if and only if

$$(u, y) \in \mathfrak{B}(\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2)) \quad \Longrightarrow \quad (u, y) \in \mathfrak{B}(\Gamma). \tag{4.40}$$

In other words, $\mathcal{C}$ should satisfy the following implication.

Implication 4.1. *If Σ_1 and Σ_2 implement $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$, respectively, then the following implication holds:*

$$(u, y) \in \mathfrak{B}(\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2)) \quad \Longrightarrow \quad \begin{cases} u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1), \\ y_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2), \\ (u, y) \in \mathfrak{B}(\Gamma). \end{cases} \tag{4.41}$$

Recall that u is free in $\mathfrak{B}(\Sigma_1 \to \Sigma_2)$ because $\Sigma_1 \to \Sigma_2$ is in input-output form. Therefore, the first part of (4.41) holds if and only if $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$,

which can be ensured by choosing assumptions A whose input behaviour is as small as possible, i.e., such that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) = \{0\}$. On the other hand, we can ensure that the third part of (4.41) holds by choosing guarantees Γ whose external behaviour is as large as possible, i.e., the whole space of smooth functions. However, there are no choices for A and Γ that ensure that the second part of (4.41) holds. Indeed, the second part holds if and only if the output of Σ_1 is guaranteed to be in $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ for any input from $\mathfrak{B}_{\mathrm{i}}(\mathrm{A})$. Since the zero input is always in $\mathfrak{B}_{\mathrm{i}}(\mathrm{A})$, it follows that the output of Σ_1 for zero input must be in $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$. This property is independent of the choice of A and Γ. In other words, there does not necessarily exist a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 4.1 for arbitrary contracts $\mathcal{C}_1$ and $\mathcal{C}_2$. This motivates the following definition.

Definition 4.7. The contract $\mathcal{C}_1$ is *series composable* to $\mathcal{C}_2$ if there exists a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 4.1.

With this in mind, we define the series composition as follows.

Definition 4.8. Suppose that $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$. The *series composition* of $\mathcal{C}_1$ to $\mathcal{C}_2$, denoted by $\mathcal{C}_1 \to \mathcal{C}_2$, is the *smallest* contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 4.1.

The definition of the series composition has the following aspects. First, the series composition must satisfy properties that support independent design, as captured by Implication 4.1. Second, the series composition must be the smallest contract that satisfies these properties. Here, smallest is with respect to refinement, see Remark 3.14. Intuitively, this means that the series composition assumes the least and guarantees the most while still ensuring that these properties are satisfied.

To get some intuition behind the series composition, and contract composition in general, for the remainder of this section, we will assume that Γ_1 and Γ_2 are output guarantees. This will make the analysis simpler and will allow us to focus on the main ideas. The general case of the series composition will be treated as a special case of the feedback composition in Section 4.4.

With this in mind, even if there exists a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 4.1, the smallest such contract might not exist. In other words, even if $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$, the series composition $\mathcal{C}_1 \to \mathcal{C}_2$ might not exist. Fortunately, this turns out to be false. By the end of this section, we will show that the series composition $\mathcal{C}_1 \to \mathcal{C}_2$ exists if $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$, and we will provide an explicit expression for it when it exists.

In the meantime, we turn to finding tractable conditions on A and Γ under which the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.1. To do this, we will make use of autonomous implementations. Consider the following definition.

Definition 4.9. An input-output system Σ is *autonomous* if

$$\Sigma : P\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y = 0, \tag{4.42}$$

where $P(s)$ is a square and invertible polynomial matrix.

In Remark 3.8, we saw that a contract with output guarantees is always consistent and there exists an autonomous system that implements it. Using the following lemma, whose proof can be found in Appendix B.3, we will show that the class of autonomous implementations is rich enough to yield necessary and sufficient conditions for the satisfaction of Implication 4.1 solely in terms of assumptions and guarantees.

Lemma 4.4. *Consider output guarantees Γ and a behaviour $\mathfrak{B}$. If $\mathfrak{B}_{\mathrm{o}}(\Sigma) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma)$ implies $\mathfrak{B}_{\mathrm{o}}(\Sigma) \subset \mathfrak{B}$ for all autonomous Σ, then $\mathfrak{B}_{\mathrm{o}}(\Gamma) \subset \mathfrak{B}$.*

Remark 4.3. *Note that, for any assumptions A, $\mathfrak{B}_{\mathrm{o}}(\mathrm{A} \wedge \Sigma) = \mathfrak{B}_{\mathrm{o}}(\Sigma)$ if Σ is autonomous. Therefore, due to Remark 3.7, if Γ are output guarantees, then an autonomous system Σ implements the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ if and only if $\mathfrak{B}_{\mathrm{o}}(\Sigma) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma)$. Consequently, Lemma 4.4 tells us that $\mathfrak{B}_{\mathrm{o}}(\Gamma) \subset \mathfrak{B}$ if $\mathfrak{B}_{\mathrm{o}}(\Sigma) \subset \mathfrak{B}$ for all autonomous Σ that implement $\mathcal{C}$. In other words, a behavioural inclusion involving an arbitrary autonomous Σ that implements $\mathcal{C}$ is guaranteed to hold only if it holds with Σ replaced by Γ.*

With Remark 4.3 in mind, we obtain the following lemma.

Lemma 4.5. *Suppose that Γ_1 and Γ_2 are output guarantees, and consider the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$. Then, the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.1 if and only if*

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1), \tag{4.43}$$

$$\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2), \tag{4.44}$$

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_2) \subset \mathfrak{B}(\Gamma). \tag{4.45}$$

Proof. We begin by proving necessity. Suppose that $\mathcal{C}$ satisfies Implication 4.1. Suppose that the autonomous systems

$$\Sigma_1 : P_1\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y_1 = 0 \quad \text{and} \quad \Sigma_2 : P_2\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y_2 = 0, \tag{4.46}$$

implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and let A be given by (3.73). Then,

$$\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2) : \begin{bmatrix} P_1\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) & 0 \\ 0 & P_2\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) \\ 0 & 0 \end{bmatrix} y = \begin{bmatrix} 0 \\ 0 \\ A\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) \end{bmatrix} u, \tag{4.47}$$

and we have that

$$\mathfrak{B}(\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2)) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \times \mathfrak{B}_{\mathrm{o}}(\Sigma_1) \times \mathfrak{B}_{\mathrm{o}}(\Sigma_2). \tag{4.48}$$

Since $\mathcal{C}$ satisfies Implication 4.1, the latter implies that

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1), \tag{4.49}$$

$$\mathfrak{B}_{\mathrm{o}}(\Sigma_1) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2), \tag{4.50}$$

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \times \mathfrak{B}_{\mathrm{o}}(\Sigma_1) \times \mathfrak{B}_{\mathrm{o}}(\Sigma_2) \subset \mathfrak{B}(\Gamma), \tag{4.51}$$

which shows that (4.43) holds. On the other hand, due to Remark 4.3, (4.50) and (4.51) hold for all autonomous Σ_1 and Σ_2 that implement $\mathcal{C}_1$ and $\mathcal{C}_2$ only if (4.44) and (4.45) hold. Indeed, let

$$\mathfrak{B}_a = \{\, u \mid (u,0,0) \in \mathfrak{B}(\Gamma) \,\}, \tag{4.52}$$

$$\mathfrak{B}_1 = \{\, y_1 \mid (0,y_1,0) \in \mathfrak{B}(\Gamma) \,\}, \tag{4.53}$$

$$\mathfrak{B}_2 = \{\, y_2 \mid (0,0,y_2) \in \mathfrak{B}(\Gamma) \,\}. \tag{4.54}$$

Note that (4.51) holds only if $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_a$, $\mathfrak{B}_{\mathrm{o}}(\Sigma_1) \subset \mathfrak{B}_1$ and $\mathfrak{B}_{\mathrm{o}}(\Sigma_2) \subset \mathfrak{B}_2$. Due to Remark 4.3, the latter two imply that $\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathfrak{B}_1$ and $\mathfrak{B}_{\mathrm{o}}(\Gamma_2) \subset \mathfrak{B}_2$, which, together with the former $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_a$, shows that (4.45) holds.

We proceed by proving sufficiency. Suppose that (4.43), (4.44) and (4.45) hold. Let Σ_1 and Σ_2 be implementations of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and let $(u,y) \in \mathfrak{B}(\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2))$, that is, $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$ and $(u,y) \in \mathfrak{B}(\Sigma_1 \to \Sigma_2)$. To show that $\mathcal{C}$ satisfies Implication 4.1, we need to show that $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$, $y_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ and $(u,y) \in \mathfrak{B}_{\mathrm{i}}(\Gamma)$. With this in mind, $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$ and (4.43) immediately imply that $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$. On the other hand, by definition of the series interconnection, $(u,y) \in \mathfrak{B}(\Sigma_1 \to \Sigma_2)$ if and only if $(u,y_1) \in \mathfrak{B}(\Sigma_1)$ and $(y_1,y_2) \in \mathfrak{B}(\Sigma_2)$. This implies that $(u,y_1) \in \mathfrak{B}(\mathrm{A}_1 \wedge \Sigma_1)$ because $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$, while $\mathfrak{B}(\mathrm{A}_1 \wedge \Sigma_1) \subset \mathfrak{B}(\Gamma_1)$ because Σ_1 implements $\mathcal{C}_1$. Therefore, we have that $(u,y_1) \in \mathfrak{B}(\Gamma_1)$ and, thus, $y_1 \in \mathfrak{B}_{\mathrm{o}}(\Gamma_1)$, which yields $y_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ due to (4.44). Similarly, we now have that $(y_1,y_2) \in \mathfrak{B}(\mathrm{A}_2 \wedge \Sigma_2)$, which implies that $y_2 \in \mathfrak{B}_{\mathrm{o}}(\Gamma_2)$ and, thus, $(u,y) \in \mathfrak{B}(\Gamma)$ due to (4.45). □

Note that the conditions in Lemma 4.5 are in terms of assumptions and guarantees only, that is, they do not refer to implementations. Furthermore, while (4.43) and (4.45) depend on $\mathcal{C}$, (4.44) is independent of it. This means that (4.44) is a necessary condition for $\mathcal{C}_1$ to be series composable to $\mathcal{C}_2$. The following theorem shows that this condition is not only necessary but also sufficient. Furthermore, it shows that the series composition $\mathcal{C}_1 \to \mathcal{C}_2$ exists if $\mathcal{C}_1$ and $\mathcal{C}_2$ are series composable, and it provides an explicit expression for it when it exists.

Theorem 4.1. *Suppose that Γ_1 and Γ_2 are output guarantees. Then, the contract $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ is series composable to $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ if and only if*

$$\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2). \tag{4.55}$$

Furthermore, if $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$, then the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ exists and is given by

$$\mathcal{C}_1 \to \mathcal{C}_2 = (\mathrm{A}_1, \Gamma_1 \to \Gamma_2). \tag{4.56}$$

Proof. Lemma 4.5 already shows that $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$ only if (4.55) holds. To show the converse, suppose that (4.55) holds. We will show that $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.1 if and only if it refines the contract $\mathcal{C}_1 \to \mathcal{C}_2$ given by (4.56). To this end, due to Lemma 4.5 and the assumption that (4.55) holds, $\mathcal{C}$ satisfies Implication 4.1 if and only if (4.43) and (4.45) hold. Let A be given by (3.73). Since Γ_1 and Γ_2 are output guarantees, we have that

$$\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2) : \begin{bmatrix} G_1\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) & 0 \\ 0 & G_2\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \\ 0 & 0 \end{bmatrix} y = \begin{bmatrix} 0 \\ 0 \\ A\left(\frac{\mathrm{d}}{\mathrm{d}t}\right) \end{bmatrix} u. \tag{4.57}$$

which implies that

$$\mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2)) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_2), \tag{4.58}$$

This means that (4.45) is equivalent to

$$\mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2)) \subset \mathfrak{B}(\Gamma). \tag{4.59}$$

Consequently, due to Theorem 3.3, (4.43) and (4.45) hold if and only if $\mathcal{C}$ refines $\mathcal{C}_1 \wedge \mathcal{C}_2$. Since a contract refines itself, this shows that $\mathcal{C}_1 \to \mathcal{C}_2$ is the smallest contract that satisfies Implication 4.1. Therefore, $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$ and the contract $\mathcal{C}_1 \wedge \mathcal{C}_2$ given by (4.56) is indeed the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$. □

The condition (4.55) is quite intuitive. It effectively says that any output that an implementation of $\mathcal{C}_1$ can generate must be an input that an environment compatible with $\mathcal{C}_2$ can generate. Nevertheless, it is still surprising that this condition is necessary. Indeed, we expect the choice of assumptions A to potentially restrict the output behaviour of Σ_1 in the interconnection $\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2)$, and, thus, to relax the requirement expressed by (4.55). This does not happen when we consider output guarantees because the corresponding contracts have autonomous implementations. Loosely speaking, the reasoning is as follows. Since Γ_1 are output guarantees, there exists at least one autonomous implementation Σ_1 of $\mathcal{C}_1$. By considering an autonomous implementation Σ_1, we decouple the behaviour of the output generated by Σ_1 from the behaviour of the input generated by A in the interconnection $\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2)$. In particular, this means that $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$ only if $\mathfrak{B}_{\mathrm{o}}(\Sigma_1) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ for all autonomous Σ_1 that implement $\mathcal{C}_1$, which yields (4.55) due to Remark 4.3.

Remark 4.4. *A contract has an autonomous implementation if and only if it is equivalent to a contract with output guarantees. To see this, suppose that $\mathcal{C} = (\mathrm{A}, \Gamma)$ has an autonomous implementation Σ. Let A and Γ be given by* (3.73) *and* (3.75)*, and let Σ be given by* (4.42)*. Then, due to Corollary 3.16, there exist polynomial matrices $T(s)$ and $M(s)$ such that*

$$\begin{bmatrix} G(s) & -H(s) \end{bmatrix} = \begin{bmatrix} T(s) & M(s) \end{bmatrix} \begin{bmatrix} P(s) & 0 \\ 0 & -A(s) \end{bmatrix}. \tag{4.60}$$

In particular, this implies that $H(s) = -M(s)A(s)$, hence

$$\begin{bmatrix} G(s) & 0 \\ 0 & -A(s) \end{bmatrix} = \begin{bmatrix} I & M(s) \\ 0 & I \end{bmatrix} \begin{bmatrix} G(s) & -H(s) \\ 0 & -A(s) \end{bmatrix}. \tag{4.61}$$

Due to Corollary 3.15, this implies that the output guarantees

$$\Gamma_0 : G\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) y = 0 \tag{4.62}$$

are such that $\mathfrak{B}(\mathrm{A} \wedge \Gamma) = \mathfrak{B}(\mathrm{A} \wedge \Gamma_0)$, and, thus, $\mathcal{C}$ is equivalent to $\mathcal{C}_0 = (\mathrm{A}, \Gamma_0)$ because of Corollary 3.21.

We conclude this section by reformulating some of the results in a manner that will make them easier to generalize. To this end, analogously to the series interconnection of input-output systems, we can define the series interconnection of assumptions. In particular, consider the assumptions A_1 and A_2 given by (4.2). The *series interconnection* of A_1 to A_2, denoted by $\mathrm{A}_1 \to \mathrm{A}_2$ is obtained by setting $u_2 = y_1$. This results in the system

$$\mathrm{A}_1 \to \mathrm{A}_2 : -A_{\mathrm{i}}\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) y = A_{\mathrm{e}}\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) u, \tag{4.63}$$

where $u = u_1$, $y = (y_1, y_2)$, and

$$A_{\mathrm{i}}(s) = \begin{bmatrix} 0 & 0 \\ A_2(s) & 0 \end{bmatrix} \quad \text{and} \quad A_{\mathrm{e}}(s) = \begin{bmatrix} A_1(s) \\ 0 \end{bmatrix}. \tag{4.64}$$

Here, the subscript i indicates that $A_{\mathrm{i}}(s)$ is related to the internal input u_2, while the subscript o indicates that $A_{\mathrm{e}}(s)$ is related to the external input u_1. Note that $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ and $y_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ if and only if $(u, y) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \to \mathrm{A}_2)$. Therefore, (4.41) holds if and only if

$$\mathfrak{B}(\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2)) \subset \mathfrak{B}(\mathrm{A}_1 \to \mathrm{A}_2), \tag{4.65}$$

$$\mathfrak{B}(\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2)) \subset \mathfrak{B}(\Gamma). \tag{4.66}$$

Similarly, (4.43) and (4.44) hold if and only if

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_2) \subset \mathfrak{B}(\mathrm{A}_1 \to \mathrm{A}_2). \tag{4.67}$$

As shown in the proof of Theorem 4.1, we have that

$$\mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2)) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_2), \tag{4.68}$$

since Γ_1 and Γ_2 are output guarantees. Consequently, Lemma 4.5 tells us that $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.1 if and only if

$$\mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2)) \subset \mathfrak{B}(\mathrm{A}_1 \to \mathrm{A}_2), \tag{4.69}$$

$$\mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2)) \subset \mathfrak{B}(\Gamma). \tag{4.70}$$

Note the parallel between the latter and (4.65) and (4.66). Furthermore, note that in the sufficiency part of the proof of Lemma 4.5, we showed that

$$\mathfrak{B}(\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2)) \subset \mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2)) \tag{4.71}$$

when (4.43) and (4.44) hold, equivalently, when (4.69) holds. The latter immediately shows that (4.65) and (4.66) hold if (4.69) and (4.70) hold.

4.3 Feedback composition with output guarantees

In this section, we will consider the feedback composition of two contracts in the special case where they have output guarantees. We will begin by defining the feedback composition of two contracts in the general case. Characterizing the latter will prove to be somewhat more challenging than characterizing the series composition, even after we restrict ourselves to the case where both contracts have output guarantees. In particular, similarly to the series composition, we will easily find necessary conditions for the existence of the feedback composition by leveraging autonomous implementations. However, showing that these conditions are also sufficient will require some effort because the feedback interconnection contains a loop, unlike the series interconnection. Nevertheless, we will obtain necessary and sufficient conditions for the existence of the feedback composition, and we will provide an explicit expression for it when it exists.

Consider the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ given by (4.2), and the partitions in (4.8). Just like the series composition, we will define the feedback composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ following the meta-theoretic definition outlined in Chapter 2. This means that the feedback composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ should be a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies the following properties. 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. First, the environments of Σ_1 and Σ_2 in the interconnection $\mathrm{E} \wedge (\Sigma_1 \leftarrow\!\!\shortmid\!\!\rightarrow \Sigma)$ should be compatible with $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Second, $\Sigma_1 \leftarrow\!\!\shortmid\!\!\rightarrow \Sigma_2$ should be an implementation of $\mathcal{C}$. However, for the latter to be possible, we require $\Sigma_1 \leftarrow\!\!\shortmid\!\!\rightarrow \Sigma_2$ to be in input-output form. In fact, we will require that $\Sigma_1 \leftarrow\!\!\shortmid\!\!\rightarrow \Sigma_2$ is well-posed, which would guarantee that it is also in

input-output form. In addition, this will ensure a sort of predictability of the behaviour of $\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2$, and, in particular, it will allow us to resolve the loop in the feedback interconnection. We will elaborate on this later in this section.

With this in mind, recall Definition 4.3 of the feedback interconnection and its graphical representation in Figure 4.3. Note that, in the interconnection $\mathrm{E} \wedge (\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2)$, the inputs of Σ_1 and Σ_2 are given by (u_{11}, y_{21}) and (y_{12}, u_{22}), respectively. Therefore, the first property holds if and only if

$$(u,y) \in \mathfrak{B}(\mathrm{E} \wedge (\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2)) \quad \Longrightarrow \quad \begin{cases} (u_{11}, y_{21}) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1), \\ (y_{12}, u_{22}) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2). \end{cases} \tag{4.72}$$

It is easily seen that the latter holds for all environments E compatible with $\mathcal{C}$ if and only if it holds for the assumptions A. On the other hand, due to Theorem 3.1, the second property holds if and only if

$$(u,y) \in \mathfrak{B}(\mathrm{A} \wedge (\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2)) \quad \Longrightarrow \quad (u,y) \in \mathfrak{B}(\Gamma). \tag{4.73}$$

With the assumption that $\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2$ is well-posed, it follows that $\mathcal{C}$ should satisfy the following implication.

Implication 4.2. *If Σ_1 and Σ_2 implement $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$, respectively, and $\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2$ is well-posed, then the following implication holds:*

$$(u,y) \in \mathfrak{B}(\mathrm{A} \wedge (\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2)) \implies \begin{cases} (u_{11}, y_{21}) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1), \\ (y_{12}, u_{22}) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2), \\ (u,y) \in \mathfrak{B}(\Gamma). \end{cases} \tag{4.74}$$

Remark 4.5. *Analogously to the feedback interconnection of input-output systems, we can define the feedback interconnection of assumptions. This allows us to rewrite* (4.74) *in a more convenient form. In particular, consider the assumptions A_1 and A_2 given by* (4.2)*, and the partition* (4.8)*. Partition the polynomial matrices*

$$A_j(s) = \begin{bmatrix} A_{j1}(s) & A_{j2}(s) \end{bmatrix}, \quad j \in \{1,2\}, \tag{4.75}$$

according to (4.8)*. The* feedback interconnection *of A_1 to A_2, denoted by $\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2$, is obtained by setting $u_{21} = y_{12}$ and $u_{12} = y_{21}$. This results in the system*

$$\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2 : -A_{\mathrm{i}}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = A_{\mathrm{e}}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u, \tag{4.76}$$

where $y = (y_{11}, y_{12}, y_{21}, y_{22})$, $u = (u_{11}, u_{22})$, and

$$A_{\mathrm{i}}(s) = \begin{bmatrix} 0 & 0 & A_{12}(s) & 0 \\ 0 & A_{21}(s) & 0 & 0 \end{bmatrix}, \tag{4.77}$$

$$A_{\mathrm{e}}(s) = \begin{bmatrix} A_{11}(s) & 0 \\ 0 & A_{22}(s) \end{bmatrix}. \tag{4.78}$$

It is easily seen that $(u_{11}, y_{21}) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ *and* $(y_{12}, u_{22}) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ *if and only if* $(u, y) \in \mathfrak{B}(\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2)$. *Therefore,* (4.74) *is equivalent to*

$$\mathfrak{B}(\mathrm{A} \wedge (\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2)) \subset \mathfrak{B}(\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2), \tag{4.79}$$

$$\mathfrak{B}(\mathrm{A} \wedge (\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2)) \subset \mathfrak{B}(\Gamma). \tag{4.80}$$

Note the similarity between the latter and (4.65) *and* (4.66).

Like with Implication 4.1, a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 4.2 does not necessarily exist for arbitrary $\mathcal{C}_1$ and $\mathcal{C}_2$, hence the following definition.

Definition 4.10. The contract $\mathcal{C}_1$ is *feedback composable* to $\mathcal{C}_2$ if there exists a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 4.2.

However, here we have an additional requirement, namely, that $\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2$ is well-posed. This might not hold for any Σ_1 and Σ_2 that implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. This motivates the following definition.

Definition 4.11. The contract $\mathcal{C}_1$ is *feedback compatible* with $\mathcal{C}_2$ if there exist implementation Σ_1 of $\mathcal{C}_1$ and Σ_2 of $\mathcal{C}_2$ such that $\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2$ is well-posed.

Unless $\mathcal{C}_1$ is feedback compatible to $\mathcal{C}_2$, Implication 4.2 is vacuously satisfied for any contract $\mathcal{C} = (\mathrm{A}, \Gamma)$, which renders the feedback composition useless. Therefore, we need to be able to determine if $\mathcal{C}_1$ is feedback compatible $\mathcal{C}_2$ before we attempt to verify feedback composability and obtain the feedback composition. Fortunately, $\mathcal{C}_1$ is guaranteed to be feedback compatible to $\mathcal{C}_2$ if both contracts have output guarantees, which we will assume later in this section. In the meantime, we define the feedback composition as follows.

Definition 4.12. Suppose that $\mathcal{C}_1$ is feedback compatible with and feedback composable to $\mathcal{C}_2$. The *feedback composition* of $\mathcal{C}_1$ to $\mathcal{C}_2$, denoted by $\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2$, is the smallest contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 4.2.

The definition of the feedback composition has the same aspects as the definition of the series composition, namely, it assumes the least and guarantees the most while ensuring the satisfaction of properties that support independent design, as captured by Implication 4.2. The only difference with the series composition is in the requirement that $\mathcal{C}_1$ and $\mathcal{C}_2$ are feedback compatible. Such a requirement was not necessary for the series composition because, unlike the feedback interconnection, the series interconnection is always well-posed.

Note that the feedback interconnection $\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2$ is well-posed if Σ_1 and Σ_2 are autonomous. Furthermore, if Γ_1 and Γ_2 are output guarantees, then, due to Remark 3.8, $\mathcal{C}_1$ and $\mathcal{C}_2$ have autonomous implementations Σ_1 and Σ_2,

respectively. Therefore, $\mathcal{C}_1$ is guaranteed to be feedback compatible to $\mathcal{C}_2$ if Γ_1 and Γ_2 are output guarantees. Motivated by this, for the remainder of this section, we will assume that Γ_1 and Γ_2 are output guarantees. As with the series composition, this will greatly simplify the analysis and will provide us with intuition behind the main ideas. The general case will be treated in the next section.

With this in mind, we now turn to finding tractable conditions on A and Γ under which the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.2. We will do this using autonomous implementations again. Similarly to the series composition, this will lead to necessary conditions. 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 the loop of the feedback interconnection.

We will overcome this problem by heavily utilizing the algebraic characterization of behavioural inclusion in Proposition 3.13. Using autonomous implementations, we will first obtain necessary conditions under which the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.2. Then, we will show that these conditions are also sufficient. We do this in the following lemma, whose proof can be found in Appendix B.4.

Lemma 4.6. *Suppose that Γ_1 and Γ_2 are output guarantees, and consider the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$. Then, the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.2 if and only if*

$$\mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2)) \subset \mathfrak{B}(\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2), \tag{4.81}$$

$$\mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2)) \subset \mathfrak{B}(\Gamma). \tag{4.82}$$

Note the parallel between (4.79) and (4.81), and (4.80) and (4.82). As shown in the sufficiency part of the proof of Lemma 4.6, if (4.81) holds, then the behaviour of $\mathrm{A} \wedge (\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2)$ is determined by that of $\mathrm{A} \wedge (\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2)$, which is useful information about the behaviour of $\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2$. To show this, we made use of the assumption that $\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2$ is well-posed. In other words, requiring well-posedness allowed us to predict the behaviour of $\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2$ based on the fact that Σ_1 and Σ_2 are implementations of $\mathcal{C}_1$ and $\mathcal{C}_2$. More importantly, Lemma 4.6 provides us with tractable conditions for the satisfaction of Implementation 4.2 that depend only on assumptions and guarantees.

Remark 4.6. *As shown in the proof of Lemma 4.6, we have that*

$$\mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2)) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_2) \tag{4.83}$$

when Γ_1 and Γ_2 are output guarantees. Consequently, due to linearity, (4.81) *holds if and only if*

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \times \{0\} \times \{0\} \subset \mathfrak{B}(\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2), \tag{4.84}$$

$$\{0\} \times \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_2) \subset \mathfrak{B}(\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2). \tag{4.85}$$

Let $\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2$ *be defined as in Remark 4.5. Then,* (4.84) *and* (4.85) *hold if and only if* $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{\mathrm{e}})$ *and*

$$\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_2) \subset \mathfrak{B}_{\mathrm{o}}(\mathrm{A}_{\mathrm{i}}), \tag{4.86}$$

respectively, where we have defined

$$\mathrm{A}_{\mathrm{e}} : 0 = A_{\mathrm{e}}\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)u \quad \textit{and} \quad \mathrm{A}_{\mathrm{i}} : -A_{\mathrm{i}}\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y = 0. \tag{4.87}$$

Consider Remark 4.6. Note that (4.86) is independent of $\mathcal{C} = (\mathrm{A}, \Gamma)$. This suggests that (4.86) is a necessary condition for feedback composability. In fact, the following theorem shows that (4.86) is not only necessary but also sufficient for feedback composability. Furthermore, it shows that the feedback composition $\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2$ exists if $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$, and provides an explicit expression for it when it exists.

Theorem 4.2. *Consider the contracts* $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ *and* $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$*. Suppose that* Γ_1 *and* Γ_2 *are output guarantees, such that* $\mathcal{C}_1$ *is feedback compatible with* $\mathcal{C}_2$*. Then,* $\mathcal{C}_1$ *is feedback composable to* $\mathcal{C}_2$ *if and only if*

$$\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_2) \subset \mathfrak{B}_{\mathrm{o}}(\mathrm{A}_{\mathrm{i}}), \tag{4.88}$$

where A_{i} *is defined as in Remark 4.6. Furthermore, if* $\mathcal{C}_1$ *is feedback composable to* $\mathcal{C}_2$*, then the feedback composition of* $\mathcal{C}_1$ *to* $\mathcal{C}_2$ *exists and is given by*

$$\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2 = (\mathrm{A}_e, \Gamma_1 \leftarrow\!\!\shortmid \Gamma_2). \tag{4.89}$$

where A_{e} *is defined as in Remark 4.6.*

Proof. In view of Remark 4.6, Lemma 4.6 already shows that $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$ only if (4.88) holds. To show the converse, suppose that (4.88) holds. We will show that a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.2 if and only if it is refined by the contract $\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2$ given by (4.89). To this end, due to Lemma 4.6, $\mathcal{C}$ satisfies Implication 4.2 if and only if (4.81) and (4.82) hold. Note that $\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2$ are output guarantees because Γ_1 and Γ_2 are output guarantees. Due to Remark 3.8, this implies that $\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2$ is consistent. Furthermore, in view of Remark 4.6 and the assumption that (4.88) holds, (4.81) holds if and only if $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{\mathrm{e}})$. Consequently, due to Theorem 3.3, (4.81) and (4.82) hold if and only if $\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2$ refines $\mathcal{C}$. Since $\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2$ refines itself, this shows that $\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2$ is the smallest contract that satisfies Implication 4.2. Therefore, $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$, and the contract $\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2$ given by (4.89) is indeed the feedback composition of $\mathcal{C}_1$ to $\mathcal{C}_2$. □

The intuition behind (4.88) is similar to the one behind (4.55) given after Theorem 4.1. To see this, note that, by definition of A_{i}, (4.88) holds if and only if $y_1 \in \mathfrak{B}_{\mathrm{o}}(\Gamma_1)$ and $y_2 \in \mathfrak{B}_{\mathrm{o}}(\Gamma_2)$ imply $(0, y_{12}) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ and $(y_{21}, 0) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$.

In particular, this means that the second part of any output that an implementation of $\mathcal{C}_1$ can generate must be the first part of an input that an environment compatible with $\mathcal{C}_2$ can generate when the second part of the input is restricted to zero. Like that of (4.55), the necessity of (4.88) is somewhat surprising. Indeed, we generally expect the choice of assumptions A to restrict the output behaviour of Σ_1 and Σ_2 in $\mathrm{A} \wedge (\Sigma_1 \leftarrow\!\!\rightarrow \Sigma_2)$ and, thus, to relax the requirement expressed by (4.88). This does not happen because we consider contracts with output guarantees, which have autonomous implementations that decouple the behaviour of the output from the behaviour of the input.

Remark 4.7. *As mentioned in Remark 4.2, if u_{12}, y_{11}, u_{22} and y_{21} are void in* (4.8)*, then the series interconnection reduces to the feedback interconnection. Consequently, Implication 4.2 reduces to Implication 4.1, which means that the feedback composition reduces to the series composition. In particular, Theorem 4.1 reduces to Theorem 4.2. Indeed, note that*

$$A_{\mathrm{i}}(s) = \begin{bmatrix} 0 & 0 \\ A_2(s) & 0 \end{bmatrix}, \tag{4.90}$$

hence (4.88) *holds if and only if* (4.55) *holds. On the other hand,*

$$A_e(s) = \begin{bmatrix} A_1(s) \\ 0 \end{bmatrix} \tag{4.91}$$

hence $\mathrm{A_e} = \mathrm{A_1}$ *and, thus,* (4.89) *reduces to* (4.56)*. This suggests that we can obtain results on the series composition from results on the feedback composition.*

4.4 Feedback composition

In this section, we will treat the general case for the feedback composition. To begin with, we will find necessary and sufficient conditions for feedback compatibility. We will see that these conditions are difficult to verify in general, but also that there is a promising strategy based on our results on contract consistency. Then, assuming feedback compatibility, we will find necessary and sufficient conditions for feedback composability. We will also show that feedback composability implies that the feedback composition exists, and we will provide an explicit expression for it when it exists.

As explained in the last section, we need to be able to verify that $\mathcal{C}_1$ is feedback compatible with $\mathcal{C}_2$ before we consider the feedback composition. Recall that $\mathcal{C}_1$ is feedback compatible with $\mathcal{C}_2$ if there exist implementations Σ_1 and Σ_2 of $\mathcal{C}_1$ and $\mathcal{C}_2$ such that $\Sigma_1 \leftarrow\!\!\rightarrow \Sigma_2$ is well-posed, which is the case only if $\mathcal{C}_1$ and $\mathcal{C}_2$ are consistent. With this in mind, throughout this section, we will assume that $\mathcal{C}_1$ and $\mathcal{C}_2$ are consistent and row-reduced. Because of Lemma 3.18, the additional assumption that $\mathcal{C}_1$ and $\mathcal{C}_2$ are row-reduced is not restrictive.

We can show that feedback compatibility is related to the well-posedness of the feedback interconnection of guarantees. In particular, the following lemma shows that $\mathcal{C}_1$ is feedback compatible to $\mathcal{C}_2$ if and only if there exist guarantees Γ_1' and Γ_2' such that the contracts $\mathcal{C}_1' = (\mathrm{A}_1, \Gamma_1')$ and $\mathcal{C}_2' = (\mathrm{A}_2, \Gamma_2')$ are equivalent to $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and $\Gamma_1' \leftarrow \Gamma_2'$ is well-posed.

Lemma 4.7. *Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ given by* (4.2) *are consistent and row-reduced. Then, $\mathcal{C}_1$ is feedback compatible with $\mathcal{C}_2$ if and only if there exist polynomial matrices $M_1(s)$ and $M_2(s)$ for which the guarantees*

$$\Gamma_j' : G_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) y_j = \big(H_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) - M_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) A_j\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)\big)\, u_j, \quad j \in \{1, 2\}, \tag{4.92}$$

are such that $\Gamma_1' \leftarrow \Gamma_2'$ is well-posed.

Proof. We begin by proving necessity. Suppose that $\mathcal{C}_1$ is feedback compatible with $\mathcal{C}_2$. This implies that there exist implementations Σ_1 and Σ_2 of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, such that $\Sigma_1 \leftarrow \Sigma_2$ is well-posed. Then, for each $j \in \{1, 2\}$, we have that $\mathfrak{B}(\mathrm{A}_j \wedge \Sigma_j) \subset \mathfrak{B}(\Gamma_j)$, which holds if and only if there exist polynomial matrices $T_j(s)$ and $M_j(s)$ such that

$$\begin{bmatrix} G_j(s) & -H_j(s) \end{bmatrix} = \begin{bmatrix} T_j(s) & M_j(s) \end{bmatrix} \begin{bmatrix} P_j(s) & -Q_j(s) \\ 0 & -A_j(s) \end{bmatrix}. \tag{4.93}$$

We can rewrite the latter to obtain

$$\begin{bmatrix} G_j(s) & -H_j(s) + M_j(s)A_j(s) \end{bmatrix} = T_j(s) \begin{bmatrix} P_j(s) & -Q_j(s) \end{bmatrix}, \tag{4.94}$$

which shows that $\mathfrak{B}(\Sigma_j) \subset \mathfrak{B}(\Gamma_j')$, where Γ_j' is defined as in (4.92). Therefore, the Σ_1 and Σ_2 are such that $\mathfrak{B}(\Sigma_1) \subset \mathfrak{B}(\Gamma_1')$, $\mathfrak{B}(\Sigma_2) \subset \mathfrak{B}(\Gamma_2')$, and $\Sigma_1 \leftarrow \Sigma_2$ is well-posed, hence $\Gamma_1' \leftarrow \Gamma_2'$ is well-posed by definition.

We proceed by proving sufficiency. Suppose that there exist polynomial matrices $M_1(s)$ and $M_2(s)$ for which the guarantees Γ_1' and Γ_2' defined in (4.92) are such that $\Gamma_1' \leftarrow \Gamma_2'$ is well-posed. This means that there exist input-output systems Σ_1 and Σ_2 such that $\mathfrak{B}(\Sigma_1) \subset \mathfrak{B}(\Gamma_1')$, $\mathfrak{B}(\Sigma_2) \subset \mathfrak{B}(\Gamma_2')$, and the feedback interconnection $\Sigma_1 \leftarrow \Sigma_2$ is well-posed. For each $j \in \{1, 2\}$, we have that $\mathfrak{B}(\Sigma_j) \subset \mathfrak{B}(\Gamma_j')$ implies that there exists a polynomial matrix $T_j(s)$ such that (4.94) holds. Consequently, (4.93) holds, hence $\mathfrak{B}(\mathrm{A}_j \wedge \Sigma_j) \subset \mathfrak{B}(\Gamma_j)$. This means that Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and are such that $\Sigma_1 \leftarrow \Sigma_2$ is well-posed, hence $\mathcal{C}_1$ is feedback compatible with $\mathcal{C}_2$. □

To use Lemma 4.7, we need to be able to verify the existence of and to construct polynomial matrices $M_1(s)$ and $M_2(s)$ for which the guarantees in (4.92) are such that $\Gamma_1' \leftarrow \Gamma_2'$ is well-posed. It is not clear if we can do this in general. However, using Proposition 4.2, we can obtain a sufficient condition on $M_1(s)$ and $M_2(s)$ under which $\Gamma_1' \leftarrow \Gamma_2'$ is well-posed that allows us to suggest promising candidates for $M_1(s)$ and $M_2(s)$. In particular, we have the following lemma, whose proof can be found in Appendix B.5.

Lemma 4.8. *Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ given by* (4.2) *are consistent and row-reduced. Consider the partitions in* (4.75) *and* (4.26)*, and let $D_1(s)$ and $D_2(s)$ be the row-degree matrices of $G_1(s)$ and $G_2(s)$, respectively. Then, the guarantees Γ_1' and Γ_2' given by* (4.92) *are such that $\Gamma_1' \hookleftarrow \Gamma_2'$ is well-posed if the rational matrices*

$$\begin{aligned} &D_1(s)^{-1}\left(H_1(s) - M_1(s)A_1(s)\right), \\ &D_2(s)^{-1}\left(H_2(s) - M_2(s)A_2(s)\right), \end{aligned} \tag{4.95}$$

are proper, and at least one of the following conditions hold:

1. *$D_1(s)^{-1}(H_{12}(s) - M_1(s)A_{12}(s))$ is strictly proper;*
2. *$D_2(s)^{-1}(H_{21}(s) - M_2(s)A_{21}(s))$ is strictly proper.*

In view of Lemma 3.19, there exist polynomial matrices $M_1(s)$ and $M_2(s)$ such that (4.95) is proper if and only if $\mathcal{C}_1$ and $\mathcal{C}_2$ are consistent. Furthermore, from Lemma 3.20 and the proof of Theorem 3.2, we know how to find polynomial matrices $M_1(s)$ and $M_2(s)$ that minimize the row degrees of $H_1(s) - M_1(s)A_1(s)$ and $H_2(s) - M_2(s)A_2(s)$. As such, the latter are good candidates for polynomial matrices $M_1(s)$ and $M_2(s)$ that satisfy at least one of the conditions in Lemma 4.8.

Note that the guarantees Γ_1' and Γ_2' in Lemma 4.7 are such that

$$\mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1) = \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1') \quad \text{and} \quad \mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_2) = \mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_2'), \tag{4.96}$$

hence, due to Corollary 3.21, the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1')$ and $\mathcal{C}_2' = (\mathrm{A}_2, \Gamma_2')$ are equivalent to $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. This means that we can replace $\mathcal{C}_1$ and $\mathcal{C}_2$ by $\mathcal{C}_1'$ and $\mathcal{C}_2'$, respectively, without affecting feedback compatibility, feedback composability, or the feedback composition. Motivated by this, for the remainder of this section, we will assume that $\Gamma_1 \hookleftarrow \Gamma_2$ is well-posed. This will guarantee that $\mathcal{C}_1$ is feedback compatible with $\mathcal{C}_2$, which will allow us to focus on feedback composability. Furthermore, by definition, it will guarantee that $\mathcal{C}_1$ and $\mathcal{C}_2$ are consistent. With this in mind, the following lemma, whose proof can be found in Appendix B.6, generalizes Lemma 4.6.

Lemma 4.9. *Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are row-reduced and $\Gamma_1 \hookleftarrow \Gamma_2$ is well-posed. Then, the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.2 if and only if*

$$\mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \hookleftarrow \Gamma_2)) \subset \mathfrak{B}(\mathrm{A}_1 \hookleftarrow \mathrm{A}_2), \tag{4.97}$$

$$\mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \hookleftarrow \Gamma_2)) \subset \mathfrak{B}(\Gamma). \tag{4.98}$$

In particular, Lemma 4.9 provides us with tractable conditions under which a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.2. These conditions depend only on assumptions and guarantees, which will ultimately allow us to obtain tractable conditions for feedback composability. Before we do that, we state the following lemma, whose proof can be found in Appendix B.7.

Lemma 4.10. *Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are row-reduced, $\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2$ is well-posed, and* (4.97) *holds. Then*

$$\mathfrak{B}(\mathrm{A} \wedge (\Sigma_1 \leftarrow\!\!\rightarrow \Sigma_2)) \subset \mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2)) \tag{4.99}$$

for all implementations Σ_1 and Σ_2 of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, such that $\Sigma_1 \leftarrow\!\!\rightarrow \Sigma_2$ is well-posed.

Lemma 4.10 is used in the proof of Lemma 4.9 and will be used again in the proof of Theorem 4.3 at the end of this section. It tells us that the behaviour of $\mathrm{A} \wedge (\Sigma_1 \leftarrow\!\!\rightarrow \Sigma_2)$ is determined by the behaviour of $\mathrm{A} \wedge (\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2)$ when (4.97) holds. As mentioned in the last section, predicting the behaviour of $\Sigma_1 \leftarrow\!\!\rightarrow \Sigma_2$ in this way is only possible because $\Sigma_1 \leftarrow\!\!\rightarrow \Sigma_2$ is required to be well-posed.

Recall Remark 4.6, where we showed that the condition (4.81) in Lemma 4.6 is partially independent of $\mathcal{C}$. Similarly, with a bit more effort, we can show that the condition (4.97) in Lemma 4.9 is partially independent of $\mathcal{C}$. This is done in the following lemma.

Lemma 4.11. *The condition* (4.97) *in Lemma 4.9 holds if and only if*

$$(0, y) \in \mathfrak{B}(\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2) \quad \Longrightarrow \quad (0, y) \in \mathfrak{B}(\mathrm{A}_1 \leftarrow\!\!\rightarrow \mathrm{A}_2), \tag{4.100}$$

and

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}((\mathrm{A}_1 \leftarrow\!\!\rightarrow \mathrm{A}_2) \wedge (\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2)). \tag{4.101}$$

Proof. We begin by proving necessity. Suppose that (4.97) holds. Suppose that $(0, y) \in \mathfrak{B}(\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2)$. Since $0 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$, we obtain $(0, y) \in \mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2))$, hence $(0, y) \in \mathfrak{B}(\mathrm{A}_1 \leftarrow\!\!\rightarrow \mathrm{A}_2)$ due to (4.97), and, thus, (4.100) holds. On the other hand, let $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$. Since $\mathcal{C}_1$ and $\mathcal{C}_2$ are row-reduced, and $\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2$ is well-posed, due to Remark 4.1, there exists y such that $(u, y) \in \mathfrak{B}(\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2)$. This implies that $(u, y) \in \mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2))$, hence $(u, y) \in \mathfrak{B}(\mathrm{A}_1 \leftarrow\!\!\rightarrow \mathrm{A}_2)$ due to (4.97), and, thus,

$$(u, y) \in \mathfrak{B}((\mathrm{A}_1 \leftarrow\!\!\rightarrow \mathrm{A}_2) \wedge (\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2)). \tag{4.102}$$

Recall that the input behaviour of a system that involves both u and y is given by projecting the external behaviour onto u. Therefore, we obtain

$$u \in \mathfrak{B}_{\mathrm{i}}((\mathrm{A}_1 \leftarrow\!\!\rightarrow \mathrm{A}_2) \wedge (\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2)), \tag{4.103}$$

which shows that (4.101) holds.

We proceed by proving sufficiency. Suppose that (4.100) and (4.101) hold. Let $(u, y) \in \mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2))$. Then, $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$ and, due to (4.101), we obtain

$$u \in \mathfrak{B}_{\mathrm{i}}((\mathrm{A}_1 \leftarrow\!\!\rightarrow \mathrm{A}_2) \wedge (\Gamma_1 \leftarrow\!\!\rightarrow \Gamma_2)). \tag{4.104}$$

This implies that there exists y' such that

$$(u, y') \in \mathfrak{B}((\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2) \wedge (\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2)), \tag{4.105}$$

and, thus, $(u, y') \in \mathfrak{B}(\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2)$ and $(u, y') \in \mathfrak{B}(\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2)$. However, we also have that $(u, y) \in \mathfrak{B}(\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2)$, hence $(0, y - y') \in \mathfrak{B}(\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2)$. Then, (4.100) implies that $(0, y - y') \in \mathfrak{B}(\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2)$, hence $(u, y) \in \mathfrak{B}(\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2)$, which shows that (4.97) holds. □

Note that (4.100) is independent of $\mathcal{C}$, hence it is a necessary condition for $\mathcal{C}_1$ to be feedback composable to $\mathcal{C}_2$. It turns out that this condition is also sufficient. We show this in the following theorem, where we also show that the feedback composition $\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2$ exists if $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$, and we provide an explicit expression for it when it exists.

Theorem 4.3. *Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are row-reduced, and $\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2$ is well-posed, such that $\mathcal{C}_1$ is feedback compatible with $\mathcal{C}_2$. Then, $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$ if and only if*

$$(0, y) \in \mathfrak{B}(\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2) \quad \Longrightarrow \quad (0, y) \in \mathfrak{B}(\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2). \tag{4.106}$$

Furthermore, if $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$, then the the feedback composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ exist and is given by

$$\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2 = (\mathrm{A}_{12}, \Gamma_1 \leftarrow\!\!\shortmid \Gamma_2), \tag{4.107}$$

where A_{12} is such that

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{12}) = \mathfrak{B}_{\mathrm{i}}((\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2) \wedge (\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2)), \tag{4.108}$$

that is, A_{12} is obtained after eliminating y from $(\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2) \wedge (\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2)$.

Proof. First, recall that $\mathcal{C}_1$ is feedback compatible with $\mathcal{C}_2$ due to Lemma 4.7 and the assumption that $\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2$ is well-posed. On the other hand, due to Lemma 4.9 and Lemma 4.11, we know that $\mathcal{C}_1$ and $\mathcal{C}_2$ are feedback composable only if (4.106) holds. To show the converse, suppose that (4.106) holds. We will show that a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.2 if and only if it is refined by the contract $\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2$ given by (4.107). To do this, we will make use of Theorem 3.3, which requires us to show that $\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2$ is consistent.

With this in mind, since (4.106) holds, due to Lemma 4.11 and the definition of A_{12}, it follows that

$$\mathfrak{B}(\mathrm{A}_{12} \wedge (\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2)) \subset \mathfrak{B}(\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2). \tag{4.109}$$

Then, Lemma 4.10 implies that

$$\mathfrak{B}(\mathrm{A}_{12} \wedge (\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2)) \subset \mathfrak{B}(\mathrm{A}_{12} \wedge (\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2)) \subset \mathfrak{B}(\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2), \tag{4.110}$$

for all implementations Σ_1 and Σ_2 of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, whose interconnection $\Sigma_1 \leftarrow \Sigma_2$ is well-posed. Since $\Gamma_1 \leftarrow \Gamma_2$ is well-posed, such implementations exists, and (4.110) shows that $\Sigma_1 \leftarrow \Sigma_2$ implements $\mathcal{C}_1 \leftarrow \mathcal{C}_2$, hence $\mathcal{C}_1 \leftarrow \mathcal{C}_2$ is consistent.

Now, due to Lemma 4.9, $\mathcal{C}$ satisfies Implication 4.2 if and only if (4.97) and (4.98) hold. In view of Lemma 4.11 and the assumption that (4.106) holds, (4.97) holds if and only if $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{12})$, where we used (4.108). Then, since $\mathcal{C}_1 \leftarrow \mathcal{C}_2$ is consistent, Theorem 3.3 tells us that $\mathcal{C}_1 \leftarrow \mathcal{C}_2$ refines $\mathcal{C}$ if and only if $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{12})$ and (4.98). In other words, $\mathcal{C}$ satisfies Implication 4.2 if and only if it is refined by $\mathcal{C}_1 \leftarrow \mathcal{C}_2$. Since $\mathcal{C}_1 \leftarrow \mathcal{C}_2$ refines itself, this shows that $\mathcal{C}_1 \leftarrow \mathcal{C}_2$ is the smallest contract that satisfies Implication 4.2. Therefore, $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$, and the contract $\mathcal{C}_1 \leftarrow \mathcal{C}_2$ given by (4.106) is indeed the feedback composition of $\mathcal{C}_1$ to $\mathcal{C}_2$. □

The intuition behind (4.106) is similar to the one behind (4.88). However, since we are no longer considering contracts with output guarantees, the choice of assumptions A does restrict the output behaviour of Σ_1 and Σ_2 in the interconnection $\mathrm{A} \wedge (\Sigma_1 \leftarrow \Sigma_2)$ and, thus, relaxes the requirement expressed by (4.88). In particular, (4.106) represents the requirement that (4.97) holds for the most restrictive assumptions A, namely, the ones such that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) = \{0\}$. Given that this requirement is satisfied, the assumptions A_{12} in Theorem 4.3 are the least restrictive assumptions that still ensure that (4.97) holds, see Lemma 4.11. The intuition behind the condition for composability and the difference when considering contracts with output guarantees is clearer for the series composition, which will be treated in the next section.

Note that (4.106) is a behavioural inclusion condition, which can be verified algorithmically. Furthermore, the assumptions and guarantees of the feedback composition in (4.107) can be obtained algorithmically from the assumptions and guarantees of the contracts that are composed. Therefore, Theorem 4.3 allows us to algorithmically verify feedback composability and compute the feedback composition.

Theorem 4.3 shows that the feedback composition $\mathcal{C}_1 \leftarrow \mathcal{C}_2$ exists when $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$. At first sight, it might seem that this is the case only when $\mathcal{C}_1$ and $\mathcal{C}_2$ are row-reduced, and $\Gamma_1 \leftarrow \Gamma_2$ is well-posed. This is not true and we obtain the following corollary of Theorem 4.3.

Corollary 4.12. *Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are such that $\mathcal{C}_1$ is feedback compatible with $\mathcal{C}_2$. If $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$, then the feedback composition $\mathcal{C}_1 \leftarrow \mathcal{C}_2$ exists.*

Proof. Recall that, by definition, $\mathcal{C}_1$ being feedback compatible with $\mathcal{C}_2$ implies that $\mathcal{C}_1$ and $\mathcal{C}_2$ are consistent. Consequently, due to Lemma 3.18, $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent to some consistent and row-reduced contracts $\mathcal{C}_1' = (\mathrm{A}_1', \Gamma_1')$ and $\mathcal{C}_2' = (\mathrm{A}_2', \Gamma_2')$, respectively. Since $\mathcal{C}_1$ is feedback compatible with $\mathcal{C}_2$, it follows that $\mathcal{C}_1'$ is feedback compatible with $\mathcal{C}_2'$. Then, due to Lemma 4.7, $\mathcal{C}_1'$ and $\mathcal{C}_2'$ are

equivalent to some row-reduced contracts $\mathcal{C}_1'' = (\mathrm{A}_1', \Gamma_1'')$ and $\mathcal{C}_2 = (\mathrm{A}_2', \Gamma_2'')$, where $\Gamma_1'' \leftarrow \Gamma_2''$ is well-posed. This means that $\mathcal{C}_1$ and $\mathcal{C}_2$ are also equivalent to $\mathcal{C}_1''$ and $\mathcal{C}_2''$, respectively. Therefore, by definition of feedback composability and the feedback composition, $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$ if and only if $\mathcal{C}_1''$ is feedback composable to $\mathcal{C}_2''$ and $\mathcal{C}_1 \leftarrow \mathcal{C}_2 = \mathcal{C}_1'' \leftarrow \mathcal{C}_2''$. Consequently, if $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$, then $\mathcal{C}_1''$ is feedback composable to $\mathcal{C}_2''$, hence, due to Theorem 4.3, $\mathcal{C}_1'' \leftarrow \mathcal{C}_2''$ exists and, thus, $\mathcal{C}_1 \leftarrow \mathcal{C}_2$ exists. □

Although we know that the feedback composition $\mathcal{C}_1 \leftarrow \mathcal{C}_2$ exists if $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$, we cannot verify the latter or obtain an expression for $\mathcal{C}_1 \leftarrow \mathcal{C}_2$ directly from $\mathcal{C}_1$ and $\mathcal{C}_2$. To do that, we need to obtain the contracts $\mathcal{C}_1''$ and $\mathcal{C}_2''$ from the proof of Corollary 4.12, which requires us to first obtain the contracts $\mathcal{C}_1'$ and $\mathcal{C}_2'$. Nevertheless, we note that

$$(\mathrm{A}_1 \leftarrow \mathrm{A}_2) \wedge (\Gamma_1 \leftarrow \Gamma_2) = (\mathrm{A}_1 \wedge \Gamma_1) \leftarrow (\mathrm{A}_2 \wedge \Gamma_2). \tag{4.111}$$

Due to Proposition 4.3 and Corollary 3.21, this implies that

$$\mathfrak{B}((\mathrm{A}_1 \leftarrow \mathrm{A}_2) \wedge (\Gamma_1 \leftarrow \Gamma_2)) = \mathfrak{B}((\mathrm{A}_1' \leftarrow \mathrm{A}_2') \wedge (\Gamma_1'' \leftarrow \Gamma_2'')), \tag{4.112}$$

if the contracts $\mathcal{C}_1'' = (\mathrm{A}_1', \Gamma_1'')$ and $\mathcal{C}_2 = (\mathrm{A}_2', \Gamma_2'')$ are equivalent to $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Therefore, the assumptions of $\mathcal{C}_1 \leftarrow \mathcal{C}_2$ can be obtained directly from $\mathcal{C}_1$ and $\mathcal{C}_2$.

We conclude this section by showing that the feedback composition satisfies the independent refinement property discussed in Chapter 2.

Theorem 4.4. *Consider the contracts $\mathcal{C}_1'$, $\mathcal{C}_2'$, $\mathcal{C}_1$ and $\mathcal{C}_2$. Suppose that $\mathcal{C}_1'$ refines $\mathcal{C}_1$ and $\mathcal{C}_2'$ refines $\mathcal{C}_2$. Then, $\mathcal{C}_1'$ is feedback compatible with $\mathcal{C}_2'$ only if $\mathcal{C}_1$ is feedback compatible with $\mathcal{C}_2$. Furthermore, if $\mathcal{C}_1'$ is feedback compatible with $\mathcal{C}_2'$, then $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$ only if $\mathcal{C}_1'$ is feedback composable to $\mathcal{C}_2'$, and $\mathcal{C}_1' \leftarrow \mathcal{C}_2'$ refines $\mathcal{C}_1 \leftarrow \mathcal{C}_2$.*

Proof. We begin by proving the first statement. Suppose that $\mathcal{C}_1'$ is feedback compatible with $\mathcal{C}_2'$. In other words, there exist implementations Σ_1 and Σ_2 of $\mathcal{C}_1'$ and $\mathcal{C}_2'$, respectively, such that $\Sigma_1 \leftarrow \Sigma_2$ is well-posed. Since $\mathcal{C}_1'$ refines $\mathcal{C}_1$ and $\mathcal{C}_2'$ refines $\mathcal{C}_2$, it follows that Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, hence $\mathcal{C}_1$ is feedback compatible with $\mathcal{C}_2$.

We proceed by proving the second statement. Suppose that $\mathcal{C}_1'$ is feedback compatible with $\mathcal{C}_2'$, and $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$. Let $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$, $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$, $\mathcal{C}_1' = (\mathrm{A}_1', \Gamma_1')$ and $\mathcal{C}_2 = (\mathrm{A}_2', \Gamma_2')$. By definition, $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$ if and only if there exists a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 4.2. On the other hand, $\mathcal{C}_1'$ is feedback composable to $\mathcal{C}_2'$ if and only if there exists a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 4.2 with $\mathcal{C}_1$ and $\mathcal{C}_2$ replaced by $\mathcal{C}_1'$ and $\mathcal{C}_2'$, respectively.

With this in mind, suppose that $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.2. Note that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1')$ and $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2')$ because $\mathcal{C}_1'$ refines $\mathcal{C}_1$ and $\mathcal{C}_2'$

refines $\mathcal{C}_2$. Moreover, by definition of $\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2$, $(u, y) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2)$ if and only if $(u_{11}, y_{21}) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ and $(y_{12}, u_{22}) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$. This implies that

$$\mathfrak{B}(\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2) \subset \mathfrak{B}(\mathrm{A}_1' \leftarrow\!\!\shortmid \mathrm{A}_2'). \tag{4.113}$$

Now, suppose that Σ_1 and Σ_2 implement $\mathcal{C}_1'$ and $\mathcal{C}_2'$, respectively, and $\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2$ is well-posed. Then, Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, hence (4.74) in Implication 4.2 holds. In view of (4.113), (4.74) holds with $\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2$ replaced by $\mathrm{A}_1' \leftarrow\!\!\shortmid \mathrm{A}_2'$, hence $\mathcal{C}$ satisfies Implication 4.2 with $\mathcal{C}_1$ and $\mathcal{C}_2$ replaced by $\mathcal{C}_1'$ and $\mathcal{C}_2'$. In other words, if $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.2, then it satisfies it with $\mathcal{C}_1$ and $\mathcal{C}_2$ replaced by $\mathcal{C}_1'$ and $\mathcal{C}_2'$, respectively. Consequently, since $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$, it follows that $\mathcal{C}_1'$ is feedback composable to $\mathcal{C}_2'$. Furthermore, due to Corollary 4.12, both $\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2$ and $\mathcal{C}_1' \leftarrow\!\!\shortmid \mathcal{C}_2'$ exist. Since $\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2$ satisfies Implication 4.2, it also satisfies it with $\mathcal{C}_1$ and $\mathcal{C}_2$ replaced by $\mathcal{C}_1'$ and $\mathcal{C}_2'$, respectively. As $\mathcal{C}_1' \leftarrow\!\!\shortmid \mathcal{C}_2'$ is the smallest such contract, it follows that $\mathcal{C}_1' \leftarrow\!\!\shortmid \mathcal{C}_2'$ refines $\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2$. □

4.5 Series composition

In this section, we will treat the general case for the series composition of two contracts. In particular, by treating the series interconnection as a special case of the feedback interconnection, we will obtain results on series composability and the series composition from our results on feedback composability and the feedback composition. Note that we already did this in Remark 4.7 for the special case where both contracts have output guarantees.

As explained in Remark 4.2, if u_{12}, y_{11}, u_{22} and y_{21} in (4.8) are void, then the series interconnection reduces to the feedback interconnection, that is,

$$\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2 = \Sigma_1 \to \Sigma_2, \tag{4.114}$$

$$\mathrm{A}_1 \leftarrow\!\!\shortmid \mathrm{A}_2 = \mathrm{A}_1 \to \mathrm{A}_2, \tag{4.115}$$

$$\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2 = \Gamma_1 \to \Gamma_2. \tag{4.116}$$

Since the series interconnection $\Sigma_1 \to \Sigma_2$ is always well-posed, it follows that $\mathcal{C}_1$ is feedback compatible with $\mathcal{C}_2$ if and only if $\mathcal{C}_1$ and $\mathcal{C}_2$ are consistent. On the other hand, Implication 4.2 reduces to Implication 4.1. This implies that $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$ if and only if $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_2$. Furthermore, the series composition $\mathcal{C}_1 \to \mathcal{C}_2$ exists if and only if the feedback composition $\mathcal{C}_1 \leftarrow\!\!\shortmid \mathcal{C}_2$ exists, and they are equal to each other. Therefore, we can use Theorem 4.3 to obtain the following theorem regarding series composability and the series composition. The proof can be found in Appendix B.8

Theorem 4.5. *Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are consistent. Then, $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$ if and only if*

$$(0, y_1) \in \mathfrak{B}(\Gamma_1) \quad \Longrightarrow \quad y_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2), \tag{4.117}$$

Furthermore, if $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$, then the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ exist and is given by

$$\mathcal{C}_1 \to \mathcal{C}_2 = (\mathrm{A}_{12}, \Gamma_1 \to \Gamma_2), \tag{4.118}$$

where A_{12} is such that

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{12}) = \mathfrak{B}_{\mathrm{i}}((\mathrm{A}_1 \to \mathrm{A}_2) \wedge (\Gamma_1 \to \Gamma_2)), \tag{4.119}$$

that is, A_{12} is obtained by eliminating y from $(\mathrm{A}_1 \to \mathrm{A}_2) \wedge (\Gamma_1 \to \Gamma_2)$.

Remark 4.8. *The difficulty in the proof of Theorem 4.5 comes from the assumptions in Theorem 4.3. Given that the feedback interconnection reduces to the series interconnection, in order to use Theorem 4.3, we need $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ to be consistent, row-reduced and such that $\Gamma_1 \to \Gamma_2$ is well-posed, which is not necessarily the case. To overcome this, in the proof of Theorem 4.5, we showed that, since they are consistent, $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent to some contracts $\mathcal{C}_1' = (\mathrm{A}_1, \Gamma_1')$ and $\mathcal{C}_2' = (\mathrm{A}_2, \Gamma_2')$, respectively, that are consistent, row-reduced and such that $\Gamma_1' \to \Gamma_2'$ is well-posed. This allowed us to use Theorem 4.3 to obtain results expressed in terms of $\mathcal{C}_1'$ and $\mathcal{C}_2'$. However, we then had to express these results in terms of $\mathcal{C}_1$ and $\mathcal{C}_2$, which, although possible, required some effort.*

This might suggest that we can relax the assumptions in Theorem 4.3 to only require that $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ is feedback compatible with $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$. Indeed, due to Lemma 3.18 and Lemma 4.7, this would imply that there exist equivalent contracts $\mathcal{C}_1' = (\mathrm{A}_1', \Gamma_1')$ and $\mathcal{C}_2 = (\mathrm{A}_1', \Gamma_1')$ that are consistent, row-reduced, and such that $\Gamma_1' \hookleftarrow \Gamma_2'$ is well-posed. Then, we would be able to use Theorem 4.3 to obtain results expressed in terms of $\mathcal{C}_1'$ and $\mathcal{C}_2'$. However, these results would not be expressible in terms of $\mathcal{C}_1$ and $\mathcal{C}_2$. The main reason is that (4.106) *is not equivalent to* (4.106) *with $\mathcal{C}_1$ and $\mathcal{C}_2$ replaced by $\mathcal{C}_1'$ and $\mathcal{C}_2'$.*

Recall the interpretation of (4.55) discussed after Theorem 4.1. In particular, recall that, if Γ_1 and Γ_2 are output guarantees, then $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$ if and only if any output that an implementation of $\mathcal{C}_1$ can generate is an input that an environment compatible with $\mathcal{C}_2$ can generate. This is not required in the general case. Indeed, (4.117) says that $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$ if and only if any output that an implementation of $\mathcal{C}_1$ can generate *for zero input* is an input that an environment compatible with $\mathcal{C}_2$ can generate. In other words, (4.117) captures the requirement that the second part of Implication 4.1 holds for the most restrictive assumptions A, namely, the ones such that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) = \{0\}$.

Note that (4.117) is sufficient for series composability because, in the worst case scenario, we can choose A to be such that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) = \{0\}$. However, we

can typically do better. Indeed, Theorem 4.5 tells us that we can choose A to be such that

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) = \mathfrak{B}_{\mathrm{i}}((\mathrm{A}_1 \to \mathrm{A}_2) \wedge (\Gamma_1 \to \Gamma_2)). \tag{4.120}$$

We can interpret this as follows. Note that $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$ if and only if there exists y such that $(u, y) \in \mathfrak{B}(\mathrm{A}_1 \to \mathrm{A}_2)$ and $(u, y) \in \mathfrak{B}(\Gamma_1 \to \Gamma_2)$. By definition of $\mathrm{A}_1 \to \mathrm{A}_2$ and $\Gamma_1 \to \Gamma_2$, the latter holds if and only if there exist y_1 and y_2 such that $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$, $y_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$, $(u, y_1) \in \mathfrak{B}(\Gamma_1)$ and $(y_1, y_2) \in \mathfrak{B}(\Gamma_2)$. Since $\mathcal{C}_2$ is consistent, it follows that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\Gamma_1)$, hence, for all $y_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$, there exists y_2 such that $(y_1, y_2) \in \mathfrak{B}(\Gamma_2)$. In particular, this implies that $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$ if and only if there exists y_1 such that $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$, $(u, y_1) \in \mathfrak{B}(\Gamma_1)$ and $y_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$. Therefore, $\mathfrak{B}_{\mathrm{i}}(\mathrm{A})$ consists of all inputs in $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ for which the corresponding output generated by Σ_1 is guaranteed to be contained in $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$. Clearly, this implies that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ if $\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$, hence we obtain the following corollary of Theorem 4.5.

Corollary 4.13. *Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are consistent, and $\mathfrak{B}_{\mathrm{o}}(\Gamma_1) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$. Then, $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$, and*

$$\mathcal{C}_1 \to \mathcal{C}_2 = (\mathrm{A}_1, \Gamma_1 \to \Gamma_2). \tag{4.121}$$

We conclude this section by showing that, like the feedback composition, the series composition satisfies the independent refinement property, described in Chapter 2. Note that this immediately follows from Theorem 4.4 because the series composition can be seen as a special case of the feedback composition, and in this case, feedback compatibility is guaranteed if the contracts are consistent.

Theorem 4.6. *Consider the consistent contracts $\mathcal{C}_1'$, $\mathcal{C}_2'$, $\mathcal{C}_1$ and $\mathcal{C}_2$. Suppose that $\mathcal{C}_1'$ refines $\mathcal{C}_1$ and $\mathcal{C}_2'$ refines $\mathcal{C}_2$. Then, $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$ only if $\mathcal{C}_1'$ is series composable to $\mathcal{C}_2'$, and $\mathcal{C}_1' \to \mathcal{C}_2'$ refines $\mathcal{C}_1 \to \mathcal{C}_2$.*

4.6 External interconnections

In this section, we will briefly discuss a noteworthy modification of the series and feedback interconnections, and the corresponding series and feedback compositions. To begin with, an alternative definition of the series interconnection is obtained by considering only the output of the second system as an external output, as shown in Figure 4.6. This is nothing more than the series interconnection from Definition 4.1 after the output of the first system is eliminated, see [63, Theorem 6.2.6] for details. More precisely, we have the following definition.

Definition 4.13. Consider the input-output systems Σ_1 and Σ_2 given by (4.1). The *external series interconnection* of Σ_1 to Σ_2, denoted by $\Sigma_1 \to_e \Sigma_2$, is obtained by eliminating the output y_1 from the series interconnection $\Sigma_1 \to \Sigma_2$,

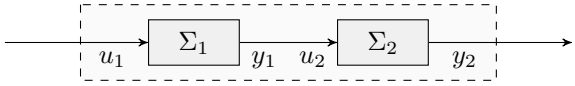

Figure 4.6: The external series interconnection $\Sigma_1 \to_e \Sigma_2$.

as defined in Definition 4.1. In other words, $(u, y_2) \in \mathfrak{B}(\Sigma_1 \to_e \Sigma_2)$ if and only if there exists y_1 such that $(u, y_1, y_2) \in \mathfrak{B}(\Sigma_1 \to \Sigma_2)$.

The corresponding external series composition needs to satisfy the same properties as the usual series composition. In particular, we are looking for a contract $\mathcal{C}_e = (\mathrm{A}_e, \Gamma_e)$ with the following properties. Let Σ_1 and Σ_2 be implementations of $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively. First, we want the environments of Σ_1 and Σ_2 in the interconnection $\mathrm{A}_e \wedge (\Sigma_1 \to_e \Sigma_2)$ to be compatible with $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Second, we want $\Sigma_1 \to_e \Sigma_2$ to implement $\mathcal{C}$. Recall the reformulation of Implication 4.1 at the end of Section 4.2. It is easily seen that the environments of Σ_1 and Σ_2 in $\mathrm{A}_e \wedge (\Sigma_1 \to_e \Sigma_2)$ are the same as in $\mathrm{A}_e \wedge (\Sigma_1 \to \Sigma_2)$. Therefore, the first property is equivalent to

$$\mathfrak{B}(\mathrm{A}_e \wedge (\Sigma_1 \to \Sigma_2)) \subset \mathfrak{B}(\mathrm{A}_1 \to \mathrm{A}_2). \tag{4.122}$$

On the other hand, due to Theorem 3.1, the second property is equivalent to

$$\mathfrak{B}(\mathrm{A}_e \wedge (\Sigma_1 \to_e \Sigma_2)) \subset \mathfrak{B}(\Gamma_e). \tag{4.123}$$

We then have the following definitions.

Definition 4.14. The contract $\mathcal{C}_1$ is *externally series composable* to $\mathcal{C}_2$ if there exists a contract $\mathcal{C}_e = (\mathrm{A}_e, \Gamma_e)$ that satisfies (4.122) and (4.123) for all implementations Σ_1 and Σ_2 of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively.

Definition 4.15. Suppose that $\mathcal{C}_1$ is externally series composable to $\mathcal{C}_2$. The *external series composition* of $\mathcal{C}_1$ to $\mathcal{C}_2$, denoted by $\mathcal{C}_1 \to_e \mathcal{C}_2$, is the *smallest* contract $\mathcal{C}_e = (\mathrm{A}_e, \Gamma_e)$ that satisfies (4.122) and (4.123) for all implementations Σ_1 and Σ_2 of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively.

Given the parallel between (4.122) and (4.65), the following result should not be surprising.

Lemma 4.14. *Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are consistent. Then, $\mathcal{C}_1$ is externally series composable to $\mathcal{C}_2$ if and only if $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$.*

Proof. We begin by proving necessity. Suppose that $\mathcal{C}_1$ is externally series composable to $\mathcal{C}_2$, that is, there exists a contract $\mathcal{C}_e = (\mathrm{A}_e, \Gamma_e)$ that satisfies (4.122) and (4.123) for all implementations Σ_1 and Σ_2 of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Suppose that Γ_e is given by

$$\Gamma_e : G_e\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) y_2 = H_e\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) u, \tag{4.124}$$

where $G_e(s)$ and $H_e(s)$ are polynomial matrices. Consider the guarantees

$$\Gamma : \begin{bmatrix} 0 & G_e\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = H_e\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) u, \tag{4.125}$$

and note that $(u, y_1, y_2) \in \mathfrak{B}(\Gamma)$ if and only if $(u, y_2) \in \mathfrak{B}(\Gamma_e)$. Consequently, by definition of $\Sigma_1 \to_e \Sigma_2$, (4.123) implies that

$$\mathfrak{B}(\mathrm{A}_e \wedge (\Sigma_1 \to \Sigma_2)) \subset \mathfrak{B}(\Gamma), \tag{4.126}$$

hence $\mathrm{A} = \mathrm{A}_e$ is such that the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies (4.65) and (4.66). As satisfaction of the latter is equivalent to satisfaction of Implication 4.1, it follows that $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$.

We proceed by proving sufficiency. Suppose that $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$, that is, there exists a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 4.1, or, equivalently, (4.65) and (4.66) for all implementations Σ_1 and Σ_2 of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Clearly, (4.65) implies that $\mathrm{A}_e = \mathrm{A}$ is such that (4.122) holds. Let Γ_e be obtained from Γ by eliminating y_1, that is, Γ_e is such that $(u, y_2) \in \mathfrak{B}(\Gamma_e)$ if and only if there exists y_1 such that $(u, y_1, y_2) \in \mathfrak{B}(\Gamma)$. Then, by definition of $\Sigma_1 \to_e \Sigma_2$, (4.66) implies (4.123). Consequently, $\mathcal{C}_e = (\mathrm{A}_e, \Gamma_e)$ satisfies (4.122) and (4.123), which shows that $\mathcal{C}_1$ is externally series composable to $\mathcal{C}_2$. □

In the proof of Lemma 4.14, we saw how to obtain a contract $\mathcal{C}_e = (\mathrm{A}_e, \Gamma_e)$ that satisfies (4.122) and (4.123) from a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies (4.65) and (4.66). In the same manner, we can obtain the external series composition $\mathcal{C}_1 \to_e \mathcal{C}_2$ from the series composition $\mathcal{C}_1 \to \mathcal{C}_2$. To this end, we first define the external series interconnection of guarantees.

Definition 4.16. Consider the guarantees Γ_1 and Γ_2 given by (4.2). The *external series interconnection* of Γ_1 to Γ_2, denoted by $\Gamma_1 \to_e \Gamma_2$, is obtained by eliminating the output y_1 from the series interconnection $\Gamma_1 \to \Gamma_2$ in Definition 4.2. In other words, $(u, y_2) \in \mathfrak{B}(\Gamma_1 \to_e \Gamma_2)$ if and only if there exists y_1 such that $(u, y_1, y_2) \in \mathfrak{B}(\Gamma_1 \to \Gamma_2)$.

The following theorem provides an explicit expression for the external series composition when it exists.

Theorem 4.7. *Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are consistent, and $\mathcal{C}_1$ is externally series composable to $\mathcal{C}_2$. Then, the external series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ exists and is given by*

$$\mathcal{C}_1 \to_e \mathcal{C}_2 = (\mathrm{A}_{12}, \Gamma_1 \to_e \Gamma_2), \tag{4.127}$$

where A_{12} is such that

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{12}) = \mathfrak{B}_{\mathrm{i}}((\mathrm{A}_1 \to \mathrm{A}_2) \wedge (\Gamma_1 \to \Gamma_2)), \tag{4.128}$$

that is, A_{12} is obtained by eliminating y from $(\mathrm{A}_1 \to \mathrm{A}_2) \wedge (\Gamma_1 \to \Gamma_2)$.

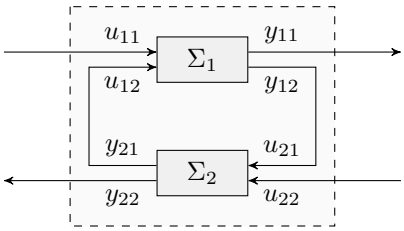

Figure 4.7: The external feedback interconnection $\Sigma_1 \leftarrow\!\!\!\rightarrow_e \Sigma_2$.

Proof. Since $\mathcal{C}_1$ is externally series composable to $\mathcal{C}_2$, Lemma 4.14 implies that $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$. Therefore, due to Theorem 4.5, the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ exists and is given by

$$\mathcal{C}_1 \to \mathcal{C}_2 = (\mathrm{A}_{12}, \Gamma_1 \to \Gamma_2). \tag{4.129}$$

In particular, this means that $\mathcal{C}_1 \to \mathcal{C}_2$ satisfies Implication 4.1. Consequently, as shown in the sufficiency part of the proof of Lemma 4.5, by definition of $\Gamma_1 \to_e \Gamma_2$, the contract $\mathcal{C}_1 \to_e \mathcal{C}_2$ given by (4.127) satisfies (4.122) and (4.123). Suppose that there is another contract $\mathcal{C}_e = (\mathrm{A}_e, \Gamma_e)$ that satisfies (4.122) and (4.123). We will show that $\mathcal{C}_1 \to_e \mathcal{C}_2$ refines $\mathcal{C}_e$, that is,

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_e) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{12}) \quad \text{and} \quad \mathfrak{B}(\mathrm{A}_e \wedge (\Gamma_1 \to_e \Gamma_2)) \subset \mathfrak{B}(\Gamma_e). \tag{4.130}$$

Suppose that Γ_e is given by (4.124) and consider the guarantees Γ given by (4.125). As shown in the proof of Lemma 4.14, the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$, where $\mathrm{A} = \mathrm{A}_e$, satisfies Implication 4.1. Since $\mathcal{C}_1 \to \mathcal{C}_2$ is the smallest such contract, it follows that $\mathcal{C}_1 \to \mathcal{C}_2$ refines $\mathcal{C}$, which, due to Theorem 3.3, implies that

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{12}) \quad \text{and} \quad \mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2)) \subset \mathfrak{B}(\Gamma). \tag{4.131}$$

Note that $(u, y_1, y_2) \in \mathfrak{B}(\Gamma)$ if and only if $(u, y_2) \in \mathfrak{B}(\Gamma_e)$, hence the relationship between $\mathfrak{B}(\Gamma)$ and $\mathfrak{B}(\Gamma_e)$ is the same as the relationship between $\mathfrak{B}(\Gamma_1 \to \Gamma_2)$ and $\mathfrak{B}(\Gamma_1 \to_e \Gamma_2)$. Therefore, (4.131) implies (4.130), where we recall that $\mathrm{A} = \mathrm{A}_e$. Due to Theorem 3.3, it follows that $\mathcal{C}_1 \to_e \mathcal{C}_2$ refines $\mathcal{C}_e$, which shows that $\mathcal{C}_1 \to_e \mathcal{C}_2$ is the smallest contract that satisfies (4.122) and (4.123). In other words, the contract $\mathcal{C}_1 \to_e \mathcal{C}_2$ given by (4.127) is indeed the external series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ □

In the same vein, we can define the external *feedback* interconnection by considering only the outputs that are not used for the interconnection as external outputs, as shown in Figure 4.7. More precisely, we have the following definition.

Definition 4.17. Consider the input-output systems Σ_1 and Σ_2 given by (4.1), and the partitions (4.8) and (4.9). The *external feedback interconnection* of Σ_1 to

Σ_2, denoted by $\Sigma_1 \leftarrow\!\!\!-_e \Sigma_2$, is obtained by eliminating the outputs y_{12} and y_{21} from the feedback interconnection $\Sigma_1 \leftarrow\!\!\!- \Sigma_2$, as defined in Definition 4.3. In other words, $(u, y_{11}, y_{22}) \in \mathfrak{B}(\Sigma_1 \leftarrow\!\!\!-_e \Sigma_2)$ if and only if there exists y_{12} and y_{21} such that $(u, y_{11}, y_{12}, y_{21}, y_{22}) \in \mathfrak{B}(\Sigma_1 \leftarrow\!\!\!- \Sigma_2)$.

Without going into details, the corresponding external feedback composition should be a contract $\mathcal{C}_e = (\mathrm{A}_e, \Gamma_e)$ that satisfies

$$\mathfrak{B}(\mathrm{A}_e \wedge (\Sigma_1 \leftarrow\!\!\!- \Sigma_2)) \subset \mathfrak{B}(\mathrm{A}_1 \leftarrow\!\!\!- \mathrm{A}_2), \tag{4.132}$$

$$\mathfrak{B}(\mathrm{A}_e \wedge (\Sigma_1 \leftarrow\!\!\!-_e \Sigma_2)) \subset \mathfrak{B}(\Gamma_e). \tag{4.133}$$

for all implementations Σ_1 and Σ_2 of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, whose interconnection $\Sigma_1 \leftarrow\!\!\!- \Sigma_2$ is well-posed. If such a contract exists, then $\mathcal{C}_1$ is *externally feedback composable* to $\mathcal{C}_2$. Moreover, the *external feedback composition* of $\mathcal{C}_1$ to $\mathcal{C}_2$, denoted by $\mathcal{C}_1 \leftarrow\!\!\!-_e \mathcal{C}_2$, is the smallest such contract.

Using arguments similar to the ones in the proof of Lemma 4.14, we can show that $\mathcal{C}_1$ is externally feedback composable to $\mathcal{C}_2$ if and only if $\mathcal{C}_1$ is feedback composable to $\mathcal{C}_1$. In this case, the external feedback composition $\mathcal{C}_1 \leftarrow\!\!\!-_e \mathcal{C}_2$ exists and can be obtained from the feedback composition $\mathcal{C}_1 \leftarrow\!\!\!- \mathcal{C}_2$. To this end, we first define the external feedback composition of guarantees.

Definition 4.18. Consider the guarantees Γ_1 and Γ_2 given by (4.2), and the partitions (4.8) and (4.26). The *external feedback interconnection* of Γ_1 to Γ_2, denoted by $\Gamma_1 \leftarrow\!\!\!-_e \Gamma_2$, is obtained by eliminating the outputs y_{12} and y_{21} from the feedback interconnection $\Gamma_1 \leftarrow\!\!\!- \Gamma_2$, as defined in Definition 4.5. In other words, $(u, y_{11}, y_{22}) \in \mathfrak{B}(\Gamma_1 \leftarrow\!\!\!-_e \Gamma_2)$ if and only if there exists y_{12} and y_{21} such that $(u, y_{11}, y_{12}, y_{21}, y_{22}) \in \mathfrak{B}(\Gamma_1 \leftarrow\!\!\!- \Gamma_2)$.

Now, using Theorem 4.3, we obtain the following theorem regarding the external feedback composition. We omit the proof as it follows reasoning similar to the one in the proof of Theorem 4.7

Theorem 4.8. *Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are row-reduced, $\Gamma_1 \leftarrow\!\!\!- \Gamma_2$ is well-posed, and $\mathcal{C}_1$ is externally feedback composable to $\mathcal{C}_2$. Then, the external feedback composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ exists and is given by*

$$\mathcal{C}_1 \leftarrow\!\!\!-_e \mathcal{C}_2 = (\mathrm{A}_{12}, \Gamma_1 \leftarrow\!\!\!-_e \Gamma_2), \tag{4.134}$$

where A_{12} is such that

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{12}) = \mathfrak{B}_{\mathrm{i}}((\mathrm{A}_1 \leftarrow\!\!\!- \mathrm{A}_2) \wedge (\Gamma_1 \leftarrow\!\!\!- \Gamma_2)), \tag{4.135}$$

that is, A_{12} is obtained after eliminating y from $(\mathrm{A}_1 \leftarrow\!\!\!- \mathrm{A}_2) \wedge (\Gamma_1 \leftarrow\!\!\!- \Gamma_2)$.

4.7 Discussion

In this chapter, we further developed the contract theory introduced in Chapter 3 by developing notions of contract composition that enable the independent design of components within interconnected systems. In particular, we defined two notions of contract composition that allow us to reason about two types of component 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 each implementation is guaranteed to operate in interconnection with an environment compatible with its contract.

In order to avoid unessential technicalities and gain better intuition, we first restricted ourselves to the special case where both contracts have output guarantees. With this restriction in place, we found necessary and sufficient conditions for the existence of the series and feedback composition, respectively. We also provided an explicit expression for each composition when it exists. Then, equipped with the intuition that the special cases provided us, we treated the general case for the feedback composition. Again, we found necessary and sufficient conditions for the existence of the feedback composition, and we provided an explicit expression for it when it exists. Finally, we treated the general case for the series composition. We did this by viewing the series interconnection as a special case of the feedback interconnection, where some of the partitioned inputs and outputs are void. This allowed us to use our results on the feedback composition to obtain results on the series composition. In particular, we found necessary and sufficient conditions for the existence of the series composition, and we provided an explicit expression for the series composition when it exists.

Note that the conditions for the existence of the series and feedback composition are in the form of behavioural inclusions involving only assumptions and guarantees, hence they can be verified algorithmically. Furthermore, the expressions for the series and feedback compositions can be obtained directly (for the series composition) or algorithmically (for the feedback composition) from the assumptions and guarantees of the contracts that are composed. To put it differently, our results are tractable and can be used in practice. On the other hand, like we obtained results on the series composition from our results on the feedback composition, we can obtain results on other types of composition by considering other special cases of the feedback interconnection.

Together with the notion of contract refinement that we introduced in Chapter 3, the notions of contract composition introduced in this chapter enable the independent design of components within interconnected systems. As explained in Chapter 1 and Chapter 2, this is done in two steps. First, the notion of contract composition allows us to reason about the specification

that an interconnected system satisfies on the basis of the specifications that its components satisfy. In other words, we can obtain the composite specification in Figure 1.3 from the local specifications in Figure 1.2. Second, the notion of contract refinement allows us to ensure that the interconnected system satisfies a preassigned global specification on the basis of the specifications that its components satisfy. More precisely, we can ensure that satisfaction of the composite specification in Figure 1.3 implies satisfaction of the global specification in Figure 1.1. In addition to supporting independent design, the notions of contract composition introduced in this chapter support independent refinement, as described in Chapter 2. This allows us to independently design interconnected systems as components of an interconnected system, see Figure 2.5.

In conclusion, the contract theory developed in this and last chapter provides a method for expressing specifications on the dynamics of linear dynamical systems that supports the independent design of components within interconnected systems. Nevertheless, we point out that our results allow us to only *verify* that satisfaction of *given* local specifications for the components leads to satisfaction of a given global specification for the interconnected system. In practice, it is often necessary to *design* local specification whose satisfaction leads to satisfaction of a given global specification. Note that this might involve the design of the interconnection topology as well. The design of such local specifications is left as a topic of further research.

Chapter 5

Simulation contracts

One limitation of the approach taken in the two last chapters is the lack of *efficient* computational tools for verifying behavioural inclusion. We address this limitation here by defining contracts using the notion of simulation as a means of comparing system behaviour.[1] Simulation is the one-sided version of bisimulation [64, 65], which is a notion of system equivalence first introduced in the theory of concurrent processes [66]. As already noted in the latter, simulation is a stronger notion than behavioural inclusion for nondeterministic systems, which are considered throughout this thesis. Furthermore, simulation can be verified efficiently using the (controlled) invariant subspace algorithm [68, 86], and its connection to geometric control theory [67] allows us to use a multitude of tools and techniques in tackling problems related to contract-based design.

With this in mind, we make the following contributions in this chapter. First, we introduce assume-guarantee contracts for linear dynamical input-state-output systems with a driving variable. We begin by defining contracts as pairs of linear dynamical systems called assumptions and guarantees, following a similar perspective as the one for behavioural contracts. We then define and characterize contract implementation using the notion of simulation. In particular, we show that a given system implements a given contract, i.e., it satisfies the specification expressed by the contract, if and only if the interconnection of the system with the assumptions is simulated by the guarantees. As already mentioned, simulation can be verified efficiently using the invariant subspace algorithm, thus allowing contract implementation to be verified efficiently.

Then, we turn to design rather than verification by considering the problem of constructing an implementation for a given contract. To this end, we first establish conditions under which the contract has an implementation at

[1] Part of this chapter has appeared in [85].

all, i.e., the contract is consistent. Using the connection between simulation and geometric control theory, we show that a contract is consistent if and only if there exists a pair of subspaces that satisfy certain geometric conditions. We then show how the existence of these subspaces can be verified by following a systematic procedure, and, in the process, we obtain an algorithm for constructing an implementation when it exists.

Next, we consider a problem related to control design. Namely, we consider the situation where a given contract expresses a specification for a given plant system. The plant system does not necessarily implement the contract but can be controlled to do so. We show that there exists a controller that turns the plant system into an implementation of the contract if and only if there exists a pair of subspaces that satisfy certain geometric properties. These properties are similar to the ones for contract consistency and are also derived using ideas from geometric control theory. We show that the existence of an appropriate controller can be verified by following a similar systematic procedure, and we obtain an algorithm for the construction of such a controller when it exists.

Lastly, we make first steps towards enabling the use of the contract for independent design of components within interconnected systems. In particular, following the meta-theoretic definition outlined in Chapter 2, we define contract refinement in order to compare contracts and to determine if one contract expresses a stricter specification than another. We obtain necessary and sufficient conditions for refinement that take the form of a pair of simulation conditions involving only assumptions and guarantees. Since simulation can be verified efficiently, this allows refinement to be verified efficiently as well. In addition to refinement, we define the series composition of two contracts according to the series interconnection of two systems, again following the meta-theoretic definition outlined in Chapter 2. We show that the series composition of two arbitrary contracts does not necessarily exists, and we obtain a necessary and sufficient condition for its existence in the form of a simulation condition involving only assumptions and guarantees. Furthermore, we provide an explicit expression for the series composition when it exists.

The rest of the chapter is structured as follows. In Section 5.1, we review the notion of simulation for the class of systems that will be used to define contracts. In Section 5.2, we define contracts and characterize contract implementation. Following this, in Section 5.3, we characterize contract consistency and provide a systematic procedure for constructing an implementation of a consistent contract. Section 5.4 is concerned with the design of a controller that turns a given plant system into an implementation of a given contract. We illustrate the results of Section 5.4 with an example in Section 5.5. In Section 5.6, we define and characterize contract refinement. Then, in Section 5.7, we define and characterize the series composition. Finally, in Section 5.8, we discuss the similarities and differences with the results from the previous two

chapters, after which we conclude this chapter with a brief discussion in Section 5.9.

5.1 Preliminaries on simulation

In this section, we will review the notion of simulation for the class of linear systems that will be used to define contracts in Section 5.2. Namely, we consider systems of the form

$$\Xi_i : \begin{cases} \dot{x}_i(t) = A_i x_i(t) + G_i d_i(t), \\ w(t) = C_i x_i(t), \\ 0 = H_i x_i(t), \end{cases} \tag{5.1}$$

with state $x_i(t) \in \mathcal{X}_i$, output $w(t) \in \mathcal{W}_i$, and driving variable $d_i(t) \in \mathcal{D}_i$, where $\mathcal{X}_i$, $\mathcal{W}$ and $\mathcal{D}_i$ are finite-dimensional vector spaces, e.g., $\mathbb{R}^{n_i}$, $\mathbb{R}^p$ and $\mathbb{R}^{q_i}$. We view the output w_i as external, and the state x_i and driving variable d_i as internal. The driving variable d_i plays the role of a generator of trajectories and introduces indeterminism in the system. It can be used to model, e.g., unknown inputs or lack of knowledge about the dynamics of Ξ_i.

Note that the systems Ξ_i include algebraic constraints. Not all initial states lead to trajectories that satisfy the algebraic constraints. This motivates the introduction of the *consistent subspace* $\mathcal{V}_i \subset \mathcal{X}_i$. The consistent subspace $\mathcal{V}_i$ is defined as the set of initial states $x_i(0)$ for which there exists a driving variable trajectory $d_i(\cdot)$ such that the resulting state trajectory $x_i(\cdot)$ satisfies the algebraic constraint $H_i x_i(t) = 0$ for all $t \geq 0$. It can be shown, see, e.g., [87, 88], that $\mathcal{V}_i$ is the *largest* subspace that satisfies

$$A_i \mathcal{V}_i \subset \mathcal{V}_i + \operatorname{im} G_i \quad \text{and} \quad \mathcal{V}_i \subset \ker H_i. \tag{5.2}$$

Our definition of a contract relies on comparing the (external) dynamic behaviour of different systems Ξ_i. We will do this using the notion of simulation, which itself relies on the notion of simulation relation. The following definition is taken from [58], see also [87, 88]. Note that, given a subspace $\mathcal{S} \subset \mathcal{X}_1 \times \mathcal{X}_2$, $\pi_{\mathcal{X}_1}(\mathcal{S})$ denotes the projection of $\mathcal{S}$ onto $\mathcal{X}_1$, that is,

$$\pi_{\mathcal{X}_1}(\mathcal{S}) = \{x_1 \in \mathcal{X}_1 \mid \exists x_2 \in \mathcal{X}_2 \text{ s.t. } (x_1, x_2) \in \mathcal{S}\}. \tag{5.3}$$

Definition 5.1. A subspace $\mathcal{S} \subset \mathcal{X}_1 \times \mathcal{X}_2$ is a *simulation relation* of Ξ_1 by Ξ_2 if $\pi_{\mathcal{X}_1}(\mathcal{S}) \subset \mathcal{V}_1$, $\pi_{\mathcal{X}_2}(\mathcal{S}) \subset \mathcal{V}_2$, and the following implication holds: for all $(x_1(0), x_2(0)) \in \mathcal{S}$ and all $d_1(\cdot)$ such that $x_1(t) \in \mathcal{V}_1$ for all $t \geq 0$, there exists $d_2(\cdot)$ such that:

1. $(x_1(t), x_2(t)) \in \mathcal{S}$ for all $t \geq 0$;
2. $C_1 x_1(t) = C_2 x_2(t)$ for all $t \geq 0$.

In particular, a simulation relation of Ξ_1 by Ξ_2 is a subspace of pairs of consistent initial conditions $(x_1(0), x_2(0))$ with the property that any consistent state trajectory of Ξ_1 starting at $x_1(0)$ can be matched by a consistent state trajectory of Ξ_2 starting at $x_2(0)$ such that the corresponding output trajectories of Ξ_1 and Ξ_2 are identical. The following characterization of a simulation relation based solely on the system matrices can be obtained using ideas from geometric control theory, see [58, 87, 88] for details.

Proposition 5.1. *A subspace $\mathcal{S} \subset \mathcal{X}_1 \times \mathcal{X}_2$ is a simulation relation of Ξ_1 by Ξ_2 if and only if*

$$\begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix} \mathcal{S} \subset \mathcal{S} + \operatorname{im} \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}, \tag{5.4}$$

$$\begin{bmatrix} \operatorname{im} G_1 \cap \mathcal{V}_1 \\ 0 \end{bmatrix} \subset \mathcal{S} + \operatorname{im} \begin{bmatrix} 0 \\ G_2 \end{bmatrix}, \tag{5.5}$$

$$\mathcal{S} \subset \ker \begin{bmatrix} C_1 & -C_2 \\ H_1 & 0 \\ 0 & H_2 \end{bmatrix}. \tag{5.6}$$

Remark 5.1. *In Proposition 5.1, we do not explicitly require that $\pi_{\mathcal{X}_1}(\mathcal{S}) \subset \mathcal{V}_1$ and $\pi_{\mathcal{X}_2}(\mathcal{S}) \subset \mathcal{V}_2$. This is because, for each $i \in \{1, 2\}$,* (5.4) *and* (5.6) *yield*

$$A_i \pi_{\mathcal{X}_i}(\mathcal{S}) \subset \pi_{\mathcal{X}_i}(\mathcal{S}) + \operatorname{im} G_i \quad \textit{and} \quad \pi_{\mathcal{X}_i}(\mathcal{S}) \subset \ker H_i, \tag{5.7}$$

respectively, which implies that $\pi_{\mathcal{X}_i}(\mathcal{S}) \subset \mathcal{V}_i$.

Remark 5.2. *If Ξ_1 does not include algebraic constraints, then $\mathcal{V}_1 = \mathcal{X}_1$ and the condition* (5.5) *reduces to*

$$\operatorname{im} \begin{bmatrix} G_1 \\ 0 \end{bmatrix} \subset \mathcal{S} + \operatorname{im} \begin{bmatrix} 0 \\ G_1 \end{bmatrix}, \tag{5.8}$$

which implies that (5.4) *is equivalent to the simpler condition*

$$\begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix} \mathcal{S} \subset \mathcal{S} + \operatorname{im} \begin{bmatrix} 0 \\ G_2 \end{bmatrix}. \tag{5.9}$$

See [65, Section V] for a treatment of simulation for systems without algebraic constraints.

It will sometimes be more convenient to use the following characterization of a simulation relation, which is easily seen to be equivalent to the characterization in Proposition 5.1.

Proposition 5.2. *A subspace $\mathcal{S} \subset \mathcal{X}_1 \times \mathcal{X}_2$ is a simulation relation of Ξ_1 by Ξ_2 if and only if for all $(x_1, x_2) \in \mathcal{S}$ and all $d_1 \in \mathcal{D}_1$ such that $A_1 x_1 + G_1 d_1 \in \mathcal{V}_1$, there exist $d_2 \in \mathcal{D}_2$ such that $(A_1 x_1 + G_1 d_1, A_2 x_2 + G_2 d_2) \in \mathcal{S}$ and*

$$C_1 x_1 = C_2 x_2, \quad H_1 x_1 = 0, \quad 0 = H_2 x_2. \tag{5.10}$$

Using simulation relations, we define simulation as follows.

Definition 5.2. A system Ξ_1 is *simulated by* Ξ_2, denoted as $\Xi_1 \preccurlyeq \Xi_2$, if there exists a simulation relation $\mathcal{S} \subset \mathcal{X}_1 \times \mathcal{X}_2$ of Ξ_1 by Ξ_2 such that $\pi_{\mathcal{X}_1}(\mathcal{S}) = \mathcal{V}_1$. A simulation relation with this property is called a *full simulation relation*.

Just like behavioural inclusion, simulation can be used to compare the (external) dynamic behaviour of two systems. Indeed, if $\Xi_1 \preccurlyeq \Xi_2$, then *any* consistent state trajectory of Ξ_1 can be matched by a consistent state trajectory of Ξ_2 such that the corresponding output trajectories of Ξ_1 and Ξ_2 are identical. This means that Ξ_2 has richer (external) dynamics than Ξ_1.

Remark 5.3. *Simulation is a stronger notion than behavioural inclusion. To see this, note that the external behaviour of Ξ consists of all output trajectories that correspond to a consistent state trajectory. Therefore, the external behaviour of Ξ_1 is contained in the external behaviour of Ξ_2 if and only if any consistent state trajectory of Ξ_1 can be matched by a consistent state trajectory of Ξ_2 such that the resulting output trajectories of Ξ_1 and Ξ_2 are identical. However, for simulation, we also fix the initial state of both systems before we go through their state trajectories. For a discussion of the closely related comparison between bisimulation and behavioural equality, we refer to [15, 65].*

Remark 5.4. *In view of* (5.2)*, computing the consistent subspace of a system Ξ_i amounts to computing the largest (A_i, G_i)-invariant subspace contained in* $\ker H_i$*. This can be done using the (controlled) invariant subspace algorithm [67, 68]. Similarly, using the same algorithm, we can compute the largest subspace $\mathcal{S}$ that satisfies* (5.4) *and* (5.6)*. If this $\mathcal{S}$ satisfies* (5.5) *as well, then it is a simulation relation of Ξ_1 by Ξ_2. In fact, it is the* largest *simulation relation of Ξ_1 by Ξ_2, which means that Ξ_1 is simulated by Ξ_2 if and only if this $\mathcal{S}$ is a* full *simulation relation. This means that simulation is supported by an efficient numerical procedure for verification.*

Remark 5.5. *We will sometimes compare systems that have multiple outputs. In such a case, when referring to simulation, we will only consider the shared outputs. For example, if Ξ_1 has the outputs w and z_1, and Ξ_2 has the outputs w and z_2, then Ξ_1 is simulated by Ξ_2 if it is simulated by Ξ_2 when the separate outputs z_1 and z_2 are ignored.*

Simulation defines a preorder, that is, it is both reflexive and transitive. Indeed, it is easily seen that the subspace $\mathcal{S} \subset \mathcal{X}_1 \times \mathcal{X}_1$ given by

$$\mathcal{S} = \{(x_1, x_1) \mid x_1 \in \mathcal{V}_1\} \tag{5.11}$$

is a full simulation relation of Ξ_1 by itself, hence $\Xi_1 \preccurlyeq \Xi_1$, which shows that simulation is reflexive. On the other hand, if $\Xi_1 \preccurlyeq \Xi_2$ with a full simulation relation $\mathcal{S}_{12}$, and $\Xi_2 \preccurlyeq \Xi_3$ with a full simulation relation $\mathcal{S}_{23}$, then the subspace $\mathcal{S}_{13} \subset \mathcal{X}_1 \times \mathcal{X}_3$ given by

$$\mathcal{S}_{13} = \{(x_1, x_3) \mid \exists x_2 \in \mathcal{X}_2 \text{ s.t. } (x_1, x_2) \in \mathcal{S}_{12},\ (x_2, x_3) \in \mathcal{S}_{23}\} \tag{5.12}$$

is a full simulation relation of Ξ_1 by Ξ_3, hence $\Xi_1 \preccurlyeq \Xi_3$, which shows that simulation is also transitive. Note that simulation is not a partial order because it is not antisymmetric, that is, $\Xi_1 \preccurlyeq \Xi_2$ and $\Xi_2 \preccurlyeq \Xi_1$ do not imply that Ξ_1 and Ξ_2 are identical. This is the case when, e.g., Ξ_1 and Ξ_2 are related by a state-space transformation.

Simulation is the one-sided version of the notion of *bisimulation*, whose definition for systems of the form (5.42) can be found in [65]. Loosely speaking, two systems are bisimilar if they cannot be distinguished by an agent that interacts only with their external variables. In [65], it is shown that Ξ_1 and Ξ_2 are bisimilar, denoted by $\Xi_1 \sim \Xi_2$, if and only if $\Xi_1 \preccurlyeq \Xi_2$ and $\Xi_2 \preccurlyeq \Xi_1$. The following proposition shows that any system of the form (5.1) is bisimilar to a system of the same form but without algebraic constraints.

Proposition 5.3. *Consider the system*

$$\Xi : \begin{cases} \dot{x}(t) = Ax(t) + Gd(t), \\ w(t) = Cx(t), \\ \quad 0 = Hx(t), \end{cases} \tag{5.13}$$

where $x(t) \in \mathcal{X}$, $d(t) \in \mathcal{D}$, and $w(t) \in \mathcal{W}$. There exists a system

$$\tilde{\Xi} : \begin{cases} \dot{\tilde{x}}(t) = \tilde{A}x(t) + \tilde{G}\tilde{d}(t), \\ w(t) = \tilde{C}x(t), \end{cases} \tag{5.14}$$

where $\tilde{x}(t) \in \tilde{\mathcal{X}}$, and $\tilde{d}(t) \in \tilde{\mathcal{D}}$, such that $\tilde{\Xi} \sim \Xi$.

Proof. Let $\mathcal{V} \subset \mathcal{X}$ be the consistent subspace of Ξ, and note that

$$A\mathcal{V} \subset \mathcal{V} + \operatorname{im} G \quad \text{and} \quad \mathcal{V} \subset \ker H, \tag{5.15}$$

Due to [68, Theorem 4.2], it follows that there exist a matrix K such that

$$(A + GK)\mathcal{V} \subset \mathcal{V}. \tag{5.16}$$

Let T be a matrix such that $\operatorname{im} GT = \operatorname{im} G \cap \mathcal{V}$. Furthermore, let V be a matrix whose columns form a basis for $\mathcal{V}$. Since V has full column rank, there exists a matrix $V^\dagger$ such that $V^\dagger V = I$. With this in mind, we will show that the system $\tilde{\Xi}$ given by (5.14) with

$$\tilde{A} = V^\dagger(A + GK)V, \qquad \tilde{G} = V^\dagger GT, \qquad \tilde{C} = CV, \tag{5.17}$$

is such that $\tilde{\Xi} \sim \Xi$.

First, we will show that the subspace $\mathcal{R} \subset \tilde{\mathcal{X}} \times \mathcal{X}$ given by

$$\mathcal{R} = \{(\tilde{x}, x) \mid V\tilde{x} = x\} \tag{5.18}$$

is a full simulation relation of $\tilde{\Xi}$ by Ξ. Let $(\tilde{x}, x) \in \mathcal{R}$ and $\tilde{d} \in \tilde{\mathcal{D}}$. This means that $V\tilde{x} = x$, hence

$$V\big(\tilde{A}\tilde{x} + \tilde{G}\tilde{d}\big) = VV^{\dagger}\big((A + GK)x + GT\tilde{d}\big). \tag{5.19}$$

Since $x \in \mathcal{V}$, (5.16) holds and $\operatorname{im} GT \subset \mathcal{V}$, it follows that $(A + GK)x \in \mathcal{V}$ and $GT\tilde{d} \in \mathcal{V}$. Then, because $VV^{\dagger}z = z$ for all $z \in \mathcal{V}$, we obtain

$$V\big(\tilde{A}\tilde{x} + \tilde{G}\tilde{d}\big) = Ax + G(Kx + T\tilde{d}), \tag{5.20}$$

hence $d = Kx + T\tilde{d}$ is such that

$$\big(\tilde{A}\tilde{x} + \tilde{G}\tilde{d}, Ax + Gd\big) \in \mathcal{R}. \tag{5.21}$$

Furthermore, we have that

$$\tilde{C}\tilde{x} = CV\tilde{x} = Cx, \qquad 0 = Hx, \tag{5.22}$$

and $\pi_{\tilde{\mathcal{X}}}(\mathcal{R}) = \tilde{\mathcal{X}}$, which, due to Proposition 5.2, shows that $\mathcal{R}$ is a full simulation relation of $\tilde{\Xi}$ by Ξ, that is, $\tilde{\Xi} \preccurlyeq \Xi$.

Next, we will show that the subspace $\mathcal{R}^{-1} \subset \mathcal{X} \times \tilde{\mathcal{X}}$ given by

$$\mathcal{R}^{-1} = \{(x, \tilde{x}) \mid x = V\tilde{x}\} \tag{5.23}$$

is a full simulation relation of Ξ by $\tilde{\Xi}$. Let $(x, \tilde{x}) \in \mathcal{R}^{-1}$ and let $d \in \mathcal{D}$ be such that $Ax + Gd \in \mathcal{V}$. Since $x \in \mathcal{V}$, it follows that $(A + GK)x \in \mathcal{V}$ and thus $Gd - GKx \in \mathcal{V}$ because of linearity. This means that

$$Gd - GKx \in \operatorname{im} G \cap \mathcal{V} = \operatorname{im} GT, \tag{5.24}$$

hence there exists $\tilde{d} \in \tilde{\mathcal{D}}$ such that

$$Gd - GKx = GT\tilde{d} = \tilde{G}\tilde{d}. \tag{5.25}$$

Then, it is easily seen that

$$V\big(\tilde{A}\tilde{x} + \tilde{G}\tilde{d}\big) = VV^{\dagger}\,(Ax + Gd) = Ax + Gd, \tag{5.26}$$

where we used the fact that $VV^{\dagger}z = z$ for all $z \in \mathcal{V}$. Consequently, we obtain

$$\big(Ax + Gd, \tilde{A}\tilde{x} + \tilde{G}\tilde{d}\big) \in \mathcal{R}^{-1}. \tag{5.27}$$

Furthermore, we have that

$$Cx = CV\tilde{x} = \tilde{C}\tilde{x} \tag{5.28}$$

and $\pi_{\mathcal{X}}(\mathcal{R}^{-1}) = \mathcal{V}$, which, due to Proposition 5.2, shows that $\mathcal{R}^{-1}$ is a full simulation relation of Ξ by $\tilde{\Xi}$, that is, $\Xi \preccurlyeq \tilde{\Xi}$. Since we also have that $\tilde{\Xi} \preccurlyeq \Xi$, this implies that $\tilde{\Xi} \sim \Xi$, as desired. □

Proposition 5.3 suggests that the class of systems of the form (5.13) is externally indistinguishable from the class of systems of the form (5.14). In other words, without loss of generality, we can restrict ourselves to systems of the form (5.14). However, including algebraic constraints makes it easier to define interconnections of systems, which will be essential in the definition of a contract and the analysis of the notions associated with it. In particular, the most common interconnection that will be considered is the meet, defined below.

Definition 5.3. Consider two systems Ξ_1 and Ξ_2 of the form (5.1). The *meet* of Ξ_1 and Ξ_2, denoted by $\Xi_1 \wedge \Xi_2$, is obtained by equating their shared output w. This results in the system

$$\Xi_1 \wedge \Xi_2 : \begin{cases} \begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \end{bmatrix} = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} + \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix} \begin{bmatrix} d_1(t) \\ d_2(t) \end{bmatrix}, \\ w(t) = \begin{bmatrix} C_1 & 0 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix}, \\ 0 = \begin{bmatrix} H_1 & 0 \\ 0 & H_2 \\ C_1 & -C_2 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix}. \end{cases} \tag{5.29}$$

Additional separate outputs Ξ_1 and Ξ_2 are also outputs of $\Xi_1 \wedge \Xi_2$.

Remark 5.6. *It is easily seen that the consistent subspace $\mathcal{V}_{12}$ of $\Xi_1 \wedge \Xi_2$ is such that $\mathcal{V}_{12} \subset \mathcal{V}_1 \times \mathcal{V}_2$, where $\mathcal{V}_1$ and $\mathcal{V}_2$ are the consistent subspaces of Ξ_1 and Ξ_2, respectively. On the other hand, in view of Proposition 5.1, if $\Xi_1 \preccurlyeq \Xi_2$, then $\mathcal{V}_{12}$ is the largest simulation relation of Ξ_1 by Ξ_2. Indeed, $\mathcal{V}_{12}$ is the largest subspace that satisfies* (5.4) *and* (5.6)*. In particular, this means that $\pi_{\mathcal{X}_1}(\mathcal{V}_{12}) = \mathcal{V}_1$.*

The meet has the following properties with respect to simulation.

Proposition 5.4. *The following statements are true:*

1. *If $\Xi_1' \preccurlyeq \Xi_1$ and $\Xi_2' \preccurlyeq \Xi_2$, then $\Xi_1' \wedge \Xi_2' \preccurlyeq \Xi_1 \wedge \Xi_2$.*
2. *If $\Xi \preccurlyeq \Xi_1 \wedge \Xi_2$, then $\Xi \preccurlyeq \Xi_1$ and $\Xi \preccurlyeq \Xi_2$.*

Proof. We begin by proving the first statement. Suppose that $\Xi_1' \preccurlyeq \Xi_1$ and $\Xi_2 \preccurlyeq \Xi_2'$, where Ξ_1 and Ξ_2 are of the form (5.1), and Ξ_1' and Ξ_2' are of the same form but with everything primed. Let $\mathcal{S}_1$ be a full simulation relation of Ξ_1' by Ξ_1, and $\mathcal{S}_2$ be a full simulation relation of Ξ_2' by Ξ_2. Furthermore, let $\mathcal{V}_{12}'$ be the consistent subspace of $\Xi_1' \wedge \Xi_2'$. We will show that the subspace $\mathcal{S} \subset \mathcal{X}_1' \times \mathcal{X}_2' \times \mathcal{X}_1 \times \mathcal{X}_2$ given by

$$\mathcal{S} = \{(x_1', x_2', x_1, x_2) \mid (x_1', x_2') \in \mathcal{V}_{12}',\ (x_1', x_1) \in \mathcal{S}_1,\ (x_2', x_2) \in \mathcal{S}_2\} \tag{5.30}$$

is a full simulation relation of $\Xi_1' \wedge \Xi_2'$ by $\Xi_1 \wedge \Xi_2$.

To this end, note that the dynamics of $\Xi_1' \wedge \Xi_2'$ are given by (5.29) but with everything primed. Let $(x_1', x_2', x_1, x_2) \in \mathcal{S}$ and let $d_1' \in \mathcal{D}_1'$ and $d_2' \in \mathcal{D}_2'$ be such that

$$(A_1'x_1' + G_1'd_1', A_2'x_2' + G_2'd_2') \in \mathcal{V}_{12}'. \tag{5.31}$$

Since $\mathcal{V}_{12}' \subset \mathcal{V}_1' \times \mathcal{V}_2'$, where $\mathcal{V}_1'$ and $\mathcal{V}_2'$ are the consistent subspaces of Ξ_1' and Ξ_2', respectively, it follows that $A_1'x_1' + G_1'd_1' \in \mathcal{V}_1'$ and $A_2'x_2' + G_2'd_2' \in \mathcal{V}_2'$. Then, since $(x_1', x_1) \in \mathcal{S}_1$ and $A_1'x_1' + G_1'd_1' \in \mathcal{V}_1'$, there exists $d_1 \in \mathcal{D}_1$ such that

$$(A_1'x_1' + G_1'd_1', A_1x_1 + G_1d_1) \in \mathcal{S}_1. \tag{5.32}$$

Similarly, there exists $d_2 \in \mathcal{D}_2$ such that

$$(A_2'x_2' + G_2'd_2', A_2x_2 + G_2d_2) \in \mathcal{S}_2. \tag{5.33}$$

On the other hand, $(x_1', x_2') \in \mathcal{V}_{12}'$ implies that

$$C_1'x_1' = C_2'x_2', \quad H_1'x_1' = 0, \quad H_2'x_2' = 0, \tag{5.34}$$

while $(x_1', x_1) \in \mathcal{S}_1$ and $(x_2', x_2) \in \mathcal{S}_2$ imply that

$$C_1'x_1' = C_1x_1, \quad H_1'x_1' = 0, \quad 0 = H_1x_1, \tag{5.35}$$

$$C_2'x_2' = C_2x_2, \quad H_2'x_2' = 0, \quad 0 = H_2x_2. \tag{5.36}$$

All things considered, we have that

$$(A_1'x_1' + G_1'd_1', A_2'x_2' + G_2'd_2', A_1x_1 + G_1d_1, A_2x_2 + G_2d_2) \in \mathcal{S}, \tag{5.37}$$

and

$$\begin{bmatrix} C_1' & 0 \end{bmatrix} \begin{bmatrix} x_1' \\ x_2' \end{bmatrix} = \begin{bmatrix} C_1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \quad \begin{bmatrix} H_1' & 0 \\ 0 & H_2' \\ C_1' & -C_2' \end{bmatrix} \begin{bmatrix} x_1' \\ x_2' \end{bmatrix} = 0, \quad 0 = \begin{bmatrix} H_1 & 0 \\ 0 & H_2 \\ C_1 & -C_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

In view of (5.29) and Proposition 5.2, it follows that $\mathcal{S}$ is a simulation relation of $\Xi_1' \wedge \Xi_2'$ by $\Xi_1 \wedge \Xi_2$. We also have that $\pi_{\mathcal{X}_1' \times \mathcal{X}_2'}(\mathcal{S}) = \mathcal{V}_{12}'$. Indeed, we have that $\pi_{\mathcal{X}_1' \times \mathcal{X}_2'}(\mathcal{S}) \subset \mathcal{V}_{12}'$ by definition of $\mathcal{S}$. On the other hand, if $(x_1', x_2') \in \mathcal{V}_{12}'$, then $x_1' \in \mathcal{V}_1'$ and $x_2' \in \mathcal{V}_2'$, hence there exist $x_1 \in \mathcal{X}_1$ and $x_2 \in \mathcal{X}_2$ such that $(x_1', x_1) \in \mathcal{S}_1$, $(x_2', x_2) \in \mathcal{S}_2$ and, thus, $(x_1', x_2', x_1, x_2) \in \mathcal{S}$. This implies that $\mathcal{V}_{12}' \subset \pi_{\mathcal{X}_1' \times \mathcal{X}_2'}(\mathcal{S})$, hence $\mathcal{S}$ is a full simulation relation and $\Xi_1' \wedge \Xi_2' \preccurlyeq \Xi_1 \wedge \Xi_2$.

We proceed by proving the second statement. Suppose that $\Xi \preccurlyeq \Xi_1 \wedge \Xi_2$. Let $\mathcal{S}$ be a full simulation relation of Ξ by $\Xi_1 \wedge \Xi_2$. We claim that $\pi_{\mathcal{X} \times \mathcal{X}_1}(\mathcal{S})$ is a full simulation relation of Ξ by Ξ_1. To show this, let $(x, x_1) \in \pi_{\mathcal{X} \times \mathcal{X}_1}(\mathcal{S})$ and let $d \in \mathcal{D}$ be such that $Ax + Gd \in \mathcal{V}$, where $\mathcal{V}$ is the consistent subspace of Ξ. Then, there exists $x_2 \in \mathcal{X}_2$ such that $(x, x_1, x_2) \in \mathcal{S}$, hence, due to Proposition 5.2, there exists $d_1 \in \mathcal{D}_1$ and $d_2 \in \mathcal{D}_2$ such that

$$(Ax + Gd, A_1x_1 + G_1d_1, A_2x_2 + G_2d_2) \in \mathcal{S}. \tag{5.38}$$

Furthermore, we have that

$$Cx = \begin{bmatrix} C_1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \quad Hx = 0, \quad 0 = \begin{bmatrix} H_1 & 0 \\ 0 & H_2 \\ C_1 & -C_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \tag{5.39}$$

and, in particular, $(Ax + Gd, A_1 x_1 + G_1 d_1) \in \pi_{\mathcal{X} \times \mathcal{X}_1}(\mathcal{S})$ and

$$Cx = C_1 x_1, \quad Hx = 0, \quad 0 = H_1 x_1. \tag{5.40}$$

Therefore, due to Proposition 5.2, $\pi_{\mathcal{X} \times \mathcal{X}_1}(\mathcal{S})$ is a simulation relation of Ξ by Ξ_1. As $\mathcal{S}$ is a full simulation relation, it follows that

$$\pi_{\mathcal{X}} \left(\pi_{\mathcal{X} \times \mathcal{X}_1}(\mathcal{S}) \right) = \pi_{\mathcal{X}}(\mathcal{S}) = \mathcal{V}, \tag{5.41}$$

which implies that $\pi_{\mathcal{X} \times \mathcal{X}_1}(\mathcal{S})$ is a full simulation relation and, thus, $\Xi \preccurlyeq \Xi_1$. Using a similar argument, we can show that $\pi_{\mathcal{X} \times \mathcal{X}_2}(\mathcal{S})$ is a full simulation relation of Ξ by Ξ_2, hence $\Xi \preccurlyeq \Xi_2$ as well. □

Remark 5.7. *Note that the second statement of Proposition 5.4 holds even when Ξ_1 and Ξ_2 have additional outputs different from the output of Ξ. This observation will be useful in the analysis of the series composition in Section 5.7.*

Recall that simulation defines a preorder. This allows us to refer to a largest and a smallest system in a given set of systems. In particular, a *largest* system in a set of systems $\mathfrak{X}$ is a system $\Xi_l \in \mathfrak{X}$ such that $\Xi \preccurlyeq \Xi_l$ for all $\Xi \in \mathfrak{X}$. Similarly, a *smallest* system is a system $\Xi_s \in \mathfrak{X}$ such that $\Xi_s \preccurlyeq \Xi$ for all $\Xi \in \mathfrak{X}$. Such a system does not necessarily exist and is not necessarily unique if it does exist. Nevertheless, since two systems are bisimilar if and only if they simulate each other, all largest (smallest) systems in a given set are bisimilar to each other.

With this in mind, Proposition 5.4 tells us that the meet $\Xi_1 \wedge \Xi_2$ is a largest system from the set of systems that are simulated by both Ξ_1 and Ξ_2. Indeed, since a system is simulated by itself, the second statement tells us that $\Xi_1 \wedge \Xi_2$ is simulated by both Ξ_1 and Ξ_2. On the other hand, it is easy to see that $\Xi \sim \Xi \wedge \Xi$ for all systems Ξ. Therefore, since simulation is transitive, the first statement tells us that $\Xi \preccurlyeq \Xi_1 \wedge \Xi_2$ for all systems Ξ that are simulated by both Ξ_1 and Ξ_2. In other words, up to bisimilarity, the meet $\Xi_1 \wedge \Xi_2$ is the greatest lower bound of the set $\{\Xi_1, \Xi_2\}$ with respect to simulation.

5.2 Contracts

In this section, we will define contracts and introduce the notion of contract implementation, which shows how a contract serves as a specification for the dynamic behaviour of a system. As the main result of this section, we will

derive necessary and sufficient conditions for contract implementation that can be verified efficiently.

To begin with, consider the system

$$\Sigma : \begin{cases} \dot{x} = Ax + Bu + Gd, \\ y = Cx, \end{cases} \tag{5.42}$$

with state $x \in \mathcal{X}$, input $u \in \mathcal{U}$, output $y \in \mathcal{Y}$, and driving variable $d \in \mathcal{D}$. We have omitted the explicit dependence on the time variable t for simplicity. We view Σ as an open system in which the input u and output y are external and interact with the environment, whereas the state x and the driving variable d are internal and do not interact with the environment. As a design goal, we are interested in specifying a desired dynamic behaviour of the external variables u and y. We will do this with the notion of a contract.

As explained in Chapter 1 and Chapter 2, a distinguishing feature of contracts is that they take the environment of a system explicitly into account. In particular, a contract specifies a desired behaviour of the system only when it is interconnected with a relevant environment. With this in mind, the environment of Σ is a linear system that generates inputs for it, that is, an *environment* E is a system of the form

$$\mathrm{E} : \begin{cases} \dot{x}_e = A_e x_e + G_e d_e, \\ u = C_e x_e, \\ 0 = H_e x_e, \end{cases} \tag{5.43}$$

with state $x_e \in \mathcal{X}_e$, driving variable $d_e \in \mathcal{D}_e$, output $u \in \mathcal{U}$, and consistent subspace $\mathcal{V}_e \subset \mathcal{X}_e$. The interconnection of E and Σ, denoted by $\mathrm{E} \wedge \Sigma$, is obtained by setting the output generated by E as input of Σ, as shown in Figure 5.1. This results in the system

$$\mathrm{E} \wedge \Sigma : \begin{cases} \begin{bmatrix} \dot{x}_e \\ \dot{x} \end{bmatrix} = \begin{bmatrix} A_e & 0 \\ BC_e & A \end{bmatrix} \begin{bmatrix} x_e \\ x \end{bmatrix} + \begin{bmatrix} G_e & 0 \\ 0 & G \end{bmatrix} \begin{bmatrix} d_e \\ d \end{bmatrix}, \\ u = \begin{bmatrix} C_e & 0 \end{bmatrix} \begin{bmatrix} x_e \\ x \end{bmatrix}, \\ y = \begin{bmatrix} 0 & C \end{bmatrix} \begin{bmatrix} x_e \\ x \end{bmatrix}, \\ 0 = \begin{bmatrix} H_e & 0 \end{bmatrix} \begin{bmatrix} x_e \\ x \end{bmatrix}. \end{cases} \tag{5.44}$$

We want our contracts to specify a desired dynamic behaviour of the interconnection $\mathrm{E} \wedge \Sigma$ for *any* relevant environment E. To this end, we will

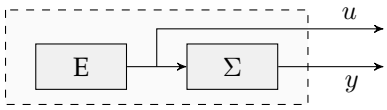

Figure 5.1: The interconnection $\mathrm{E} \wedge \Sigma$.

introduce two more systems. First, the *assumptions* A are a system of the form

$$\mathrm{A} : \begin{cases} \dot{x}_a = A_a x_a + G_a d_a, \\ u = C_a x_a, \\ 0 = H_a x_a, \end{cases} \tag{5.45}$$

with state $x_a \in \mathcal{X}_a$, driving variable $d_a \in \mathcal{D}_a$, output $u \in \mathcal{U}$, and consistent subspace $\mathcal{V}_a \subset \mathcal{X}_a$. The assumptions A have the same form as an environment E and they can be compared using the notion of simulation. Second, the *guarantees* Γ are a system of the form

$$\Gamma : \begin{cases} \dot{x}_g = A_g x_g + G_g d_g, \\ u = C_g^u x_g, \\ y = C_g^y x_g, \\ 0 = H_g x_g, \end{cases} \tag{5.46}$$

with state $x_g \in \mathcal{X}_g$, driving variable $d_g \in \mathcal{D}_g$, outputs $u \in \mathcal{U}$ and $y \in \mathcal{Y}$, and consistent subspace $\mathcal{V}_g \subset \mathcal{X}_g$. The guarantees Γ have the same form as the interconnection $\mathrm{E} \wedge \Sigma$ and they can be compared using simulation. Now, we define a contract as follows.

Definition 5.4. A contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ is a pair of assumptions and guarantees.

The following definition shows how a contract serves as a specification.

Definition 5.5. An environment E is *compatible* with $\mathcal{C} = (\mathrm{A}, \Gamma)$ if

$$\mathrm{E} \preccurlyeq \mathrm{A}. \tag{5.47}$$

A system Σ *implements* $\mathcal{C}$ if

$$\mathrm{E} \wedge \Sigma \preccurlyeq \Gamma, \tag{5.48}$$

for any environment E compatible with $\mathcal{C}$.

A contract serves as a specification through two aspects. First, the assumptions capture the available information about the dynamic behaviour of the environment in which the system is expected to operate, thus leading to a class of compatible environments. Second, the guarantees specify the desired dynamic behaviour of the system when interconnected with a compatible environment, thus leading to a class of implementations.

Remark 5.8. *We can allow an environment* E *to have additional outputs. As explained in Section 5.1, we will still interpret* $\mathrm{E} \preccurlyeq \mathrm{A}$ *by considering* u *as the only output of* E*. Allowing environments to have additional outputs will be useful in the analysis of the series composition in Section 5.7.*

Remark 5.9. *The following observation about condition* (5.48) *will be useful at several points throughout this chapter. Namely, note that* $\mathrm{E} \wedge \Sigma \preccurlyeq \Gamma$ *if and only if* $\mathrm{E} \wedge \Sigma \preccurlyeq \mathrm{E} \wedge \Gamma$*. Indeed, due to Proposition 5.4,* $\mathrm{E} \wedge \Sigma \preccurlyeq \Gamma$ *if* $\mathrm{E} \wedge \Sigma \preccurlyeq \mathrm{E} \wedge \Gamma$*. Conversely, if* $\mathrm{E} \wedge \Sigma \preccurlyeq \Gamma$ *and* $\mathcal{S}$ *is a full simulation relation of* $\mathrm{E} \wedge \Sigma$ *by* Γ*, then it is straightforward to show that the subspace* $\mathcal{S}' \subset \mathcal{X}_e \times \mathcal{X} \times \mathcal{X}_e \times \mathcal{X}_g$ *given by*

$$\mathcal{S}' = \{(x_e, x, x_e, x_g) \mid (x_e, x, x_g) \in \mathcal{S}\} \tag{5.49}$$

is a full simulation relation of $\mathrm{E} \wedge \Sigma$ *by* $\mathrm{E} \wedge \Gamma$*, hence* $\mathrm{E} \wedge \Sigma \preccurlyeq \mathrm{E} \wedge \Gamma$*. This holds even when* E *has additional outputs.*

We can check if a given system Σ implements a given contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ without having to construct all compatible environments. To show this, we will make use of the following lemma.

Lemma 5.5. *If the environments* E_1 *and* E_2 *are such that* $\mathrm{E}_1 \preccurlyeq \mathrm{E}_2$*, then*

$$\mathrm{E}_1 \wedge \Sigma \preccurlyeq \mathrm{E}_2 \wedge \Sigma. \tag{5.50}$$

Proof. Let E_1 and E_2 be given by (5.43) with the index e replaced by e_1 and e_2, respectively. Suppose that $\mathrm{E}_1 \preccurlyeq \mathrm{E}_2$ and let $\mathcal{S}_e$ be a full simulation relation of E_1 by E_2. Then, the subspace $\mathcal{S} \subset (\mathcal{X}_{e_1} \times \mathcal{X}) \times (\mathcal{X}_{e_2} \times \mathcal{X})$ defined by

$$\mathcal{S} = \{(x_{e_1}, x, x_{e_2}, x) \mid (x_{e_1}, x_{e_2}) \in \mathcal{S}_e\} \tag{5.51}$$

is a full simulation relation of $\mathrm{E}_1 \wedge \Sigma$ by $\mathrm{E}_2 \wedge \Sigma$. To show this, first note that the consistent subspace of $\mathrm{E}_1 \wedge \Sigma$ is given by $\mathcal{V}_{e_1} \times \mathcal{X}$, and the consistent subspace of $\mathrm{E}_2 \wedge \Sigma$ is given by $\mathcal{V}_{e_2} \times \mathcal{X}$. Since $\pi_{\mathcal{X}_{e_1}}(\mathcal{S}_e) = \mathcal{V}_{e_1}$ and $\pi_{\mathcal{X}_{e_2}}(\mathcal{S}_e) \subset \mathcal{V}_{e_2}$, it follows that $\pi_{\mathcal{X}_{e_1} \times \mathcal{X}}(\mathcal{S}) = \mathcal{V}_{e_1} \times \mathcal{X}$ and $\pi_{\mathcal{X}_{e_2} \times \mathcal{X}}(\mathcal{S}) \subset \mathcal{V}_{e_2} \times \mathcal{X}$.

Now, let $(x_{e_1}, x, x_{e_2}, x) \in \mathcal{S}$, and let $d_{e_1} \in \mathcal{D}_{e_1}$ and $d \in \mathcal{D}$ be such that

$$(A_{e_1} x_{e_1} + G_{e_1} d_{e_1}, Ax + BC_{e_1} x_{e_1} + Gd) \in \mathcal{V}_{e_1} \times \mathcal{X}, \tag{5.52}$$

where we recall the dynamics (5.44). For later reference, let

$$s = Ax + BC_{e_1} x_{e_1} + Gd. \tag{5.53}$$

As $(x_{e_1}, x_{e_2}) \in \mathcal{S}_e$ and $A_{e_1} x_{e_1} + G_{e_1} d_{e_1} \in \mathcal{V}_{e_1}$, Proposition 5.2 implies that there exists $d_{e_2} \in \mathcal{D}_{e_2}$ such that $(A_{e_1} x_{e_1} + G_{e_1} d_{e_1}, A_{e_2} x_{e_2} + G_{e_2} d_{e_2}) \in \mathcal{S}_e$ and

$$C_{e_1} x_{e_1} = C_{e_2} x_{e_2}, \quad H_{e_1} x_{e_1} = 0, \quad 0 = H_{e_2} x_{e_2}. \tag{5.54}$$

By definition of $\mathcal{S}$, it follows that

$$(A_{e_1}x_{e_1} + G_{e_1}d_{e_1}, s, A_{e_2}x_{e_2} + G_{e_2}d_{e_2}, s) \in \mathcal{S}. \tag{5.55}$$

On the other hand, due to (5.54), we can replace $C_{e_1}x_{e_1}$ by $C_{e_2}x_{e_2}$ in the definition of s to obtain $s = Ax + BC_{e_2}x_{e_2} + Gd$. Furthermore, we obtain

$$\begin{bmatrix} C_{e_1} & 0 \\ 0 & C \end{bmatrix}\begin{bmatrix} x_{e_1} \\ x \end{bmatrix} = \begin{bmatrix} C_{e_2} & 0 \\ 0 & C \end{bmatrix}\begin{bmatrix} x_{e_2} \\ x \end{bmatrix}, \quad \begin{bmatrix} H_{e_1} & 0 \end{bmatrix}\begin{bmatrix} x_{e_1} \\ x \end{bmatrix} = 0, \quad 0 = \begin{bmatrix} H_{e_2} & 0 \end{bmatrix}\begin{bmatrix} x_{e_2} \\ x \end{bmatrix},$$

which, together with (5.55) and Proposition 5.2, implies that $\mathcal{S}$ is a full simulation relation of $\mathrm{E}_1 \wedge \Sigma$ by $\mathrm{E}_2 \wedge \Sigma$ and, thus, $\mathrm{E}_1 \wedge \Sigma \preccurlyeq \mathrm{E}_2 \wedge \Sigma$. □

Remark 5.10. *Note that the statement of Lemma 5.5 is very similar to the first statement in Proposition 5.4. The difference is that* Σ *is not of the form* (5.1) *since it contains an external input, not only an external output.*

Remark 5.11. *As can be seen from the proof, the statement of Lemma 5.5 holds even if* E_1 *and* E_2 *have additional shared outputs. This observation will be useful in the analysis of the series composition in Section 5.7.*

Using Lemma 5.5, we obtain the following necessary and sufficient condition for contract implementation.

Theorem 5.1. *A system* Σ *implements the contract* $\mathcal{C} = (\mathrm{A}, \Gamma)$ *if and only if*

$$\mathrm{A} \wedge \Sigma \preccurlyeq \Gamma. \tag{5.56}$$

Proof. Suppose that Σ implements $\mathcal{C}$. Since A is an environment compatible with $\mathcal{C}$, it follows that (5.56) holds. Conversely, suppose that (5.56) holds and let E be compatible with $\mathcal{C}$, that is, $\mathrm{E} \preccurlyeq \mathrm{A}$. In view of Lemma 5.5, we have that $\mathrm{E} \wedge \Sigma \preccurlyeq \mathrm{A} \wedge \Sigma$, hence $\mathrm{E} \wedge \Sigma \preccurlyeq \Gamma$ because simulation is transitive. Since $\mathrm{E} \wedge \Sigma \preccurlyeq \Gamma$ for any E compatible with $\mathcal{C}$, we conclude that Σ implements $\mathcal{C}$. □

Remark 5.12. *Clearly, two contracts define the same class of compatible environments if and only if their assumptions are bisimilar. However, two contracts can define the same class of implementations even if their guarantees are not bisimilar. For instance,* $\mathcal{C} = (\mathrm{A}, \Gamma)$ *defines the same class of implementations as* $\mathcal{C}' = (\mathrm{A}, \mathrm{A} \wedge \Gamma)$*, where* $\mathrm{A} \wedge \Gamma$ *is the meet of* A *and* Γ*, that is,*

$$\mathrm{A} \wedge \Gamma : \begin{cases} \begin{bmatrix} \dot{x}_a \\ \dot{x}_g \end{bmatrix} = \begin{bmatrix} A_a & 0 \\ 0 & A_g \end{bmatrix}\begin{bmatrix} x_a \\ x_g \end{bmatrix} + \begin{bmatrix} G_a & 0 \\ 0 & G_g \end{bmatrix}\begin{bmatrix} d_a \\ d_g \end{bmatrix}, \\ u = \begin{bmatrix} C_a & 0 \end{bmatrix}\begin{bmatrix} x_a \\ x_g \end{bmatrix}, \\ y = \begin{bmatrix} 0 & C_g^y \end{bmatrix}\begin{bmatrix} x_a \\ x_g \end{bmatrix}, \\ 0 = \begin{bmatrix} H_a & 0 \\ 0 & H_g \\ C_a & -C_g^u \end{bmatrix}. \end{cases} \tag{5.57}$$

Indeed, due to Theorem 5.1, Σ implements $\mathcal{C}$ if and only if $\mathrm{A} \wedge \Sigma \preccurlyeq \Gamma$, which, due to Remark 5.9, holds if and only if $\mathrm{A} \wedge \Sigma \preccurlyeq \mathrm{A} \wedge \Gamma$, i.e., Σ implements $\mathcal{C}'$.

We stress that, as mentioned in Remark 5.4, simulation can be verified efficiently, hence Theorem 5.1 provides an efficient method for verifying whether a given system Σ implements a given contract $\mathcal{C}$. However, in the context of system design, we would like to *construct* an implementation for a given contract $\mathcal{C}$. Of course, before we attempt to do that, we should know whether an implementation even exists. This is the issue of contract consistency, which is discussed in the following section.

5.3 Consistency

In this section, we will consider the notion of contract consistency.

Definition 5.6. A contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ is *consistent* if there exists a system Σ that implements it.

In particular, we will find necessary and sufficient conditions for contract consistency and, in the process, we will obtain a systematic procedure for constructing an implementation of a given contract. The main result of this section is in Theorem 5.2, where we show that a contract is consistent if and only if a pair of subspaces that satisfy certain conditions exist. While the existence of one of these spaces is easy to verify, verifying the existence of the other requires additional work. Therefore, the secondary result in this section is concerned with verifying the existence of the latter.

We begin by noting that not every contract is consistent. To see this, note that u is an input of Σ, hence the dynamics of u in $\mathrm{A} \wedge \Sigma$ are restricted only by A. Therefore, in order to have $\mathrm{A} \wedge \Sigma \preccurlyeq \Gamma$ for some Σ, the restrictions that Γ imposes on the dynamics of u must already be imposed by A. Indeed, we will see that $\mathrm{A} \preccurlyeq \Gamma$ is a necessary condition for consistency, where $\mathrm{A} \preccurlyeq \Gamma$ if A is simulated by Γ with u as the only output, see Remark 5.5. However, this condition is not sufficient, and an extra (technical) condition needs to be satisfied. To show this, we will make use of the following lemma, whose proof can be found in Appendix B.9.

Lemma 5.6. *Suppose that the subspaces $\bar{\mathcal{R}} \subset \mathcal{R}$ satisfy*

$$A'\mathcal{R} \subset \mathcal{R} + \operatorname{im} B' + \operatorname{im} G', \tag{5.58}$$

$$A'\left(\bar{\mathcal{R}} \cap \ker C'\right) \subset \bar{\mathcal{R}} + \operatorname{im} G', \tag{5.59}$$

where A', B', C' and G' are matrices of appropriate dimensions. Then, there exist

matrices K', M', L' and N such that

$$(A' + G'K' + B'M')\mathcal{R} \subset \mathcal{R}, \tag{5.60}$$
$$(A' + G'K' - L'C')\bar{\mathcal{R}} \subset \bar{\mathcal{R}}, \tag{5.61}$$
$$(A' + G'K' + B'NC')\bar{\mathcal{R}} \subset \mathcal{R}. \tag{5.62}$$

Furthermore, if R is a matrix whose columns form a basis for $\mathcal{R}$, and $R^\dagger$ is such that $R^\dagger R = I$, then the matrices

$$K = R^\dagger(A' + G'K' - B'NC' + B'M' - L'C')R, \tag{5.63}$$
$$L = R^\dagger(B'N + L'), \tag{5.64}$$
$$M = (M' - NC')R, \tag{5.65}$$

are such that the subspace

$$\mathcal{S}' = \left\{(x + \bar{x}, w) \;\middle|\; x = Rw, \bar{x} \in \bar{\mathcal{R}}\right\} \tag{5.66}$$

satisfies

$$\begin{bmatrix} A' + B'NC' & B'M \\ LC' & K \end{bmatrix}\mathcal{S}' \subset \mathcal{S}' + \operatorname{im}\begin{bmatrix} G' \\ 0 \end{bmatrix}. \tag{5.67}$$

Lemma 5.6 is essential in proving the sufficiency of the conditions for consistency presented in the following theorem, whose proof can be found in Appendix B.10.

Theorem 5.2. *The contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ is consistent if and only if there exist subspaces $\mathcal{R} \subset \mathcal{X}_a \times \mathcal{X}_g$ and $\bar{\mathcal{R}} \subset \mathcal{X}_a \times \mathcal{X}_g$ such that $\bar{\mathcal{R}} \subset \mathcal{R}$ and the following conditions are satisfied:*

1. *$\mathcal{R}$ is such that $\pi_{\mathcal{X}_a}(\mathcal{R}) = \mathcal{V}_a$ and*

$$\begin{bmatrix} A_a & 0 \\ 0 & A_g \end{bmatrix}\mathcal{R} \subset \mathcal{R} + \operatorname{im}\begin{bmatrix} G_a & 0 \\ 0 & G_g \end{bmatrix}, \tag{5.68}$$
$$\mathcal{R} \subset \ker\begin{bmatrix} C_a & -C_g^u \\ H_a & 0 \\ 0 & H_g \end{bmatrix}. \tag{5.69}$$

2. *$\bar{\mathcal{R}}$ is such that $\pi_{\mathcal{X}_a}(\bar{\mathcal{R}}) = \mathcal{V}_a$ and*

$$\begin{bmatrix} A_a & 0 \\ 0 & A_g \end{bmatrix}\left(\bar{\mathcal{R}} \cap \ker\begin{bmatrix} C_a & 0 \end{bmatrix}\right) \subset \bar{\mathcal{R}} + \operatorname{im}\begin{bmatrix} G_a & 0 \\ 0 & G_g \end{bmatrix}, \tag{5.70}$$
$$\begin{bmatrix} \operatorname{im} G_a \cap \mathcal{V}_a \\ 0 \end{bmatrix} \subset \bar{\mathcal{R}} + \operatorname{im}\begin{bmatrix} 0 \\ G_g \end{bmatrix}, \tag{5.71}$$
$$\bar{\mathcal{R}} \subset \ker\begin{bmatrix} 0 & -C_g^y \end{bmatrix}. \tag{5.72}$$

Remark 5.13. *Suppose that $\bar{\mathcal{R}}$ and $\mathcal{R}$ satisfy the conditions in Theorem 5.2. Since $\bar{\mathcal{R}} \subset \mathcal{R}$,* (5.71) *holds with $\bar{\mathcal{R}}$ replaced by $\mathcal{R}$. Together with* (5.68) *and* (5.69)*, this implies that $\mathcal{R}$ is a simulation relation of* A *by* Γ*. Moreover, as $\pi_{\mathcal{X}_a}(\mathcal{R}) = \mathcal{V}_a$, it follows that $\mathcal{R}$ is a full simulation relation and, thus,* $\mathrm{A} \preccurlyeq \Gamma$ *is a necessary condition for consistency, which confirms our intuition.*

Theorem 5.2 does not immediately provide a systematic procedure for verifying consistency. Indeed, we have just translated the problem of finding an implementation Σ of $\mathcal{C} = (\mathrm{A}, \Gamma)$ to the problem of finding subspaces $\bar{\mathcal{R}}$ and $\mathcal{R}$ that satisfy the conditions in Theorem 5.2. Therefore, we will devote the rest of this section to deriving a systematic procedure for the construction of subspaces $\mathcal{R}$ and $\bar{\mathcal{R}}$ that satisfy the conditions in Theorem 5.2. Note that, since the proof of Theorem 5.2 is constructive, being able to construct $\mathcal{R}$ and $\bar{\mathcal{R}}$ will also allow us to construct an implementation.

To this end, as mentioned in Remark 5.13, $\mathcal{R}$ is a full simulation relation of A by Γ, which can be constructed using the invariant subspace algorithm, see Remark 5.4. In particular, we can find the largest subspace $\mathcal{R}$ that satisfies (5.68) and (5.69), and then verify that $\pi_{\mathcal{X}_a}(\mathcal{R}) = \mathcal{V}_a$. Now, given $\mathcal{R}$ that satisfies the first condition in Theorem 5.2, we turn to finding a subspace $\bar{\mathcal{R}} \subset \mathcal{R}$ that satisfies the second condition. This requires more effort because, unlike $\mathcal{R}$, $\bar{\mathcal{R}}$ is not controlled invariant and we cannot use the invariant subspace algorithm.

Instead, we will exploit the structure of the matrices involved in the second condition of Theorem 5.2 to derive a set of linear equations that can be solved to obtain a basis for an appropriate $\bar{\mathcal{R}}$. First, we state and prove the following intermediate result.

Lemma 5.7. *Suppose that the matrix F_a is such that*

$$(A_a + G_a F_a)\mathcal{V}_a \subset \mathcal{V}_a. \tag{5.73}$$

Then $\bar{\mathcal{R}}$ satisfies the second condition in Theorem 5.2 if and only if it satisfies the same condition with (5.70) *replaced by*

$$\begin{bmatrix} A_a + G_a F_a & 0 \\ 0 & A_g \end{bmatrix} \left(\bar{\mathcal{R}} \cap \ker \begin{bmatrix} C_a & 0 \end{bmatrix}\right) \subset \bar{\mathcal{R}} + \operatorname{im} \begin{bmatrix} 0 \\ G_g \end{bmatrix}. \tag{5.74}$$

Proof. It is easily seen that (5.74) implies (5.70) for any matrix F_a. Therefore, we only need to prove that $\bar{\mathcal{R}}$ satisfies (5.74) if it satisfies the second condition of Theorem 5.2. To this end, suppose that $\bar{\mathcal{R}}$ satisfies the second condition in Theorem 5.2. Let $(\bar{x}_a, \bar{x}_g) \in \bar{\mathcal{R}} \cap \ker \begin{bmatrix} C_a & 0 \end{bmatrix}$ and note that, due to (5.70), there exist $d_a \in \mathcal{D}_a$ and $d_g \in \mathcal{D}_g$ such that

$$\begin{bmatrix} \bar{r}_a \\ \bar{r}_g \end{bmatrix} = \begin{bmatrix} A_a \bar{x}_a - G_a d_a \\ A_g \bar{x}_g - G_g d_g \end{bmatrix} \in \bar{\mathcal{R}}. \tag{5.75}$$

With this in mind, we can write

$$\begin{bmatrix}(A_a + G_a F_a)\bar{x}_a \\ A_g \bar{x}_g\end{bmatrix} = \begin{bmatrix}\bar{r}_a \\ \bar{r}_g\end{bmatrix} + \begin{bmatrix}G_a(d_a + F_a \bar{x}_a) \\ G_g d_g\end{bmatrix}. \tag{5.76}$$

Since $\pi_{\mathcal{X}_a}(\bar{\mathcal{R}}) = \mathcal{V}_a$ and F_a satisfies (5.73), it follows that $\bar{r}_a \in \mathcal{V}_a$ and $(A_a + G_a F_a)\bar{x}_a \in \mathcal{V}_a$, hence $G_a(d_a + F_a \bar{x}_a) \in \mathcal{V}_a$. But then (5.71) implies that there exists $(\bar{r}'_a, \bar{r}'_g) \in \bar{\mathcal{R}}$ and $d'_g \in \mathcal{D}_g$ such that

$$\begin{bmatrix}G_a(d_a + F_a \bar{x}_a) \\ 0\end{bmatrix} = \begin{bmatrix}\bar{r}'_a \\ \bar{r}'_g\end{bmatrix} + \begin{bmatrix}0 \\ G_g d'_g\end{bmatrix}. \tag{5.77}$$

Using (5.76) and (5.77), we obtain

$$\begin{bmatrix}(A_a + G_a F_a)\bar{x}_a \\ A_g \bar{x}_g\end{bmatrix} = \begin{bmatrix}\bar{r}_a + \bar{r}'_a \\ \bar{r}_g + \bar{r}'_g\end{bmatrix} + \begin{bmatrix}0 \\ G_g\end{bmatrix}(d_g + d'_g), \tag{5.78}$$

which shows that (5.74) holds, as desired. □

Note that the existence of F_a such that (5.73) holds is guaranteed since the consistent subspace $\mathcal{V}_a$ is such that $A_a \mathcal{V}_a \subset \mathcal{V}_a + \operatorname{im} G_a$, see [68, Theorem 4.2]. Now, the following lemma, whose proof can be found in Appendix B.11, shows that a suitable $\bar{\mathcal{R}}$ can be obtained by solving a set of linear matrix equations.

Lemma 5.8. *Suppose that $\mathcal{R} \subset \mathcal{X}_a \times \mathcal{X}_g$ satisfies the first condition in Theorem 5.2 and let $R_a^\perp$ and $R_g^\perp$ be such that*

$$\ker \begin{bmatrix}R_a^\perp & R_g^\perp\end{bmatrix} = \mathcal{R}. \tag{5.79}$$

Let $\bar{\mathcal{R}}_g^0$ be the largest subspace satisfying

$$A_g \bar{\mathcal{R}}_g^0 \subset \bar{\mathcal{R}}_g^0 + \operatorname{im} G_g, \quad \bar{\mathcal{R}}_g^0 \subset \ker \begin{bmatrix}R_g^\perp \\ -C_g^y\end{bmatrix}. \tag{5.80}$$

Let $\bar{R}_g^0$, V_a, $C_a^{\mathcal{V}}$ and $G_a^{\mathcal{V}}$ be matrices whose columns form bases for $\bar{\mathcal{R}}_g^0$, $\mathcal{V}_a$, $\ker C_a V_a$ and $\operatorname{im} G_a \cap \mathcal{V}_a$, respectively. Furthermore, let F_a be a matrix such that (5.73) holds, and let $V_a^\dagger$ be such that $V_a^\dagger V_a = I$. Then there exists a subspace $\bar{\mathcal{R}} \subset \mathcal{R}$ that satisfies the second condition in Theorem 5.2 if and only if there exist matrices $\bar{R}_g$, W, X, Y and Z such that

$$A_g \bar{R}_g C_a^{\mathcal{V}} = \bar{R}_g V_a^\dagger (A_a + G_a F_a) V_a C_a^{\mathcal{V}} + \bar{R}_g^0 X + G_g Y, \tag{5.81}$$

$$0 = \bar{R}_g V_a^\dagger G_a^{\mathcal{V}} + \bar{R}_g^0 W + G_g Z, \tag{5.82}$$

$$0 = \begin{bmatrix}R_a^\perp & R_g^\perp \\ 0 & -C_g^y\end{bmatrix}\begin{bmatrix}V_a \\ \bar{R}_g\end{bmatrix}. \tag{5.83}$$

In such a case, a suitable $\bar{\mathcal{R}}$ is given by

$$\bar{\mathcal{R}} = \operatorname{im} \begin{bmatrix}V_a & 0 \\ \bar{R}_g & \bar{R}_g^0\end{bmatrix}. \tag{5.84}$$

Given a subspace $\mathcal{R} \subset \mathcal{X}_a \times \mathcal{X}_g$, Lemma 5.8 provides an efficient procedure to verify the existence of $\bar{\mathcal{R}} \subset \mathcal{R}$ that satisfies the second condition of Theorem 5.2. Indeed, the subspaces $\bar{\mathcal{R}}_g^0$ and $\mathcal{V}_a$ can be computed efficiently using the invariant subspace algorithm, and all required matrices can be computed using elementary linear algebra techniques. Then the equations (5.81)-(5.83) are linear in the unknowns $\bar{R}_g^0$, W, X, Y and Z, hence they can easily be solved to obtain an appropriate $\bar{R}_g^0$ and corresponding $\bar{\mathcal{R}}$. Of course, the outcome of this procedure depends on the given $\mathcal{R}$, but this dependence can be avoided if we take $\mathcal{R}$ to be the *largest* subspace that satisfies the first condition in Theorem 5.2, which can, again, be done efficiently using the invariant subspace algorithm.

Remark 5.14. *On an abstract technical level, the problem of designing an implementation for a given contract is similar to the problem of controller synthesis for bisimilarity [19], see also [17]. To see this, note that designing an implementation amounts to constructing* Σ *such that* $\mathrm{A} \wedge \Sigma \preccurlyeq \Gamma$. *We can interpret* A *as a plant system,* Γ *as a specification system, and* Σ *as a controller. Then, the problem of controller synthesis for bisimilarity is similar to the problem of designing an implementation, with the main difference being the stronger requirement that* $\mathrm{A} \wedge \Sigma \sim \Gamma$. *Another notable difference is in the system classes to which* A, Σ *and* Γ *belong. Nevertheless, the results on control for bisimilarity can help tackle problems related to contract-based design.*

We conclude this section with Algorithm 1, which outlines a systematic procedure for verifying if a given contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ is consistent and constructing an implementation if it is. In particular, if Algorithm 1 terminates at step 2 or step 4, then we conclude that $\mathcal{C}$ is not consistent. Otherwise, $\mathcal{C}$ is consistent and the system Σ obtained in step 8 is an implementation.

Algorithm 1 Constructing an implementation for $\mathcal{C} = (\mathrm{A}, \Gamma)$

1: Construct the largest $\mathcal{R}$ that satisfies (5.68) and (5.69).
2: **if** $\pi_{\mathcal{X}_a}(\mathcal{R}) \neq \mathcal{V}_a$ **then** terminate.
3: Construct $R_a^\perp$, $R_g^\perp$, $\bar{R}_g^0$, V_a, $C_a^{\mathcal{V}}$, $G_a^{\mathcal{V}}$ and F_a as in Lemma 5.8.
4: **if** $\nexists \bar{R}_g$ satisfying (5.81)–(5.83) **then** terminate.
5: Construct $\bar{R}_g$ satisfying (5.81)–(5.83) and let $\bar{\mathcal{R}}$ be as in (5.84).
6: Define $B' = 0$, and A', G' and C' as in (B.161).
7: Construct R, K and L as in Lemma 5.6.
8: Define Σ as in (5.42) with

$$A = K, \quad B = L, \quad G = 0, \quad C = \begin{bmatrix} 0 & C_g^y \end{bmatrix} R$$

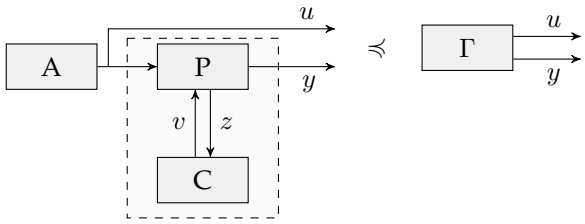

Figure 5.2: Control of P for implementation of $\mathcal{C} = (\mathrm{A}, \Gamma)$.

5.4 Control for implementation

In this section, we will consider the problem of control for implementation. In particular, we will consider the situation where we have a given plant system and a specification for it in the form of a given contract. The plant system will not necessarily implement the contract but will admit a control input so that implementation of the contract might be enforced using appropriate control. With this in mind, we will find necessary and sufficient conditions for the existence of a controller that turns a given plant system into an implementation of a given contract. In the process, we will also develop a procedure for constructing an appropriate controller if it exists. The main result of this section is in Theorem 5.3, where we show that such a controller exists if and only if a pair of subspaces that satisfy certain conditions exist. These conditions resemble the conditions for consistency in Theorem 5.3 and, thus, can be verified in a similar manner.

To begin with, consider the plant system

$$\mathrm{P}: \begin{cases} \dot{x}_p = A_p x_p + B_p^u u + B_p^v v, \\ y = C_p^y x_p, \\ z = C_p^z x_p, \end{cases} \tag{5.85}$$

with state $x_p \in \mathcal{X}_p$, external input $u \in \mathcal{U}$, external output $y \in \mathcal{Y}$, control input $v \in \mathcal{V}$, and measured output $z \in \mathcal{Z}$. Suppose that we are given the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$. We want to find a controller C for the plant P such that the controlled plant $\mathrm{P} \wedge \mathrm{C}$ implements $\mathcal{C}$, as shown in Figure 5.2. Of course, the existence of such a controller is not guaranteed for arbitrary contract $\mathcal{C}$ and plant P. Therefore, as a first step, we will find conditions under which such a controller exists. To this end, consider a controller of the form

$$\mathrm{C}: \begin{cases} \dot{w} = Kw + Lz, \\ v = Mw + Nz, \end{cases} \tag{5.86}$$

with state $w \in \mathcal{W}$, input $z \in \mathcal{Z}$ and output $v \in \mathcal{V}$. The interconnection of the

plant P and the controller C is given by

$$\mathrm{P} \wedge \mathrm{C} : \begin{cases} \begin{bmatrix} \dot{x}_p \\ \dot{w} \end{bmatrix} = \begin{bmatrix} A_p + B_p^v N C_p^z & B_p^v M \\ L C_p^z & K \end{bmatrix} \begin{bmatrix} x_p \\ w \end{bmatrix} + \begin{bmatrix} B_p^u \\ 0 \end{bmatrix} u, \\ \quad y = \begin{bmatrix} C_p^y & 0 \end{bmatrix} \begin{bmatrix} x_p \\ w \end{bmatrix}. \end{cases} \tag{5.87}$$

Finding conditions for the existence of a controller C such that $\mathrm{P} \wedge \mathrm{C}$ implements $\mathcal{C}$ turns out to be very similar to finding conditions for contract consistency. Indeed, by adapting the ideas in the proof of Theorem 5.2, we can derive necessary and sufficient conditions for the existence of an appropriate controller C. This is the content of the following theorem, whose proof can be found in Appendix B.12.

Theorem 5.3. *There exists a controller* C *such that* $\mathrm{P} \wedge \mathrm{C}$ *implements* $\mathcal{C} = (\mathrm{A}, \Gamma)$ *if and only if there exist subspaces* $\mathcal{R} \subset \mathcal{X}_a \times \mathcal{X}_p \times \mathcal{X}_g$ *and* $\bar{\mathcal{R}} \subset \mathcal{X}_a \times \mathcal{X}_p \times \mathcal{X}_g$ *such that* $\bar{\mathcal{R}} \subset \mathcal{R}$ *and the following conditions are satisfied:*

1. *$\mathcal{R}$ is such that $\pi_{\mathcal{X}_a \times \mathcal{X}_p}(\mathcal{R}) = \mathcal{V}_a \times \mathcal{X}_p$ and*

$$\begin{bmatrix} A_a & 0 & 0 \\ B_p^u C_a & A_p & 0 \\ 0 & 0 & A_g \end{bmatrix} \mathcal{R} \subset \mathcal{R} + \operatorname{im} \begin{bmatrix} 0 & G_a & 0 \\ B_p^v & 0 & 0 \\ 0 & 0 & G_g \end{bmatrix}, \tag{5.88}$$

$$\mathcal{R} \subset \ker \begin{bmatrix} C_a & 0 & -C_g^u \\ 0 & C_p^y & -C_g^y \\ H_a & 0 & 0 \\ 0 & 0 & H_g \end{bmatrix}. \tag{5.89}$$

2. *$\bar{\mathcal{R}}$ is such that $\pi_{\mathcal{X}_a \times \mathcal{X}_p}(\bar{\mathcal{R}}) = \mathcal{V}_a \times \mathcal{X}_p$ and*

$$\begin{bmatrix} A_a & 0 & 0 \\ B_p^u C_a & A_p & 0 \\ 0 & 0 & A_g \end{bmatrix} \left(\bar{\mathcal{R}} \cap \ker \begin{bmatrix} 0 & C_p^z & 0 \end{bmatrix}\right) \subset \bar{\mathcal{R}} + \operatorname{im} \begin{bmatrix} G_a & 0 \\ 0 & 0 \\ 0 & G_g \end{bmatrix}, \tag{5.90}$$

$$\begin{bmatrix} \operatorname{im} G_a \cap \mathcal{V}_a \\ 0 \\ 0 \end{bmatrix} \subset \bar{\mathcal{R}} + \operatorname{im} \begin{bmatrix} 0 \\ 0 \\ G_g \end{bmatrix}. \tag{5.91}$$

The conditions in Theorem 5.3 closely resemble the conditions in Theorem 5.2. Therefore, we can use the ideas in Section 5.3 to obtain a systematic procedure for the construction of subspaces $\mathcal{R}$ and $\bar{\mathcal{R}}$ that satisfy the conditions in Theorem 5.3, given that such spaces exist. To this end, a subspace $\mathcal{R}$ that satisfies the first condition in Theorem 5.3 can be constructed using the invariant subspace algorithm. In particular, we can find the largest subspace $\mathcal{R}$ that satisfies (5.88) and (5.89) and then verify that $\pi_{\mathcal{X}_a \times \mathcal{X}_p}(\mathcal{R}) = \mathcal{V}_a \times \mathcal{X}_p$.

On the other hand, a subspace $\bar{\mathcal{R}} \subset \mathcal{R}$ that satisfies the second condition in Theorem 5.3 can be constructed using the ideas in Lemma 5.8. Indeed, we obtain (5.90) and (5.91) from (5.70) and (5.71), respectively, by replacing

$$A_a \longleftarrow \begin{bmatrix} A_a & 0 \\ B_p^u C_a & A_p \end{bmatrix}, \qquad G_a \longleftarrow \begin{bmatrix} G_a \\ 0 \end{bmatrix}, \tag{5.92}$$

$$C_a \longleftarrow \begin{bmatrix} 0 & C_p^z \end{bmatrix}, \qquad \mathcal{V}_a \longleftarrow \mathcal{V}_a \times \mathcal{X}_p, \tag{5.93}$$

where $X \longleftarrow Y$ indicates that X is replaced by Y. Furthermore, (5.72) is vacuously satisfied by replacing

$$C_g^y \longleftarrow 0. \tag{5.94}$$

Therefore, $\bar{\mathcal{R}}$ satisfies the second condition in Theorem 5.3 if and only if it satisfies the second condition in Theorem 5.2 with the aforementioned replacements. This means that Lemma 5.8 can be used to obtain a subspace $\bar{\mathcal{R}} \subset \mathcal{R}$ that satisfies the second condition of Theorem 5.3. Note that the same replacements must also be made in Lemma 5.7 to obtain the correct matrix F_a in Lemma 5.8.

The sufficiency part of the proof of Theorem 8 tells us how to construct an appropriate controller C from $\mathcal{R}$ and $\bar{\mathcal{R}}$. Using this, we obtain Algorithm 2, which outlines a systematic procedure that addresses the following two objectives. First, steps 1-5 can be used to verify the existence of a controller C that turns a given plant system P into an implementation of a given contract $\mathcal{C} = (\mathrm{A}, \Gamma)$. In particular, if the algorithm does not terminate in steps 2 or 4, then such a controller exists. Second, steps 6-10 can be used to construct such a controller if it exists.

Algorithm 2 Constructing a controller for P that achieves implementation of $\mathcal{C} = (\mathrm{A}, \Gamma)$

1: Construct the largest $\mathcal{R}$ that satisfies (5.88) and (5.89).
2: **if** $\pi_{\mathcal{X}_a}(\mathcal{R}) \neq \mathcal{V}_a \times \mathcal{X}_p$ **then** terminate.
3: Make the replacements (5.92), (5.93) and (5.94).
4: Construct $R_a^{\perp}$, $R_g^{\perp}$, $\bar{R}_g^0$, V_a, $C_a^{\mathcal{V}}$, $G_a^{\mathcal{V}}$ and F_a as in Lemma 5.8.
5: **if** $\nexists \bar{R}_g$ satisfying (5.81)–(5.83) **then** terminate.
6: Construct $\bar{R}_g$ satisfying (5.81)–(5.83), and let $\bar{\mathcal{R}}$ be as in (5.84).
7: Unmake the replacements (5.92), (5.93) and (5.94).
8: Define A', B', G' and C' as in (B.205) and (B.206).
9: Construct R, K, L, M and N as in Lemma 5.6.
10: Define C as in (5.86).

Remark 5.15. *We have assumed that the controller* C *has access only to the control output* z*. However, there might be cases where the external input* u *of the plant is*

also available. In such a case, we want to find a controller

$$\mathrm{C}: \begin{cases} \dot{w} = Kw + L_u u + L_z z, \\ v = Mw + N_u u + N_z z, \end{cases} \tag{5.95}$$

such that $\mathrm{P} \wedge \mathrm{C}$ *implements* $\mathcal{C} = (\mathrm{A}, \Gamma)$*. This amounts to finding* C *such that* $\mathrm{A} \wedge (\mathrm{P} \wedge \mathrm{C}) \preccurlyeq \Gamma$*, hence we can think of* C *being a controller for* $\mathrm{A} \wedge \mathrm{P}$*, which has both* u *and* z *as outputs. Consequently, a controller* C *of the form* (5.95) *such that* $\mathrm{P} \wedge \mathrm{C}$ *implements* $\mathcal{C} = (\mathrm{A}, \Gamma)$ *exists if and only if the conditions in Theorem 5.3 are satisfied with* (5.90) *replaced by*

$$\begin{bmatrix} A_a & 0 & 0 \\ B_p^u C_a & A_p & 0 \\ 0 & 0 & A_g \end{bmatrix} \left(\bar{\mathcal{R}} \cap \ker \begin{bmatrix} C_a & 0 & 0 \\ 0 & C_p^z & 0 \end{bmatrix} \right) \subset \bar{\mathcal{R}} + \operatorname{im} \begin{bmatrix} G_a & 0 \\ 0 & 0 \\ 0 & G_g \end{bmatrix}. \tag{5.96}$$

Note that (5.96) *is less restrictive than* (5.90)*, which is to be expected since the class of controllers of the form* (5.95) *is larger than those of the form* (5.86)*. To obtain* C *of the form* (5.95)*, the matrices* L *and* N *obtained in the proof of Theorem 5.3 should be partitioned as*

$$L = \begin{bmatrix} L_u & L_z \end{bmatrix}, \quad N = \begin{bmatrix} N_u & N_z \end{bmatrix}. \tag{5.97}$$

Remark 5.16. *If we can find* $\bar{\mathcal{R}} = \mathcal{R}$ *such that the conditions in Theorem 5.3 are satisfied, then the controller* C *can be static. Indeed, due to [68, Theorem 6.2], if* (5.88) *and* (5.90) *hold for* $\mathcal{R} = \bar{\mathcal{R}}$ *, then we can find a matrix* N *such that*

$$\left(\begin{bmatrix} A_a & 0 & 0 \\ B_p^u C_a & A_p & 0 \\ 0 & 0 & A_g \end{bmatrix} + \begin{bmatrix} 0 \\ B_p^v \\ 0 \end{bmatrix} N \begin{bmatrix} 0 & C_p^z & 0 \end{bmatrix} \right) \mathcal{R} \subset \mathcal{R} + \operatorname{im} \begin{bmatrix} G_a & 0 \\ 0 & 0 \\ 0 & G_g \end{bmatrix}, \tag{5.98}$$

which implies that the static controller

$$\mathrm{C}: v = Nz \tag{5.99}$$

is such that $\mathcal{R}$ *is a full simulation relation of* $\mathrm{A} \wedge (\mathrm{P} \wedge \mathrm{C})$ *by* Γ*, i.e.,* $\mathrm{P} \wedge \mathrm{C}$ *implements* $\mathcal{C} = (\mathrm{A}, \Gamma)$*.*

5.5 Illustrative example

In this section, we will demonstrate how Theorem 5.3 can be used in practice with a simple example of a vehicle following system. Consider two vehicles: the leader E and the follower P, as shown in Figure 5.3. We assume that the positions p_{E}, p_{P}, and velocities v_{E}, v_{P} of E and P, respectively, are external variables that are available for measurement. Our goal is to design a controller C

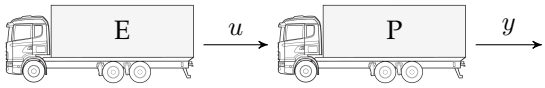

Figure 5.3: A vehicle following system.

for P such that the resulting controlled vehicle P ∧ C achieves tracking of the so-called headway spacing policy

$$p_{\mathrm{E}} - p_{\mathrm{P}} = h v_{\mathrm{P}}, \tag{5.100}$$

where $h > 0$ is a constant parameter. In other words, we want $p_{\mathrm{E}} - p_{\mathrm{P}} - h v_{\mathrm{P}}$ to asymptotically converge to 0. Note that this would be the case if

$$\tfrac{\mathrm{d}}{\mathrm{d}t}\left(p_{\mathrm{E}} - p_{\mathrm{P}} - h v_{\mathrm{P}}\right) = -k\left(p_{\mathrm{E}} - p_{\mathrm{P}} - h v_{\mathrm{P}}\right) \tag{5.101}$$

for some positive constant $k > 0$.

We can express this specification for the controlled vehicle P ∧ C in the form of a contract. To this end, let

$$u = \begin{bmatrix} p_{\mathrm{E}} \\ v_{\mathrm{E}} \end{bmatrix} \quad \text{and} \quad y = \begin{bmatrix} p_{\mathrm{P}} \\ v_{\mathrm{P}} \end{bmatrix} \tag{5.102}$$

be the external input and output of P, respectively. We will model P as a simple mechanical system with unit mass, that is, P is given by (5.85) with

$$A_p = A, \quad B_p^v = B, \quad B_p^u = 0, \quad C_p^z = C_p^y = I, \tag{5.103}$$

where

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{5.104}$$

Note that $B_p^u = 0$, i.e., the external input u does not directly influence the dynamics of P. Instead, the controller C will use the external input u, as well as the measured output z, to provide an appropriate control input v to P. We assume that the external input u indeed represents the position and velocity of E, that is, the assumptions A are given by (5.45) with

$$A_a = A, \quad G_a = B, \quad C_a = I, \quad H_a = 0, \tag{5.105}$$

and they capture the kinematic relationship between the entries of u. On the other hand, satisfaction of (5.101) is captured by the guarantees Γ given by (5.46) with

$$A_g = \begin{bmatrix} A & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & -k \end{bmatrix}, \qquad G_g = \begin{bmatrix} B & 0 \\ 0 & B \\ 0 & 0 \end{bmatrix}, \tag{5.106}$$

$$H_g = \begin{bmatrix} H_u & H_y & -1 \end{bmatrix}, \qquad \begin{bmatrix} C_g^u \\ C_g^y \end{bmatrix} = \begin{bmatrix} I & 0 & 0 \\ 0 & I & 0 \end{bmatrix}, \tag{5.107}$$

where

$$H_u = -\begin{bmatrix}1 & 0\end{bmatrix}, \quad H_y = \begin{bmatrix}1 & h\end{bmatrix}. \tag{5.108}$$

Note that the guarantees Γ require both u and y to be vectors of positions and velocities, in addition to enforcing the desired spacing error dynamics (5.101). Now, A and Γ are such that the specification for $\mathrm{P} \wedge \mathrm{C}$ is captured by the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$. Therefore, our goal is to find a controller C of the form (5.95) (both u and z are available for measurement) such that the controlled vehicle $\mathrm{P} \wedge \mathrm{C}$ implements $\mathcal{C}$.

Due to Theorem 5.3 and Remark 5.15, such a controller exists if and only if there exists a subspace $\mathcal{R} \subset \mathcal{X}_a \times \mathcal{X}_p \times \mathcal{X}_g$ that satisfies $\pi_{\mathcal{X}_a \times \mathcal{X}_p}(\mathcal{R}) = \mathcal{X}_a \times \mathcal{X}_p$, (5.88) and (5.89), and a subspace $\bar{\mathcal{R}} \subset \mathcal{R}$ that satisfies $\pi_{\mathcal{X}_a \times \mathcal{X}_p}(\bar{\mathcal{R}}) = \mathcal{X}_a \times \mathcal{X}_p$, (5.96) and (5.91). With this in mind, consider $\mathcal{R} = \operatorname{im} R$, where

$$R = \left[\begin{array}{cc} I & 0 \\ \hdashline 0 & I \\ \hdashline I & 0 \\ 0 & I \\ -H_u & -H_y \end{array}\right]. \tag{5.109}$$

Clearly, $\mathcal{R}$ satisfies $\pi_{\mathcal{X}_a \times \mathcal{X}_p}(\mathcal{R}) = \mathcal{X}_a \times \mathcal{X}_p$ and (5.89) (in fact, with equality instead of inclusion). To show that $\mathcal{R}$ satisfies (5.88) as well, consider the matrices

$$N_u = \frac{1}{h}\begin{bmatrix}k & 1\end{bmatrix}, \quad N_z = -\frac{1}{h}\begin{bmatrix}k & hk+1\end{bmatrix}, \tag{5.110}$$

and note that

$$-k\begin{bmatrix}H_u & H_y\end{bmatrix} = \begin{bmatrix}H_u & H_y\end{bmatrix}\begin{bmatrix}A & 0 \\ BN_u & A+BN_z\end{bmatrix}. \tag{5.111}$$

This implies that

$$\left[\begin{array}{c|c|cc|c} A & 0 & 0 & 0 & 0 \\ \hline 0 & A & 0 & 0 & 0 \\ \hline 0 & 0 & A & 0 & 0 \\ 0 & 0 & 0 & A & 0 \\ 0 & 0 & 0 & 0 & -k \end{array}\right] R = R\begin{bmatrix}A & 0 \\ BN_u & A+BN_z\end{bmatrix} - \left[\begin{array}{c|c|cc} 0 & B & 0 & 0 \\ \hline B & 0 & 0 & 0 \\ \hline 0 & 0 & B & 0 \\ 0 & 0 & 0 & B \\ 0 & 0 & 0 & 0 \end{array}\right]\begin{bmatrix}N_u & N_z \\ 0 & 0 \\ 0 & 0 \\ N_u & N_z\end{bmatrix}, \tag{5.112}$$

which shows that (5.88) holds. Now, let $\bar{\mathcal{R}} = \mathcal{R} = \operatorname{im} R$. It is easily seen that $\pi_{\mathcal{X}_a \times \mathcal{X}_p}(\bar{\mathcal{R}}) = \mathcal{X}_a \times \mathcal{X}_p$ and

$$\bar{\mathcal{R}} \cap \ker \left[\begin{array}{c:c:c:c:c} I & 0 & 0 & 0 & 0 \\ \hdashline 0 & I & 0 & 0 & 0 \end{array}\right] = \{0\}, \tag{5.113}$$

hence (5.96) holds trivially. Furthermore, (5.91) holds because

$$\left[\begin{array}{c} B \\ \hdashline 0 \\ \hdashline 0 \\ 0 \\ 0 \end{array}\right] = R \begin{bmatrix} B \\ 0 \end{bmatrix} + \left[\begin{array}{cc} 0 & 0 \\ \hdashline 0 & 0 \\ \hdashline B & 0 \\ 0 & B \\ 0 & 0 \end{array}\right] \begin{bmatrix} -1 \\ 0 \end{bmatrix}. \tag{5.114}$$

Consequently, we have found $\bar{\mathcal{R}} = \mathcal{R}$ such that the conditions in Theorem 5.3 (according to Remark 5.15) are satisfied. In view of Remark 5.16, this means that there exists a *static* controller C such that P $\wedge$ C implements $\mathcal{C}$. To find C, note that

$$\begin{bmatrix} I & 0 & 0 & 0 & 0 \\ 0 & I & 0 & 0 & 0 \end{bmatrix} R = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}, \tag{5.115}$$

hence, due to (5.112), we obtain

$$\left(\left[\begin{array}{c:c:c:c:c} A & 0 & 0 & 0 & 0 \\ \hdashline 0 & A & 0 & 0 & 0 \\ \hdashline 0 & 0 & A & 0 & 0 \\ 0 & 0 & 0 & A & 0 \\ 0 & 0 & 0 & 0 & -k \end{array}\right] + \left[\begin{array}{c} B \\ \hdashline 0 \\ \hdashline 0 \\ 0 \\ 0 \end{array}\right] \begin{bmatrix} N_u & N_z \end{bmatrix} \left[\begin{array}{c:c:c:c:c} I & 0 & 0 & 0 & 0 \\ \hdashline 0 & I & 0 & 0 & 0 \end{array}\right] \right) \mathcal{R}$$

$$\subset \mathcal{R} + \operatorname{im} \left[\begin{array}{cc} 0 & 0 \\ \hdashline 0 & 0 \\ \hdashline B & 0 \\ 0 & B \\ 0 & 0 \end{array}\right]. \tag{5.116}$$

Finally, this implies that the controller

$$\mathrm{C} : v = N_u u + N_z z, \tag{5.117}$$

is such that P $\wedge$ C implements $\mathcal{C}$, as desired.

We conclude this section by demonstrating that the controlled vehicle P$\wedge$C achieves tracking of the headway spacing policy for any leading vehicle E. In particular, we consider two vehicles E_1 and E_2 given by

$$\mathrm{E}_i : \begin{cases} \dot{x}_{e,i} = \begin{bmatrix} 0 & 1 \\ 0 & -c_i \end{bmatrix} x_{e,i} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} d_{e,i}, & i \in \{1, 2\}, \\ u = x_{e,i}, \end{cases} \tag{5.118}$$

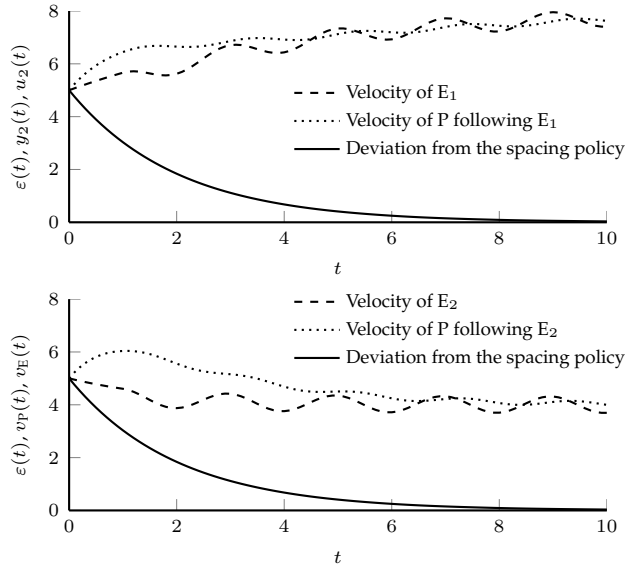

Figure 5.4: Simulation of P following E_i with $h = 1$, $k = 0.5$, $x_{e,i}(0) = [10 \quad 5]^\top$, $x_p(0) = [0 \quad 5]^\top$, $d_{e,i}(t) = 2$ for $t \in [0, 1]$ and $d_{e,i}(t) = 2 + \sin(\pi t - \pi)$ for $t > 1$, .

where $c_1 = 0.25$ and $c_2 = 0.5$. It is easily seen that $\mathrm{E}_i \preccurlyeq \mathrm{A}$ and, thus, that E_i is compatible with $\mathcal{C}$ for both $i \in \{1, 2\}$. As can be seen in Figure 5.4, for both vehicles E_1 and E_2, the controlled vehicle $\mathrm{P} \wedge \mathrm{C}$ achieves tracking of the headway spacing policy, as expected. Note that the deviation from the spacing policy converges to zero at the same rate for both vehicles. This is because the convergence rate is determined by the constant k in (5.101) and is thus guaranteed by the implementation of the contract $\mathcal{C}$.

5.6 Refinement

In this section, we define the notion of refinement, which allows us to compare two contracts and, in particular, to determine if one contract expresses a stricter specification than another contract. As explained in Chapter 2, refinement has an essential role in enabling the independent design of components within interconnected systems. Following the meta-theoretic definition outlined in Chapter 2, we define refinement as follows.

Definition 5.7. A contract $\mathcal{C}_1$ *refines* another contract $\mathcal{C}_2$ if:

1. any environment compatible with $\mathcal{C}_2$ is compatible with $\mathcal{C}_1$;

2. any implementation of $\mathcal{C}_1$ is an implementation of $\mathcal{C}_2$.

Said differently, $\mathcal{C}_1$ refines $\mathcal{C}_2$ if it has a larger class of compatible environments but a smaller class of implementations. The intuition here is the same as in Chapter 3, namely, $\mathcal{C}_1$ imposes stricter guarantees that have to be satisfied under weaker assumptions. Therefore, $\mathcal{C}_1$ can be seen as expressing a stricter specification than $\mathcal{C}_2$.

Just like in Chapter 3, we can verify refinement based on assumptions and guarantees alone. To this end, let $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$, and note that the first condition in Definition 5.7 holds if and only if $\mathrm{A}_2 \preccurlyeq \mathrm{A}_1$. If $\mathcal{C}_1$ is not consistent, then the second condition is vacuously satisfied, hence $\mathcal{C}_1$ refines $\mathcal{C}_2$ if and only if $\mathrm{A}_2 \preccurlyeq \mathrm{A}_1$. If $\mathcal{C}_1$ is consistent, then we can show that the second condition holds if and only if $\mathrm{A}_2 \wedge \Gamma_1 \preccurlyeq \Gamma_2$. To do this, we will first show that a consistent contract has an implementation whose dynamics are, in some sense, the richest among all implementations of the contract. This is done in the following lemma, whose proof can be found in Appendix B.13.

Lemma 5.9. *Suppose that the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ is consistent. Then there exists a system Σ that implements $\mathcal{C}$ and is such that*

$$\mathrm{E} \wedge \Gamma \preccurlyeq \mathrm{E} \wedge \Sigma \tag{5.119}$$

for all environments E *compatible with $\mathcal{C}$.*

Remark 5.17. *Note that the statement of Lemma 5.9 remains true even if* E *has additional outputs. Indeed, the simulation relation $\mathcal{S}_{gs}$ in the proof of Lemma 5.9 is such that the state trajectory of* E *in* $\mathrm{E} \wedge \Gamma$ *is matched by the state trajectory of* E *in* $\mathrm{E} \wedge \Sigma$*, hence any additional output trajectories of* E *in* $\mathrm{E} \wedge \Gamma$ *are matched by the corresponding output trajectories of* E *in* $\mathrm{E} \wedge \Sigma$*. This observation will be useful in the analysis of the series composition in Section 5.7.*

Recall from Theorem 5.1 that a system Σ implements $\mathcal{C} = (\mathrm{A}, \Gamma)$ if and only if $\mathrm{A} \wedge \Sigma \preccurlyeq \Gamma$, which holds if and only if $\mathrm{A} \wedge \Sigma \preccurlyeq \mathrm{A} \wedge \Gamma$, see Remark 5.9. Therefore, since two systems are bisimilar if they simulate each other, a particular consequence of Lemma 5.9 is that every consistent contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ has an implementation Σ such that $\mathrm{A} \wedge \Gamma \sim \mathrm{A} \wedge \Sigma$. Intuitively, this implementation Σ completely captures the relevant dynamics of the guarantees Γ. Indeed, in view of Remark 5.12, it is the dynamics of $\mathrm{A} \wedge \Gamma$ rather than Γ that determine the class of implementations of $\mathcal{C}$. Furthermore, another system Σ' implements $\mathcal{C}$ if and only if $\mathrm{A} \wedge \Sigma' \preccurlyeq \mathrm{A} \wedge \Sigma$, which, in a sense, means that the relevant dynamics of Σ are the richest among all implementations of $\mathcal{C}$.

With this in mind, in the following theorem, we use Lemma 5.9 to obtain necessary and sufficient conditions for refinement.

Theorem 5.4. *Suppose that $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ is consistent. Then, $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ refines $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ if and only if*

$$\mathrm{A}_2 \preccurlyeq \mathrm{A}_1 \quad \textit{and} \quad \mathrm{A}_2 \wedge \Gamma_1 \preccurlyeq \Gamma_2. \tag{5.120}$$

Proof. We begin by proving necessity. Suppose that $\mathcal{C}_1$ refines $\mathcal{C}_2$. Note that A_2 is an environment compatible with $\mathcal{C}_2$. Therefore, from the first condition in Definition 5.7, A_2 is compatible with $\mathcal{C}_1$ and, thus, $\mathrm{A}_2 \preccurlyeq \mathrm{A}_1$. On the other hand, since $\mathcal{C}_1$ is consistent, because of Lemma 5.9, we know there exists an implementation Σ of $\mathcal{C}_1$ such that $\mathrm{E} \wedge \Gamma_1 \preccurlyeq \mathrm{E} \wedge \Sigma$ for all environments compatible with $\mathcal{C}_1$. In particular, this means that $\mathrm{A}_2 \wedge \Gamma_1 \preccurlyeq \mathrm{A}_2 \wedge \Sigma$. But, from the second condition in Definition 5.7, we also know that Σ is an implementation of $\mathcal{C}_2$, hence $\mathrm{A}_2 \wedge \Sigma \preccurlyeq \Gamma_2$. Since simulation is transitive, we conclude that $\mathrm{A}_2 \wedge \Gamma_1 \preccurlyeq \Gamma_2$, as desired.

We proceed by proving sufficiency. Suppose that (5.120) holds. Let E be an environment compatible with $\mathcal{C}_2$, that is, $\mathrm{E} \preccurlyeq \mathrm{A}_2$. Since $\mathrm{A}_2 \preccurlyeq \mathrm{A}_1$ and simulation is transitive, it follows that $\mathrm{E} \preccurlyeq \mathrm{A}_1$ and, thus, E is compatible with $\mathcal{C}_1$. Next, suppose that Σ implements $\mathcal{C}_1$. Note that A_2 is an environment compatible with $\mathcal{C}_1$ because $\mathrm{A}_2 \preccurlyeq \mathrm{A}_1$. Consequently, we must have that $\mathrm{A}_2 \wedge \Sigma \preccurlyeq \Gamma_1$. As explained in Remark 5.12, this implies that $\mathrm{A}_2 \wedge \Sigma \preccurlyeq \mathrm{A}_2 \wedge \Gamma_1$, hence $\mathrm{A}_2 \wedge \Sigma \preccurlyeq \Gamma_2$ because $\mathrm{A}_2 \wedge \Gamma_1 \preccurlyeq \Gamma_2$ and simulation is transitive. Due to Theorem 5.1, it follows that Σ implements $\mathcal{C}_2$. This shows that both conditions in Definition 5.7 are satisfied, hence $\mathcal{C}_1$ refines $\mathcal{C}_2$, as desired. □

Theorem 5.4 tells us that contract refinement can be verified by verifying a pair of simulation conditions. As explained in Remark 5.4, simulation can be verified efficiently using the invariant subspace algorithm, hence Theorem 5.4 tells us that refinement can be verified efficiently.

5.7 Series composition

In this section, we will consider the series composition of two contracts. The series composition can be used to reason about the series interconnection of systems on the basis of the contracts on its components. Loosely speaking, the series composition of two contracts is a contract that is implemented by the series interconnection of *any* of their implementations. We will see that such a contract does not necessarily exist. Indeed, we will find necessary and sufficient conditions for its existence that are not satisfied for arbitrary contracts. Nevertheless, these conditions will be easy to verify and we will provide an explicit expression for the series composition when it exists.

Throughout this section, for each $i \in \{1, 2\}$, we will consider the system

$$\Sigma_i : \begin{cases} \dot{x}_i = A_i x_i + B_i u_i + G_i d_i, \\ y_i = C_i x_i, \end{cases} \tag{5.121}$$

with state $x_i \in \mathcal{X}_i$, input $u_i \in \mathcal{U}_i$, output $y_i \in \mathcal{Y}_i$ and driving variable $d_i \in \mathcal{D}_i$. Furthermore, we will consider the contract $\mathcal{C}_i = (\mathrm{A}_i, \Gamma_i)$, where A_i is given

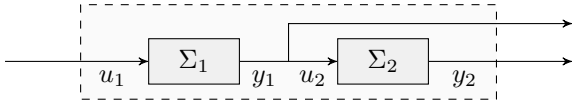

Figure 5.5: The series interconnection $\Sigma_1 \to \Sigma_2$.

by

$$\mathrm{A}_i : \begin{cases} \dot{x}_{a_i} = A_{a_i} x_{a_i} + G_{a_i} d_{a_i}, \\ u_i = C_{a_i} x_{a_i}, \\ 0 = H_{a_i} x_{a_i}, \end{cases} \tag{5.122}$$

with state $x_{a_i} \in \mathcal{X}_{a_i}$, driving variable $d_{a_i} \in \mathcal{D}_{a_i}$, output $u_i \in \mathcal{U}_i$, and consistent subspace $\mathcal{V}_{a_i} \subset \mathcal{X}_{a_i}$, and Γ_i is given by

$$\Gamma_i : \begin{cases} \dot{x}_{g_i} = A_{g_i} x_{g_i} + G_{g_i} d_{g_i}, \\ u_i = C^u_{g_i} x_{g_i}, \\ y_i = C^y_{g_i} x_{g_i}, \\ 0 = H_{g_i} x_{g_i}, \end{cases} \tag{5.123}$$

with state $x_{g_i} \in \mathcal{X}_{g_i}$, driving variable $d_{g_i} \in \mathcal{D}_{g_i}$, outputs $u_i \in \mathcal{U}_i$ and $y_i \in \mathcal{Y}_i$, and consistent subspace $\mathcal{V}_{g_i} \subset \mathcal{X}_{g_i}$.

We begin by defining the series interconnection of two systems. The following definition makes sense only if $\mathcal{Y}_1 = \mathcal{U}_2$, which we will assume from now on.

Definition 5.8. Consider the systems Σ_1 and Σ_2 given by (5.121). The *series interconnection* of Σ_1 to Σ_2, denoted by $\Sigma_1 \to \Sigma_2$, is obtained by setting the output of Σ_1 as input of Σ_2, as shown in Figure 5.5. This results in the system

$$\Sigma_1 \to \Sigma_2 : \begin{cases} \begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} A_1 & 0 \\ B_2 C_1 & A_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} B_1 \\ 0 \end{bmatrix} u + \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \end{bmatrix}, \\ y = \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \end{cases} \tag{5.124}$$

where $u = u_1$ and $y = (y_1, y_2)$.

Following the meta-theoretic definition outlined in Chapter 2, we want the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ to be a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies the following two properties. Let E be an environment compatible with $\mathcal{C}$, and let Σ_1 and Σ_2 be implementations of $\mathcal{C}_1$ and $\mathcal{C}_2$. First, the environments of Σ_1 and Σ_2 in the interconnection $\mathrm{E} \wedge (\Sigma_1 \to \Sigma_2)$ should be compatible with $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively. Second, $\Sigma_1 \to \Sigma_2$ should implement $\mathcal{C}$.

Note the interconnection $\mathrm{E} \wedge (\Sigma_1 \to \Sigma_2)$ shown in Figure 5.6. Loosely speaking, the first property holds if the output u of E can be matched by A_1,

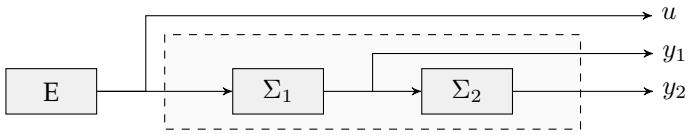

Figure 5.6: The interconnection $\mathrm{E} \wedge (\Sigma_1 \to \Sigma_2)$.

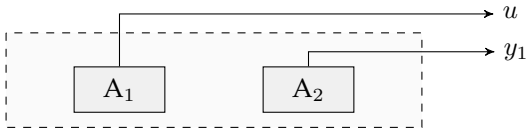

Figure 5.7: The interconnection $\mathrm{A}_1 \to \mathrm{A}_2$.

and the output y_1 of Σ_1 can be matched by A_2. To formalize this, we will define the series interconnection $\mathrm{A}_1 \to \mathrm{A}_2$, as shown in Figure 5.7. Namely, $\mathrm{A}_1 \to \mathrm{A}_2$ is obtained from A_1 and A_2 by relabelling u_1 to u and u_2 to y_1, which results in the system

$$\mathrm{A}_1 \to \mathrm{A}_2 : \begin{cases} \begin{bmatrix} \dot{x}_{a_1} \\ \dot{x}_{a_2} \end{bmatrix} = \begin{bmatrix} A_{a_1} & 0 \\ 0 & A_{a_2} \end{bmatrix} \begin{bmatrix} x_{a_1} \\ x_{a_2} \end{bmatrix} + \begin{bmatrix} G_{a_1} & 0 \\ 0 & G_{a_2} \end{bmatrix} \begin{bmatrix} d_{a_1} \\ d_{a_2} \end{bmatrix}, \\ u = \begin{bmatrix} C_{a_1} & 0 \end{bmatrix} \begin{bmatrix} x_{a_1} \\ x_{a_2} \end{bmatrix}, \\ y_1 = \begin{bmatrix} 0 & C_{a_2} \end{bmatrix} \begin{bmatrix} x_{a_1} \\ x_{a_2} \end{bmatrix}, \\ 0 = \begin{bmatrix} H_{a_1} & 0 \\ 0 & H_{a_2} \end{bmatrix} \begin{bmatrix} x_{a_1} \\ x_{a_2} \end{bmatrix}. \end{cases} \tag{5.125}$$

Now, the first property holds if and only if $\mathrm{E} \wedge (\Sigma_1 \to \Sigma_2) \preccurlyeq \mathrm{A}_1 \to \mathrm{A}_2$. In view of Lemma 5.5, this holds for all environments E compatible with $\mathcal{C}$ if and only if $\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2) \preccurlyeq \mathrm{A}_1 \to \mathrm{A}_2$. On the other hand, due to Theorem 5.1, the second property holds if and only if $\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2) \preccurlyeq \Gamma$. Therefore, the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ is a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies the following implication.

Implication 5.1. *If Σ_1 and Σ_2 implement $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$, respectively, then*

$$\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2) \preccurlyeq \mathrm{A}_1 \to \mathrm{A}_2, \tag{5.126}$$

$$\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2) \preccurlyeq \Gamma. \tag{5.127}$$

Unless $\mathcal{C}_1$ and $\mathcal{C}_2$ are both consistent, Implication 5.1 is vacuously satisfied for any $\mathcal{C} = (\mathrm{A}, \Gamma)$, which renders the series composition useless. Therefore,

for the remainder of this section, we will assume that $\mathcal{C}_1$ and $\mathcal{C}_2$ are consistent. This does not guarantee that there exists a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 5.1, which motivates the following definition.

Definition 5.9. The contract $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$ if there exists a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 5.1.

On the other hand, there might be multiple contracts $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfy Implication 5.1. Then, the series composition is chosen to be the smallest one with respect to refinement.

Definition 5.10. Suppose that $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$. The series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$, denoted by $\mathcal{C}_1 \to \mathcal{C}_2$, is the smallest contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 5.1.

Intuitively, the series composition assumes the least and guarantees the most while still ensuring the satisfaction of Implication 5.1, which captures properties that enable independent design, as explained in Chapter 2. Note that, even if $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$, the series composition $\mathcal{C}_1 \to \mathcal{C}_2$ might not exist, that is, there might be no *smallest* contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 5.1. Fortunately, this turns out to be false, as will be shown later in this section. In the meantime, we turn to finding tractable conditions on A and Γ under which the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 5.1. This will naturally lead us to consider the series interconnection of guarantees, defined below.

Definition 5.11. Consider guarantees Γ_1 and Γ_2 given by (5.123). The *series interconnection* of Γ_1 to Γ_2, denoted by $\Gamma_1 \to \Gamma_2$, is obtained by setting $y_1 = u_2$ of Γ_2, as shown in Figure 5.8. This results in the system

$$\Gamma_1 \to \Gamma_2 : \begin{cases} \begin{bmatrix} \dot{x}_{g_1} \\ \dot{x}_{g_2} \end{bmatrix} = \begin{bmatrix} A_{g_1} & 0 \\ 0 & A_{g_2} \end{bmatrix} \begin{bmatrix} x_{g_1} \\ x_{g_2} \end{bmatrix} + \begin{bmatrix} G_{g_1} & 0 \\ 0 & G_{g_2} \end{bmatrix} \begin{bmatrix} d_{g_1} \\ d_{g_2} \end{bmatrix}, \\ u = \begin{bmatrix} C^u_{g_1} & 0 \end{bmatrix} \begin{bmatrix} x_{g_1} \\ x_{g_2} \end{bmatrix}, \\ y = \begin{bmatrix} C^y_{g_1} & 0 \\ 0 & C^y_{g_2} \end{bmatrix} \begin{bmatrix} x_{g_1} \\ x_{g_2} \end{bmatrix}, \\ 0 = \begin{bmatrix} H_{g_1} & 0 \\ 0 & H_{g_2} \\ C^y_{g_1} & -C^u_{g_2} \end{bmatrix} \begin{bmatrix} x_{g_1} \\ x_{g_2} \end{bmatrix}. \end{cases} \tag{5.128}$$

where $u = u_1$ and $y = (y_1, y_2)$.

With this in mind, consider the following lemma, whose proof can be found in Appendix B.14.

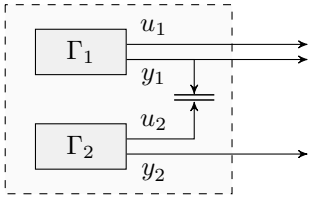

Figure 5.8: The series interconnection $\Gamma_1 \to \Gamma_2$. The long equality sign indicates the constraint $u_2 = y_1$.

Lemma 5.10. *Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are consistent. Then, the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 5.1 if and only if*

$$\hat{\mathrm{A}} \preccurlyeq \mathrm{A}_1, \tag{5.129}$$

$$\hat{\mathrm{A}} \wedge \hat{\Gamma}_1 \preccurlyeq \mathrm{A}_2, \tag{5.130}$$

$$\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2) \preccurlyeq \Gamma, \tag{5.131}$$

where $\hat{\mathrm{A}}$ is obtained from A by relabelling u to u_1, and $\hat{\Gamma}_1$ is obtained from Γ_1 by relabelling y_1 to u_2.

The conditions in Lemma 5.10 should not be surprising given the interconnection structure of $\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2)$. Indeed, the first condition says that the outputs generated by A must be outputs that can be generated by A_1. Similarly, the second condition says that any output generated by Σ_1 corresponding to an input generated by A must be an output that can be generated by A_2. On the other hand, the last condition captures the requirement that $\Sigma_1 \to \Sigma_2$ should be an implementation of $\mathcal{C}$ for all implementations Σ_1 and Σ_2 of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively.

The second condition in Lemma 5.10 is partially independent of $\mathcal{C}$. To see this, note that A can always generate a zero output. In particular, this means that the second condition holds only if any output y_1 generated by Γ_1 while u_1 is set to zero is an output that A_2 can generate. This is formalized in the following lemma, whose proof can be found in Appendix B.15.

Lemma 5.11. *Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are consistent, and consider the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$. Let $\hat{\Gamma}_1$ be obtained from Γ_1 by relabelling y_1 to u_2, and let $\hat{\mathrm{A}}$ be obtained from A by relabelling u to u_1. Then, A is such that*

$$\hat{\mathrm{A}} \preccurlyeq \mathrm{A}_1 \quad \textit{and} \quad \hat{\mathrm{A}} \wedge \hat{\Gamma}_1 \preccurlyeq \mathrm{A}_2 \tag{5.132}$$

if and only if

$$\hat{\mathrm{A}} \preccurlyeq \mathrm{A}_1 \wedge \hat{\Gamma}_1 \wedge \mathrm{A}_2 \quad \textit{and} \quad \hat{\Gamma}_1^0 \preccurlyeq \mathrm{A}_2, \tag{5.133}$$

where $\hat{\Gamma}_1^0$ is obtained from $\hat{\Gamma}_1$ by setting $u_1 = 0$.

Lemma 5.11 has the following aspects. First, it provides us with an upper bound on the assumptions of a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 5.1. Second, since the condition $\hat{\Gamma}_1^0 \preccurlyeq \mathrm{A}_2$ is independent of $\mathcal{C}$, it provides us with a necessary condition for series composability. We can show that this condition is also sufficient. This is done in the following theorem, where we also show that the series composition $\mathcal{C}_1 \to \mathcal{C}_2$ exists when $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$, and we provide an explicit expression for it when it exists.

Theorem 5.5. *Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are consistent. Let A_1, Γ_1, A_2 and Γ_2 be given by* (5.122) *and* (5.123)*. Then, $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$ if and only if there exists a subspace $\mathcal{S}^0 \subset \mathcal{X}_{g_1} \times \mathcal{X}_{a_2}$ such that*

$$\begin{bmatrix} A_{g_1} & 0 \\ 0 & A_{a_2} \end{bmatrix} \mathcal{S}^0 \subset \mathcal{S}^0 + \operatorname{im} \begin{bmatrix} G_{g_1} & 0 \\ 0 & G_{a_2} \end{bmatrix}, \tag{5.134}$$

$$\begin{bmatrix} \operatorname{im} G_{g_1} \cap \mathcal{V}_{g_1}^0 \\ 0 \end{bmatrix} \subset \mathcal{S}^0 + \operatorname{im} \begin{bmatrix} 0 \\ G_{a_2} \end{bmatrix}, \tag{5.135}$$

$$\mathcal{S}^0 \subset \begin{bmatrix} C_{g_2}^y & -C_{a_2} \\ H_{g_1} & 0 \\ -C_{g_1}^u & 0 \\ 0 & H_{a_2} \end{bmatrix}, \tag{5.136}$$

and $\pi_{\mathcal{X}_{g_1}}(\mathcal{S}^0) = \mathcal{V}_{g_1}^0$, where $\mathcal{V}_{g_1}^0$ is the largest subspace such that

$$A_{a_{g_1}} \mathcal{V}_{g_1}^0 \subset \mathcal{V}_{g_1}^0 + \operatorname{im} G_{g_1} \quad \textit{and} \quad \mathcal{V}_{g_1}^0 \subset \ker \begin{bmatrix} H_{g_1} \\ C_{g_1}^u \end{bmatrix}. \tag{5.137}$$

Furthermore, if $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$, then the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ exists and is given by

$$\mathcal{C}_1 \to \mathcal{C}_2 = (\mathrm{A}_{12}, \Gamma_1 \to \Gamma_2), \tag{5.138}$$

where $\Gamma_1 \to \Gamma_2$ is given by (5.128) *and A_{12} is given by*

$$\mathrm{A}_{12} : \begin{cases} \begin{bmatrix} \dot{x}_{a_1} \\ \dot{x}_{g_1} \\ \dot{x}_{a_2} \end{bmatrix} = \begin{bmatrix} A_{a_1} & 0 & 0 \\ 0 & A_{g_1} & 0 \\ 0 & 0 & A_{a_2} \end{bmatrix} \begin{bmatrix} x_{a_1} \\ x_{g_1} \\ x_{a_2} \end{bmatrix} + \begin{bmatrix} G_{a_1} & 0 & 0 \\ 0 & G_{g_1} & 0 \\ 0 & 0 & G_{a_2} \end{bmatrix} \begin{bmatrix} d_{a_1} \\ d_{g_1} \\ d_{a_2} \end{bmatrix}, \\ u = \begin{bmatrix} C_{a_1} & 0 & 0 \end{bmatrix} \begin{bmatrix} x_{a_1} \\ x_{g_1} \\ x_{a_2} \end{bmatrix}, \\ 0 = \begin{bmatrix} C_a & -C_{g_1}^u & 0 \\ 0 & C_{g_2}^y & -C_{a_2} \\ H_{a_1} & 0 & 0 \\ 0 & H_{g_1} & 0 \\ 0 & 0 & H_{a_2} \end{bmatrix} \begin{bmatrix} x_{a_1} \\ x_{g_1} \\ x_{a_2} \end{bmatrix}. \end{cases} \tag{5.139}$$

Proof. We begin by proving necessity. Suppose that $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$, that is, there exists a contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ that satisfies Implication 5.1. Due to Lemma 5.10, this implies that (5.129) and (5.130) hold. Then, due to Lemma 5.11, it follows that (5.133) holds, and, in particular, that $\hat{\Gamma}_1^0 \preccurlyeq \mathrm{A}_2$, where $\hat{\Gamma}_1^0$ is defined as in Lemma 5.11. Let $\mathcal{S}^0$ be a full simulation relation of $\hat{\Gamma}_1^0$ by A_2. Note that $\mathcal{V}_{g_1}^0$ is the consistent subspace of $\hat{\Gamma}_1^0$, hence, due to Proposition 5.1, $\mathcal{S}_0$ is such that (5.134), (5.135) and (5.136) hold, and $\pi_{\mathcal{X}_{g_1}}(\mathcal{S}^0) = \mathcal{V}_{g_1}^0$.

We proceed by proving sufficiency. Suppose that there exists a subspace $\mathcal{S}_0$ such that (5.134), (5.135) and (5.136) hold, and $\pi_{\mathcal{X}_{g_1}}(\mathcal{S}^0) = \mathcal{V}_{g_1}^0$. Let $\hat{\Gamma}_1^0$ be defined as in Lemma 5.11. Since $\mathcal{V}_{g_1}^0$ is the consistent subspace of $\hat{\Gamma}_1^0$, due to Proposition 5.1, it follows that $\mathcal{S}_0$ is a full simulation relation of $\hat{\Gamma}_1^0$ by A_2, hence $\hat{\Gamma}_1^0 \preccurlyeq \mathrm{A}_2$. Now, we will show that the contract $\mathcal{C}_1 \to \mathcal{C}_2$ given by (5.138) satisfies Implication 5.1. To this end, let $\hat{\mathrm{A}}_{12}$ be obtained from A_{12} by relabelling u to u_1, and let $\hat{\Gamma}_1$ be obtained from Γ_1 by relabelling y_1 to u_2, like in Lemma 5.10. By definition, $\hat{\mathrm{A}}_{12}$ is obtained from $\mathrm{A}_1 \wedge \hat{\Gamma}_1 \wedge \mathrm{A}_2$ by ignoring the output u_2. This implies that

$$\hat{\mathrm{A}}_{12} \preccurlyeq \mathrm{A}_1 \wedge \hat{\Gamma}_1 \wedge \mathrm{A}_2. \tag{5.140}$$

Since we also have that $\hat{\Gamma}_1^0 \preccurlyeq \mathrm{A}_2$, Lemma 5.11 implies that

$$\hat{\mathrm{A}}_{12} \preccurlyeq \mathrm{A}_1 \quad \text{and} \quad \hat{\mathrm{A}}_{12} \wedge \hat{\Gamma}_1 \preccurlyeq \mathrm{A}_2. \tag{5.141}$$

Furthermore, it is easily seen that

$$\mathrm{A}_{12} \wedge (\Gamma_1 \to \Gamma_2) \preccurlyeq \Gamma_1 \to \Gamma_2, \tag{5.142}$$

which, due to Lemma 5.10, shows that $\mathcal{C}_1 \to \mathcal{C}_2$ satisfies Implication 5.1. This means that $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$. Since $\mathcal{C}_1$ and $\mathcal{C}_2$ are consistent, this also means that $\mathcal{C}_1 \to \mathcal{C}_2$ is consistent.

With this in mind, we now turn to showing that $\mathcal{C}_1 \to \mathcal{C}_2$ is indeed the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$, that is, $\mathcal{C}_1 \to \mathcal{C}_2$ is the smallest contract that satisfies Implication 5.1. Since $\hat{\Gamma}_1^0 \preccurlyeq \mathrm{A}_2$, Lemma 5.10 and Lemma 5.11 tell us that $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 5.1 if and only if $\hat{\mathrm{A}} \preccurlyeq \mathrm{A}_1 \wedge \hat{\Gamma}_1 \wedge \mathrm{A}_2$ and $\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2) \preccurlyeq \Gamma$, where $\hat{\mathrm{A}}$ is obtained from A by relabelling u to u_1. Recall that $\hat{\mathrm{A}}_{12}$ is obtained from $\mathrm{A}_1 \wedge \hat{\Gamma}_1 \wedge \mathrm{A}_2$ ignoring the output u_2. Therefore, $\hat{\mathrm{A}} \preccurlyeq \mathrm{A}_1 \wedge \hat{\Gamma}_1 \wedge \mathrm{A}_2$ is equivalent to $\hat{\mathrm{A}} \preccurlyeq \hat{\mathrm{A}}_{12}$, which is equivalent to $\mathrm{A} \preccurlyeq \mathrm{A}_{12}$ after relabelling u_1 to u. In view of Theorem 5.2, this means that $\mathcal{C}$ satisfies Implication 5.1 if and only if it is refined by the contract $\mathcal{C}_1 \to \mathcal{C}_2$. This shows that $\mathcal{C}_1 \to \mathcal{C}_2$ is the smallest contract that satisfies Implication 5.1 and, thus, $\mathcal{C}_1 \to \mathcal{C}_2$ is indeed the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$. □

The condition for series composability in Theorem 5.5 is nothing more than a spelling out of the condition that $\hat{\Gamma}_1^0 \preccurlyeq \mathrm{A}_2$ from Lemma 5.11. In other

words, Theorem 5.5 tells us that $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ is series composable to $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ if and only if any output y_1 that Γ_1 can generate when u_1 is set to zero is guaranteed to be an output that A_2 can generate. On the other hand, the assumptions A_{12} are obtained from the system $\mathrm{A}_1 \wedge \hat{\Gamma}_1 \wedge \mathrm{A}_2$ in Lemma 5.11 after relabelling u_1 to u and ignoring the output u_2. Therefore, the outputs that A_{12} can generate are precisely the outputs u_1 that A_1 can generate for which the corresponding output y_1 generated by Γ_1 is guaranteed to be an output that A_2 can generate. A notable special case is obtained when A_2 can generate any output y_1 that Γ_1 can generate when u_1 is generated by A_1, that is, $\mathrm{A}_1 \wedge \hat{\Gamma}_1 \preccurlyeq \mathrm{A}_2$.

Corollary 5.12. *Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are consistent and such that $\mathrm{A}_1 \wedge \hat{\Gamma}_1 \preccurlyeq \mathrm{A}_2$, where $\hat{\Gamma}_1$ is obtained from Γ_1 by relabelling y_1 to u_2. Then, $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$. Furthermore, the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ exist and is given by*

$$\mathcal{C}_1 \to \mathcal{C}_2 = (\hat{\mathrm{A}}_1, \Gamma_1 \to \Gamma_2), \tag{5.143}$$

where $\hat{\mathrm{A}}_1$ is obtained from A_1 by relabelling u_1 to u.

Proof. We claim that $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 5.1 if and only if

$$\mathrm{A} \preccurlyeq \hat{\mathrm{A}}_1 \quad \text{and} \quad \mathrm{A} \wedge (\Gamma_1 \to \Gamma_2) \preccurlyeq \Gamma. \tag{5.144}$$

Indeed, due to Lemma 5.10, $\mathcal{C}$ satisfies Implication 5.1 if and only if (5.129), (5.130) and (5.131) hold. We know that (5.130) holds by assumption, while (5.129) is equivalent to $\mathrm{A} \preccurlyeq \hat{\mathrm{A}}_1$ by relabelling u_1 to u. Together with (5.131), this shows that $\mathcal{C}$ satisfies Implication 5.1 if and only if (5.144) holds.

Now, it is easily seen that

$$\hat{\mathrm{A}}_1 \preccurlyeq \hat{\mathrm{A}}_1 \quad \text{and} \quad \hat{\mathrm{A}}_1 \wedge (\Gamma_1 \to \Gamma_2) \preccurlyeq \Gamma_1 \to \Gamma_2, \tag{5.145}$$

hence the contract $\mathcal{C}_1 \to \mathcal{C}_2$ given by (5.143) satisfies Implication 5.1. This implies that $\mathcal{C}_1 \to \mathcal{C}_2$ is consistent. Consequently, due to Theorem 5.1, (5.144) holds if and only if $\mathcal{C}_1 \to \mathcal{C}_2$ refines $\mathcal{C}$. In other words, $\mathcal{C}_1 \to \mathcal{C}_2$ is the smallest contract that satisfies Implication 5.1, hence it is indeed the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$. □

We conclude this section by showing that the series composition satisfies the independent refinement property described in Chapter 2.

Theorem 5.6. *Suppose that the contracts $\mathcal{C}_1'$, $\mathcal{C}_2'$, $\mathcal{C}_1$ and $\mathcal{C}_2$ are consistent. If $\mathcal{C}_1'$ refines $\mathcal{C}_1$ and $\mathcal{C}_2'$ refines $\mathcal{C}_2$, then $\mathcal{C}_1'$ is series composable to $\mathcal{C}_2'$ if $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$, and $\mathcal{C}_1' \to \mathcal{C}_2'$ refines $\mathcal{C}_1 \to \mathcal{C}_2$.*

Proof. Let $\mathcal{C}_1' = (\mathrm{A}_1', \Gamma_1')$, $\mathcal{C}_2' = (\mathrm{A}_2', \Gamma_2')$, $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$. Suppose that $\mathcal{C}_1'$ refines $\mathcal{C}_1$ and $\mathcal{C}_2'$ refines $\mathcal{C}_2$. Due to Theorem 5.4, this implies that $\mathrm{A}_1 \preccurlyeq \mathrm{A}_1'$ and $\mathrm{A}_2 \preccurlyeq \mathrm{A}_2'$. This means that $\mathrm{A}_1 \to \mathrm{A}_2 \preccurlyeq \mathrm{A}_1' \to \mathrm{A}_2'$. Indeed, if $\mathcal{S}_1$ is a full simulation relation of A_1 by A_1', and $\mathcal{S}_2$ is a full simulation relation of A_2 by A_2', then it is straightforward to show that

$$\mathcal{S} = \left\{ (x_{a_1}, x_{a_2}, x'_{a_1}, x'_{a_2}) \;\middle|\; (x_{a_1}, x'_{a_1}) \in \mathcal{S}_1,\ (x_{a_2}, x'_{a_2}) \in \mathcal{S}_2 \right\} \tag{5.146}$$

is a full simulation relation of $\mathrm{A}_1 \to \mathrm{A}_2$ by $\mathrm{A}_1' \to \mathrm{A}_2'$.

With this in mind, suppose that $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 5.1. Let Σ_1 and Σ_2 be implementations of $\mathcal{C}_1'$ and $\mathcal{C}_2'$, respectively. Since $\mathcal{C}_1'$ refines $\mathcal{C}_1$ and $\mathcal{C}_2'$ refines $\mathcal{C}_2$, it follows that Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Consequently, since $\mathcal{C}$ satisfies Implication 5.1, it follows that (5.126) and (5.127) hold. But we have that $\mathrm{A}_1 \to \mathrm{A}_2 \preccurlyeq \mathrm{A}_1' \to \mathrm{A}_2'$ and simulation is transitive, hence (5.126) holds with $\mathrm{A}_1 \to \mathrm{A}_2$ replaced by $\mathrm{A}_1' \to \mathrm{A}_2'$. This shows that $\mathcal{C}$ satisfies Implication 5.1 with $\mathcal{C}_1$ and $\mathcal{C}_2$ replaced by $\mathcal{C}_1'$ and $\mathcal{C}_2'$, respectively. Therefore, if $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$, then $\mathcal{C}_1'$ is series composable to $\mathcal{C}_2'$. Furthermore, both $\mathcal{C}_1 \to \mathcal{C}_2$ and $\mathcal{C}_1' \to \mathcal{C}_2'$ exist. On the other hand, as we just showed, since $\mathcal{C}_1 \to \mathcal{C}_2$ satisfies Implication 5.1, it also satisfies it with $\mathcal{C}_1$ and $\mathcal{C}_2$ replaced by $\mathcal{C}_1'$ and $\mathcal{C}_2$', respectively. But $\mathcal{C}_1' \to \mathcal{C}_2'$ is the smallest such contract, hence $\mathcal{C}_1' \to \mathcal{C}_2'$ refines $\mathcal{C}_1 \to \mathcal{C}_2$. □

5.8 Comparison with behavioural contracts

In this section, we will compare the simulation contracts presented in this chapter and the behavioural contracts presented in Chapter 3. The two types of contracts are very similar, as is made evident by the definitions and characterizations of implementation, refinement, series composability and the series composition, see Table 5.1. The main difference is that behavioural contracts are defined using behavioural inclusion as a method for system comparison, whereas simulation contracts are defined using simulation. Since simulation is a stronger notion than behavioural inclusion for non-deterministic systems (e.g., assumptions and guarantees), simulation contracts tend to express stricter specifications than behavioural contracts.

Before we can show this, we need to consider another difference, namely, that the class of implementations of a simulation contract consists of input-state-output systems with a driving variable, whereas the class of implementations of a behavioural contract consists of input-output systems. Due to [77, Theorem 6.2], the class of input-output systems is (behaviourally) equivalent to the class of input-state-output systems. Therefore, for a fair comparison, we will restrict the class of systems that can be implementations of a simulation contract to input-state-output systems, i.e., systems of the form (5.42) with $G = 0$.

	Behavioural	Simulation
Implementation	$\mathfrak{B}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}(\Gamma)$	$\mathrm{A} \wedge \Sigma \preccurlyeq \Gamma$
Refinement	$\mathfrak{B}(\mathrm{A}_2) \subset \mathfrak{B}(\mathrm{A}_1)$ $\mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_1) \subset \mathfrak{B}(\Gamma_2)$	$\mathrm{A}_2 \preccurlyeq \mathrm{A}_1$ $\mathrm{A}_2 \wedge \Gamma_1 \preccurlyeq \Gamma_2$
Series composability	$(0, y) \in \mathfrak{B}(\Gamma_1) \implies y \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$	$\hat{\Gamma}_1^0 \preccurlyeq \mathrm{A}_2$
Series composition	$(\mathrm{A}_{12}, \Gamma_1 \to \Gamma_2)$, with A_{12} from $(\mathrm{A}_1 \to \mathrm{A}_2) \wedge (\Gamma_1 \to \Gamma_2)$	$(\mathrm{A}_{12}, \Gamma_1 \to \Gamma_2)$, with A_{12} from $\mathrm{A}_1 \wedge \hat{\Gamma}_1 \wedge \mathrm{A}_2$

Table 5.1: Summary of comparable results

We will first show how a simulation contract can be interpreted as a behavioural contract. Consider the simulation contract $\mathcal{C} = (\mathrm{A}, \Gamma)$. Let A be given by

$$\mathrm{A} : \begin{cases} \dot{x}_a(t) = A_a x_a(t) + G_a d_a(t), \\ u(t) = C_a x_a(t), \\ 0 = H_a x_a(t), \end{cases} \tag{5.147}$$

where $x_a(t) \in \mathbb{R}^{n_a}$, $d_a(t) \in \mathbb{R}^{r_a}$, and $u(t) \in \mathbb{R}^m$. The input behaviour of A is defined in the obvious way, that is,

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) = \left\{ u \in \mathscr{C}_m^\infty \;\middle|\; \exists (x_a, d_a) \in \mathscr{C}_{n_a + r_a}^\infty \text{ s.t. (5.147) holds} \right\}. \tag{5.148}$$

On the other hand, let Γ be given by

$$\Gamma : \begin{cases} \dot{x}_g(t) = A_g x_g(t) + G_g d_g(t), \\ u(t) = C_g^u x_g(t), \\ y(t) = C_g^y x_g(t), \\ 0 = H_g x_g(t), \end{cases} \tag{5.149}$$

where $x_g(t) \in \mathbb{R}^{n_g}$, $d_g(t) \in \mathbb{R}^{r_g}$, $u(t) \in \mathbb{R}^m$ and $y(t) \in \mathbb{R}^p$. The external behaviour of Γ is also defined in the obvious way, that is,

$$\mathfrak{B}(\Gamma) = \left\{ (u, y) \in \mathscr{C}_{m+p}^\infty \;\middle|\; \exists (x_g, d_g) \in \mathscr{C}_{n_g + r_g}^\infty \text{ s.t. (5.149) holds} \right\}. \tag{5.150}$$

Then, we can interpret $\mathcal{C}$ as a behavioural contract as follows. First, an environment E is compatible with $\mathcal{C}$ if $\mathfrak{B}_{\mathrm{i}}(\mathrm{E}) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A})$. Second, an input-state-output system Σ implements $\mathcal{C}$ if $\mathfrak{B}(\mathrm{E} \wedge \Sigma) \subset \mathfrak{B}(\Gamma)$ for all E compatible with $\mathcal{C}$. As shown in Theorem 3.1, the latter holds if and only if $\mathfrak{B}(\mathrm{A} \wedge \Sigma) \preccurlyeq \mathfrak{B}(\Gamma)$.

The classes of compatible environments and implementations are enlarged when a simulation contract is interpreted as a behavioural contract. This is because simulation is a stronger notion than behavioural inclusion, that is,

simulation implies behavioural inclusion, but behavioural inclusion does not imply simulation. Consequently, an input-state-output system Σ implements $\mathcal{C} = (\mathrm{A}, \Gamma)$ as a simulation contract only if it implements it as a behavioural contract. Indeed, this follows from Theorem 3.1, Theorem 5.1, and the fact that $\mathrm{A} \wedge \Sigma \preccurlyeq \Gamma$ implies $\mathfrak{B}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}(\Gamma)$. The converse is generally not true, as demonstrated in the following example.

Example 5.1. Consider the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$, where

$$\mathrm{A} : \begin{cases} \dot{x}_a = d_a, \\ u = x_a, \end{cases} \tag{5.151}$$

and

$$\Gamma : \begin{cases} \dot{x}_g = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} x_g + \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} d_g \\ u = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} x_g \\ y = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} x_g \end{cases} \tag{5.152}$$

Note that $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) = \mathscr{C}_1^\infty$ since $x_a = u$ and $d_a = \dot{u}$ satisfy (5.151) for all $u \in \mathscr{C}_1^\infty$. Similarly, $\mathfrak{B}(\Gamma) = \mathscr{C}_2^\infty$ since $x_g = (u, \dot{u}, y)$ and $d_g = (\ddot{u}, \dot{y})$ satisfy (5.152) for all $(u, y) \in \mathscr{C}_2^\infty$. With this in mind, consider the system

$$\Sigma : \begin{cases} \dot{x} = u, \\ y = x. \end{cases} \tag{5.153}$$

Since $\mathfrak{B}(\Gamma) = \mathscr{C}_2^\infty$, it follows that $\mathfrak{B}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}(\Gamma)$, hence Σ implements $\mathcal{C}$ as a behavioural contract.

However, Σ does not implement $\mathcal{C}$ as a simulation contract. We will show this by contradiction. Suppose that Σ implements $\mathcal{C}$ as a simulation contract, that is, $\mathrm{A} \wedge \Sigma \preccurlyeq \Gamma$. Note that

$$\mathrm{A} \wedge \Sigma : \begin{cases} \begin{bmatrix} \dot{x}_a \\ \dot{x} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_a \\ x \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} d_a, \\ u = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} x_a \\ x \end{bmatrix}, \\ y = \begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} x_a \\ x \end{bmatrix}. \end{cases} \tag{5.154}$$

Let $\mathcal{S}$ be a full simulation relation of $\mathrm{A} \wedge \Sigma$ by Γ. By definition of simulation relation, if $(x_a(0), x(0), x_g(0)) \in \mathcal{S}$, then for all $d_a(\cdot)$, there exists $d_g(\cdot)$ such that

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_a(t) \\ x(t) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} x_g(t), \qquad \text{for all } t \geq 0, \tag{5.155}$$

where $(x_a(t), x(t))$ is the corresponding state trajectory of $\mathrm{A} \wedge \Sigma$, and $x_g(t)$ is the corresponding state trajectory of Γ. Fix $(x_a(0), x(0), x_g(0)) \in \mathcal{S}$. Note that

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \dot{x}_a(0) \\ \dot{x}(0) \end{bmatrix} = \begin{bmatrix} d_a(0) \\ x_a(0) \end{bmatrix}. \tag{5.156}$$

On the other hand,

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \dot{x}_g(0) = \begin{bmatrix} x_{g,2}(0) \\ d_{g,2}(0) \end{bmatrix}, \tag{5.157}$$

where $x_{g,2}(0)$ is the second entry of $x_g(0)$, and $d_{g,2}(0)$ is the second entry of $d_g(0)$. Consequently, if $d_a(\cdot)$ is such that $d_a(0) \neq x_{g,2}(0)$, then there does not exist $d_g(\cdot)$ such that (5.155) holds. This is a contradiction, hence $\mathrm{A} \wedge \Sigma$ is not simulated by Γ and, thus, Σ does not implement $\mathcal{C}$ as a simulation contract.

It can be shown that the contract in Example 5.1 is not consistent when treated as a simulation contract. In particular, it can be shown that A is not simulated by Γ, which is necessary for consistency due to Theorem 5.2 and Remark 5.13. This shows that a contract might be consistent when treated as a behavioural contract but not consistent when treated as a simulation contract. The converse is not true because simulation implies behavioural inclusion. In fact, if the conditions in Theorem 5.2 are satisfied, then Algorithm 1 produces an input-state-output system Σ, *without* a driving variable, that implements $\mathcal{C} = (\mathrm{A}, \Gamma)$ when treated as a simulation contract. This means that $\mathrm{A} \wedge \Sigma \preccurlyeq \Gamma$, which implies that $\mathfrak{B}(\mathrm{A} \wedge \Sigma) \subset \mathfrak{B}(\Gamma)$, hence Σ implements $\mathcal{C}$ when treated as a behavioural contract as well. Therefore, Theorem 5.2 provides sufficient conditions for consistency of $\mathcal{C}$ when treated as a behavioural contract, and a particular implementation can be constructed using Algorithm 1. This presents an alternative approach to the one taken in Section 3.4.

Another noteworthy difference between behavioural contracts and simulation contracts has to do with the conditions for refinement. Consider the simulation contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$. Due to Theorem 3.3, when treated as behavioural contracts, $\mathcal{C}_1$ refines $\mathcal{C}_2$ if and only if $\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2) \subset \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$ and $\mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_1) \subset \mathfrak{B}(\Gamma_2)$. Analogously, due to Theorem 5.4, when treated as simulation contracts, $\mathcal{C}_1$ refines $\mathcal{C}_2$ if and only if $\mathrm{A}_2 \preccurlyeq \mathrm{A}_1$ and $\mathrm{A}_2 \wedge \Gamma_1 \preccurlyeq \Gamma_2$, see Table 5.1. However, to show the necessity of the latter, we made use of input-state-output systems *with* a driving variable, see Lemma 5.9. With the restriction to input-state-output systems without a driving variable, this condition is no longer necessary, that is, $\mathcal{C}_1$ might refine $\mathcal{C}_2$ even if $\mathrm{A}_2 \wedge \Gamma_1$ is not simulated by Γ_2. This is demonstrated in the following example.

Example 5.2. Consider the contract $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$, where

$$\mathrm{A}_1 : \begin{cases} \dot{x}_a = d_a, \\ u = x_a, \end{cases} \qquad \Gamma_1 : \begin{cases} \dot{x}_{g_1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} d_{g_1}, \\ u = \begin{bmatrix} 1 & 0 \end{bmatrix} x_{g_1}, \\ y = \begin{bmatrix} 0 & 1 \end{bmatrix} x_{g_1}. \end{cases} \tag{5.158}$$

and the contract $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$, where

$$\mathrm{A}_2 : \begin{cases} \dot{x}_a = d_a, \\ u = x_a, \end{cases} \qquad \Gamma_2 : \begin{cases} \dot{x}_{g_2} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} x_{g_2} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} d_{g_2}, \\ u = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} x_{g_2}, \\ y = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} x_{g_2}. \end{cases} \tag{5.159}$$

Since $\mathcal{C}_1$ and $\mathcal{C}_2$ have the same assumptions, it follows that they have the same classes of compatible environments. Therefore, to show that $\mathcal{C}_1$ refines $\mathcal{C}_2$, it is enough to show that an input-state-output system Σ implements $\mathcal{C}_2$ if it implements $\mathcal{C}_1$. We will do this by showing that *any* input-state-output system Σ implements $\mathcal{C}_2$. To this end, consider the system

$$\Sigma : \begin{cases} \dot{x} = Ax + Bu, \\ y = Cx, \end{cases} \tag{5.160}$$

where $x \in \mathbb{R}^n$, and note that

$$\mathrm{A} \wedge \Sigma : \begin{cases} \begin{bmatrix} \dot{x}_a \\ \dot{x} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ B & A \end{bmatrix} \begin{bmatrix} x_a \\ x \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} d_a, \\ u = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} x_a \\ x \end{bmatrix}, \\ y = \begin{bmatrix} 0 & C \end{bmatrix} \begin{bmatrix} x_a \\ x \end{bmatrix}. \end{cases} \tag{5.161}$$

We claim that the subspace $\mathcal{S} \subset \mathbb{R} \times \mathbb{R}^n \times \mathbb{R}^3$ given by

$$\mathcal{S} = \left\{ (x_a, x, x_{g_2}) \;\middle|\; \begin{bmatrix} 1 & 0 \\ 0 & C \\ CB & CA \end{bmatrix} \begin{bmatrix} x_a \\ x \end{bmatrix} = x_{g_2} \right\} \tag{5.162}$$

is a full simulation relation of $\mathrm{A}_2 \wedge \Sigma$ by Γ_2. To show this, let $(x_a, x, x_{g_2}) \in \mathcal{S}$ and $d_a \in \mathbb{R}$. In view of Proposition 5.2, we need to find $d_{g_2} \in \mathbb{R}^2$ such that

$$\begin{bmatrix} 1 & 0 \\ 0 & C \\ CB & CA \end{bmatrix} \left(\begin{bmatrix} 0 & 0 \\ B & A \end{bmatrix} \begin{bmatrix} x_a \\ x \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} d_a \right) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} x_{g_2} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} d_{g_2}. \tag{5.163}$$

From the first and third rows of the latter, we obtain

$$d_{g_2} = \begin{bmatrix} 1 & 0 \\ CB & CA \end{bmatrix} \left(\begin{bmatrix} 0 & 0 \\ B & A \end{bmatrix} \begin{bmatrix} x_a \\ x \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} d_a \right), \tag{5.164}$$

while the second row reads

$$\begin{bmatrix} CB & CA \end{bmatrix} \begin{bmatrix} x_a \\ x \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} x_{g_2}, \tag{5.165}$$

which holds by definition of $\mathcal{S}$. In other words, $d_{g_2} \in \mathbb{R}^2$, as defined in (5.164), is such that (5.163) holds. Furthermore, by definition of $\mathcal{S}$, we have that

$$\begin{bmatrix} 1 & 0 \\ 0 & C \end{bmatrix} \begin{bmatrix} x_a \\ x \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} x_{g_2}, \tag{5.166}$$

hence, due to Proposition 5.2, $\mathcal{S}$ is a simulation relation of $\mathrm{A}_2 \wedge \Sigma$ by Γ_2. As $\pi_{\mathbb{R}\times\mathbb{R}^n}(\mathcal{S}) = \mathbb{R} \times \mathbb{R}^n$, it follows that $\mathcal{S}$ is a full simulation relation. This implies that $\mathrm{A}_2 \wedge \Sigma \preccurlyeq \Gamma_2$ and thus, Σ implements $\mathcal{C}_2$.

We have shown that any input-state-output system Σ implements $\mathcal{C}_2$, hence $\mathcal{C}_1$ refines $\mathcal{C}_2$. However, it is not true that $\mathrm{A}_2 \wedge \Gamma_1 \preccurlyeq \Gamma_2$. To see this, note that

$$\mathrm{A}_2 \wedge \Gamma_1 : \begin{cases} \begin{bmatrix} \dot{x}_a \\ \dot{x}_{g_1} \end{bmatrix} = \begin{bmatrix} d_a \\ d_{g_1} \end{bmatrix}, \\ \qquad u = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_a \\ x_{g_1} \end{bmatrix}, \\ \qquad y = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_a \\ x_{g_1} \end{bmatrix}, \\ \qquad 0 = \begin{bmatrix} 1 & -1 & 0 \end{bmatrix} \begin{bmatrix} x_a \\ x_{g_1} \end{bmatrix}. \end{cases} \tag{5.167}$$

It is easy to verify that the consistent subspace of $\mathrm{A}_2 \wedge \Gamma_1$ is given by

$$\mathcal{V}_{ag} = \ker \begin{bmatrix} 1 & -1 & 0 \end{bmatrix}. \tag{5.168}$$

With this in mind, we will show that $\mathrm{A}_2 \wedge \Gamma_1$ is not simulated by Γ_2 by contradiction. Suppose that $\mathrm{A}_2 \wedge \Gamma_1 \preccurlyeq \Gamma_2$. Let $\mathcal{S}'$ be a full simulation relation of $\mathrm{A}_2 \wedge \Gamma_1$ by Γ_2. By definition of simulation relation, we have that $\pi_{\mathbb{R}\times\mathbb{R}^2}(\mathcal{S}') = \mathcal{V}_{ag}$. Furthermore, if $(x_a(0), x_{g_1}(0), x_{g_2}(0)) \in \mathcal{S}'$, then for all $d_a(\cdot)$ and $d_{g_1}(\cdot)$ such that $(x_a(t), x_{g_1}(t)) \in \mathcal{V}_{ag}$ for all $t \geq 0$, there exists $d_{g_2}(\cdot)$ such that

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_a(t) \\ x_{g_1}(t) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} x_{g_2}(t), \qquad \text{for all } t \geq 0, \tag{5.169}$$

where $(x_a(t), x_{g_1}(t))$ is the corresponding state trajectory of $\mathrm{A}_2 \wedge \Gamma_1$ and $x_{g_2}(t)$ is the corresponding state trajectory of Γ_2.

Now, let $(x_a(0), x_{g_1}(0), x_{g_2}(0)) \in \mathcal{S}'$. Then, $(x_a(0), x_{g_1}(0)) \in \mathcal{V}_{ag}$, hence $x_a(0) = x_{g_1,1}(0)$, where $x_{g_1,1}(t)$ is the first entry of $x_{g_1}(t)$. Consequently, for any $d_a(\cdot)$ and any $d_{g_1,2}(\cdot)$, we have that

$$d_{g_1}(t) = \begin{bmatrix} d_a(t) \\ d_{g_1,2}(t) \end{bmatrix}, \tag{5.170}$$

is such that $x_a(t) = x_{g_1,1}(t)$ for all $t \geq 0$, hence $(x_a(t), x_{g_1}(t)) \in \mathcal{V}_{ag}$ for all $t \geq 0$. Let $d_a(\cdot)$ be arbitrary and define $d_{g_2}(\cdot)$ as above with $d_{g_1,2}(\cdot)$ such that $d_{g_1,2}(0) \neq x_{g_2,3}(0)$, where $x_{g_2,3}(t)$ is the third entry of $x_{g_2}(t)$. Note that

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \dot{x}_a(0) \\ \dot{x}_{g_1}(0) \end{bmatrix} = \begin{bmatrix} d_a(0) \\ d_{g_1,2}(0) \end{bmatrix}. \tag{5.171}$$

On the other hand,

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \dot{x}_{g_2}(0) = \begin{bmatrix} d_{g_2,1}(0) \\ x_{g,3}(0) \end{bmatrix}, \tag{5.172}$$

where $d_{g_2,1}(t)$ is the first entry of $d_{g_2}(t)$. Since $d_{g_1,2}(0) \neq x_{g,3}(0)$, there does not exist $d_{g_2}(\cdot)$ such that (5.169). This contradicts the assumption that $\mathcal{S}'$ is a full simulation relation, hence $\mathrm{A}_2 \wedge \Gamma_1$ is not simulated by Γ_2. This shows that the condition $\mathrm{A}_2 \wedge \Gamma_1 \preccurlyeq \Gamma_2$ is not necessary for refinement.

The above example shows that the condition $\mathrm{A}_2 \wedge \Gamma_1 \preccurlyeq \Gamma_1$ is not necessary for $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ to refine $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ when treated as simulation contracts whose implementations are restricted to input-state-output systems. Nevertheless, it can be shown that the behavioural counterpart of this condition is actually still necessary, i.e., it is still necessary to have $\mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_1) \subset \mathfrak{B}(\Gamma_2)$ for $\mathcal{C}_1$ to refine $\mathcal{C}_2$, even when treated as simulation contracts. It is worthwhile noting that the condition $\mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_1) \subset \mathfrak{B}(\Gamma_2)$ is not sufficient for $\mathcal{C}_1$ to refine $\mathcal{C}_2$. This means that, if it can be formulated, the true necessary and sufficient condition is stronger than $\mathfrak{B}(\mathrm{A}_2 \wedge \Gamma_1) \subset \mathfrak{B}(\Gamma_2)$ but weaker than $\mathrm{A}_2 \wedge \Gamma_1 \preccurlyeq \Gamma_2$.

The fact that the second condition in Theorem 5.4 is not necessary for refinement when implementations are restricted to input-state-output systems has consequences for the series composition as well. In particular, without necessary conditions for refinement, it is difficult to obtain necessary conditions for series composability. Furthermore, even if such conditions are obtained, it is difficult to obtain an explicit expression for the series composition, i.e., it is unclear how one can determine the smallest contract that satisfies Implication 5.1.

In conclusion, the behavioural contracts in Chapter 3 and the simulation contracts in this chapter are very similar. They define almost the same type of specification, with the only difference being the fact that simulation is a stronger notion than behavioural inclusion for non-deterministic systems. One consequence of this is that the classes of compatible environments and

implementations are enlarged when a simulation contract is interpreted as a behavioural contract. Of course, this is the case only when we restrict implementations to be input-state-output systems without a driving variable. Unfortunately, with this restriction in place, we no longer have tractable necessary conditions for refinement and, thus, for series composability. Still, this is a somewhat minor disadvantage that is offset by the added computational efficiency when using simulation instead of behavioural inclusion to define contracts.

5.9 Discussion

We presented assume-guarantee contracts for linear dynamical input-state-output systems. Using the notion of simulation, we defined and characterized contract implementation via system comparison with the assumptions and guarantees. This allowed us to efficiently verify contract implementation by using the (controlled) invariant subspace algorithm to verify simulation. Then, we turned away from verification and considered two problems in contract-based design.

First, we considered the problem of constructing an implementation for a given contract. In particular, we showed that a contract is consistent, i.e., it has an implementation, if and only if a pair of subspaces with certain geometric properties exists. We provided a systematic procedure to verify the existence of these subspaces. Additionally, we provided a systematic procedure for constructing a particular implementation when these subspaces exist.

Second, we considered the problem where a given contract is a specification for a given plant system. The premise was that the plant system does not necessarily implement the contract but can be controlled to achieve implementation. We showed that this is possible if and only if a pair of subspaces that satisfy certain properties exists. These properties were very similar to the ones for consistency, which allowed us to use the same ideas to provide a systematic procedure for verifying the existence of a controller that turns the plant system into an implementation of the contract. Given these subspaces, we also provided a systematic procedure for constructing an appropriate controller.

Finally, we made first steps towards enabling independent design of components within interconnected systems by introducing notions of refinement and series composition for contracts. We obtained necessary and sufficient conditions for refinement involving only assumptions and guarantees. Similarly, we also obtained necessary and sufficient conditions for the existence of the series composition, and we provided an explicit expression for it when it exists. All relevant conditions are in terms of simulation involving only assumptions and guarantees, hence they can be verified efficiently.

This chapter contains some fundamental results related to the development of a contract design, which we would like to extend to a complete instantiation of the meta-theory. To this end, we would need a notion of composition that allows more general interconnections to be treated. Furthermore, it would be worthwhile to address the problem of interconnected system design using contracts, i.e., how to pick contracts for components based on the contract for their interconnection.

Chapter 6

Conclusion

In this thesis, we introduced assume-guarantee contracts for linear dynamical systems with inputs and outputs. These contracts are defined as a pair of linear systems called assumptions and guarantees, and are used to express specifications for components through two aspects. First, the assumptions represent the expected dynamics of the environment in which a component operates, thus leading to a class of compatible environments. Second, the guarantees represent the required dynamics of the component when interconnected with a compatible environment, thus leading to a class of implementations. The classes of compatible environments and implementations are obtained by comparison with the assumptions and guarantees. For this comparison, we considered two notions: behavioural inclusion and simulation. Following the meta-theory outlined in Chapter 2, we developed a contract theory using each of these two notions.

We began in Chapter 3, where we defined contracts using behaviours and behavioural inclusion, referred to as behavioural contracts. The main contribution of this chapter was in developing a theory of behavioural contracts as specifications. Specifically, we defined and characterized notions of implementation, refinement, and conjunction, which allow us to express, compare and combine specifications using contracts. We characterized implementation and refinement as behavioural inclusions involving only assumptions and guarantees. We showed how these inclusions can be verified algorithmically and, thus, how implementation and refinement can be verified algorithmically. Moreover, we found necessary and sufficient conditions under which a contract is consistent, i.e., it has an implementation. In the process, we also obtained a systematic procedure for constructing an implementation of a consistent contract, thus allowing behavioural contracts to be used for design, not only verification. On the other hand, we showed that the conjunction of two arbitrary contracts does not necessarily exist. Nevertheless, we presented two special cases where the conjunction exists, and we pro-

vided an explicit expression for it in these cases.

We continued in Chapter 4 by further developing the theory of behavioural contracts to enable the independent design of components within interconnected systems. To this end, we defined and characterized two notions of contract composition based on two types of system interconnections: series and feedback. The purpose of the composition was to allow us to reason about the contract that an interconnection implements based on the contracts that its components implement. Indeed, a defining property of the composition of two contracts is that it is implemented by an interconnection of any of the implementations of the two contracts. In addition to that, we required the composition to be the smallest such contract with respect to refinement. This meant that the composition expresses the strictest specification that the interconnection of arbitrary implementations is guaranteed to satisfy. We showed that neither composition necessarily exists, but we provided a necessary and sufficient condition for its existence. This took the form of a behavioural inclusion, which can be verified algorithmically, thus allowing the existence of each composition to be verified algorithmically. Furthermore, we provided an explicit expression for each composition when it exists.

The behavioural contract theory developed in Chapter 3 and Chapter 4 is a complete instantiation of the meta-theory outlined in Chapter 2. It contains definitions and characterizations of all notions that enable the use of contracts for expressing specifications and for independent design of components within interconnected systems. It is also equipped with algorithms for verification and systematic procedures for design. However, there were some limitations. Namely, the algorithms for verification are not necessarily efficient, and the systematic procedures for design do not lend themselves to other problems related to contract based-design. To address these limitations, we took a slightly different approach and defined contracts using simulation instead of behavioural inclusion, hereafter referred to as simulation contracts. The motivation behind this was based on the fact that, unlike behavioural inclusion, simulation is supported by efficient numerical procedures for verification, namely, the (controlled) invariant subspace algorithm. Furthermore, simulation has a strong connection to geometric control theory and, specifically, controlled and conditioned invariant subspaces. This allows us to use a multitude of existing techniques in tackling problems related to contract-based design.

With this in mind, in Chapter 5, we defined and characterized notions of implementation, refinement, and series composition for simulation contracts. The characterizations of implementation, refinement, and the existence of the series composition were in terms of simulation conditions involving only assumptions and guarantees. As simulation can be verified efficiently, this means that simulation contracts are supported by efficient algorithms for verification. On the other hand, we treated two problems related to contract-

based design. First, we considered the problem of designing an implementation for a given contract. We found necessary and sufficient conditions under which an implementation exists, i.e., the contract is consistent, and we provided a systematic procedure for the construction of an implementation when it exists. Second, we considered the problem of designing a controller that turns a given plant system into an implementation of a given contract. We found necessary and sufficient conditions under which such a controller exists, and we provided a systemic procedure for its construction when it exists. We also illustrated this procedure with a simple example of a vehicle following system. For both design problems, we made extensive use of the notions of controlled and conditioned invariance, as well as the construction techniques related to them.

6.1 Future research

For the simulation contract theory developed in Chapter 5 to become a complete instantiation of the meta-theory, we still require a notion of composition that is more general than the simple series composition, e.g., feedback composition. In Chapter 4, we saw that the feedback composition of behavioural contracts is much more difficult to characterize than the series composition because the feedback interconnection contains a loop. The same difficulty remains when trying to characterize the feedback composition of simulation contracts. However, we note that the results on the feedback composition of behavioural contracts are a good indication of what we can expect from the feedback composition of simulation contracts. Indeed, we already saw that the results on implementation, refinement, and the series composition for simulation contracts are very similar to the ones for behavioural contracts.

As already mentioned in the conclusion of Chapter 4, our results allow us to only *verify* that implementation of *given* local contracts for the components leads to the implementation of a given global contract for the interconnected system. In practice, it is often necessary to *design* local contracts whose implementation leads to the implementation of a given global contract. In view of our results, this amounts to designing local contracts whose composition refines the global contract. Note that this problem is not well-posed without restrictions on the interconnection topology and the choice of local contracts. Indeed, we can always insert an arbitrarily long series of identity components between any two components in an interconnected system without changing the behaviour of the overall system. With this in mind, we recommend considering the following problem: given an interconnection topology, a global contract, and a set of available local contracts, choose local contracts for all components such that their composition refines the global contract.

Finally, we suggest a few extensions and modifications of the contract theory presented in this thesis. First, the theory can be extended to different

system classes. In particular, since bisimulation is also characterized for nonlinear systems [65], an extension of simulation contracts to nonlinear systems seems attainable. On the other hand, an extension to systems with inequality constraints will be particularly relevant in the design of, e.g., smart grids, which impose limits on voltage, current, power flow and frequency. Second, the theory can be modified by using a different notion for system comparison. Note that both behavioural inclusion and simulation are notions for *exact* system comparison. Since models are rarely an exact representation of reality, a model satisfying a specification expressed by exact comparison does not guarantee that the corresponding physical component also satisfies the specification. To deal with this, we can use a method for comparison that guarantees a more robust relationship between systems, such as approximate bisimulation [89–92] or (γ, δ)-similarity [93].

Appendix A

Lemmas

In this chapter of the appendix, we will prove a few technical lemmas that are used in the proofs in Appendix B. We start with the following lemma, which is used in the proof of Proposition 4.2, see Appendix B.2.

Lemma A.1. *Suppose that the matrices*

$$\begin{bmatrix} A_1 & A_2 \end{bmatrix}, \quad \begin{bmatrix} D_1 & D_2 \end{bmatrix} \quad \textit{and} \quad \begin{bmatrix} A_1 & A_2 & B_1 & 0 \\ 0 & C_1 & D_1 & D_2 \end{bmatrix} \tag{A.1}$$

have full row rank. Then there exist matrices A_3, A_4, B_2, C_2, D_3 and D_4 such that the matrices

$$\begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix}, \quad \begin{bmatrix} D_1 & D_2 \\ D_3 & D_4 \end{bmatrix} \quad \textit{and} \quad \begin{bmatrix} A_1 & A_2 & B_1 & 0 \\ A_3 & A_4 & B_2 & 0 \\ 0 & C_1 & D_1 & D_2 \\ 0 & C_2 & D_3 & D_4 \end{bmatrix} \tag{A.2}$$

are square and invertible.

Proof. We will assume that A_1 and D_2 do not have full row rank. The case where one or both of them do have full row rank follows a similar reasoning. With this in mind, since A_1 and D_2 do not have full row rank, there exist square and invertible matrices T_A and T_D such that

$$T_A A_1 = \begin{bmatrix} A_{11} \\ 0 \end{bmatrix} \quad \text{and} \quad T_D D_2 = \begin{bmatrix} D_{21} \\ 0 \end{bmatrix}, \tag{A.3}$$

where A_{11} and D_{21} have full row rank. Let

$$\begin{bmatrix} A_{21} \\ A_{22} \end{bmatrix} = T_A A_2 \quad \text{and} \quad \begin{bmatrix} D_{11} \\ D_{12} \end{bmatrix} = T_D D_1, \tag{A.4}$$

and note that, since T_A and T_D are invertible, the matrices

$$T_A \begin{bmatrix} A_1 & A_2 \end{bmatrix} = \begin{bmatrix} A_{11} & A_{21} \\ 0 & A_{22} \end{bmatrix} \quad \text{and} \quad T_D \begin{bmatrix} D_1 & D_2 \end{bmatrix} = \begin{bmatrix} D_{11} & D_{21} \\ D_{12} & 0 \end{bmatrix}, \tag{A.5}$$

have full row rank, hence A_{22} and D_{12} have full row rank. Similarly, let

$$\begin{bmatrix} B_{11} \\ B_{12} \end{bmatrix} = T_A B_1 \quad \text{and} \quad \begin{bmatrix} C_{11} \\ C_{12} \end{bmatrix} = T_D C_1 \tag{A.6}$$

and note that the matrix

$$\begin{bmatrix} T_A & 0 \\ 0 & T_D \end{bmatrix} \begin{bmatrix} A_1 & A_2 & B_1 & 0 \\ 0 & C_1 & D_1 & D_2 \end{bmatrix} = \begin{bmatrix} A_{11} & A_{21} & B_{11} & 0 \\ 0 & A_{22} & B_{12} & 0 \\ 0 & C_{11} & D_{11} & D_{21} \\ 0 & C_{12} & D_{12} & 0 \end{bmatrix}, \tag{A.7}$$

has full row rank, hence

$$\begin{bmatrix} A_{22} & B_{12} \\ C_{12} & D_{12} \end{bmatrix} \tag{A.8}$$

has full row rank. Since A_{11} and D_{21} have full row rank, there exist matrices A_{31} and D_{41} such that

$$\begin{bmatrix} A_{11} \\ A_{31} \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} D_{21} \\ D_{41} \end{bmatrix} \tag{A.9}$$

are square and invertible. Let

$$A_3 = \begin{bmatrix} A_{31} \\ 0 \end{bmatrix}, \quad A_4 = \begin{bmatrix} 0 \\ A_{42} \end{bmatrix}, \quad D_3 = \begin{bmatrix} 0 \\ D_{32} \end{bmatrix} \quad \text{and} \quad D_4 = \begin{bmatrix} D_{41} \\ 0 \end{bmatrix}, \tag{A.10}$$

where the matrices A_{42} and D_{32} are to be determined. Note that

$$\begin{bmatrix} T_A & 0 \\ 0 & I \end{bmatrix} \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix} = \begin{bmatrix} A_{11} & A_{21} \\ 0 & A_{22} \\ A_{31} & 0 \\ 0 & A_{42} \end{bmatrix} \tag{A.11}$$

is square and invertible if and only if

$$\begin{bmatrix} A_{22} \\ A_{42} \end{bmatrix} \tag{A.12}$$

is square and invertible. Similarly,

$$\begin{bmatrix} T_D & 0 \\ 0 & I \end{bmatrix} \begin{bmatrix} D_1 & D_2 \\ D_3 & D_4 \end{bmatrix} = \begin{bmatrix} D_{11} & D_{21} \\ D_{12} & 0 \\ 0 & D_{41} \\ D_{32} & 0 \end{bmatrix} \tag{A.13}$$

is square and invertible if and only if

$$\begin{bmatrix} D_{12} \\ D_{32} \end{bmatrix} \tag{A.14}$$

is square and invertible. Furthermore, let

$$B_2 = \begin{bmatrix} 0 \\ B_{22} \end{bmatrix} \quad \text{and} \quad C_2 = \begin{bmatrix} 0 \\ C_{22} \end{bmatrix}, \tag{A.15}$$

where the matrices B_{22} and C_{22} are to be determined, and note that

$$\begin{bmatrix} T_A & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & T_D & 0 \\ 0 & 0 & 0 & I \end{bmatrix} \begin{bmatrix} A_1 & A_2 & B_1 & 0 \\ A_3 & A_4 & B_2 & 0 \\ 0 & C_1 & D_1 & D_2 \\ 0 & C_2 & D_3 & D_4 \end{bmatrix} = \begin{bmatrix} A_{11} & A_{21} & B_{11} & 0 \\ 0 & A_{22} & B_{12} & 0 \\ A_{31} & 0 & 0 & 0 \\ 0 & A_{42} & B_{22} & 0 \\ 0 & C_{11} & D_{11} & D_{21} \\ 0 & C_{12} & D_{12} & 0 \\ 0 & 0 & 0 & D_{41} \\ 0 & C_{22} & D_{32} & 0 \end{bmatrix} \tag{A.16}$$

is square and invertible if and only if

$$\begin{bmatrix} A_{22} & B_{12} \\ A_{42} & B_{22} \\ C_{12} & D_{12} \\ C_{22} & D_{32} \end{bmatrix} \tag{A.17}$$

is square and invertible. Therefore, the matrices in (A.2) are square and invertible if and only if the matrices in (A.12), (A.14) and (A.17) are square and invertible, where A_{42}, B_{22}, C_{22} and D_{32} are to be determined. Now, since A_{22} and D_{12} have full row rank, there exist matrices A'_{42} and D'_{32} such that

$$\begin{bmatrix} A_{22} \\ A'_{42} \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} D_{12} \\ D'_{32} \end{bmatrix} \tag{A.18}$$

are square and invertible. Similarly, since (A.8) has full row rank, there exist matrices A''_{42}, B_{22}, C_{22} and D''_{32} such that

$$\begin{bmatrix} A_{22} & B_{12} \\ A''_{42} & B_{22} \\ C_{12} & D_{12} \\ C_{22} & D''_{32} \end{bmatrix} \tag{A.19}$$

is square and invertible. With this in mind, consider the matrices

$$A_{42}(\lambda) = \lambda A'_{42} + (1-\lambda)A''_{42} \quad \text{and} \quad D_{32}(\lambda) = \lambda D'_{32} + (1-\lambda)D''_{32}, \tag{A.20}$$

where $\lambda \in \mathbb{R}$. Since the matrices

$$\begin{bmatrix} A_{22} \\ A_{42}(\lambda) \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} D_{12} \\ D_{32}(\lambda) \end{bmatrix} \tag{A.21}$$

are invertible for $\lambda = 1$, it follows that they are invertible for all but finitely many $\lambda \in \mathbb{R}$. Similarly, the matrix

$$\begin{bmatrix} A_{22} & B_{12} \\ A_{42}(\lambda) & B_{22} \\ C_{12} & D_{12} \\ C_{22} & D_{32}(\lambda) \end{bmatrix} \tag{A.22}$$

is invertible for $\lambda = 0$, hence it is invertible for all but finitely many $\lambda \in \mathbb{R}$. This means that there exists $\bar{\lambda} \in \mathbb{R}$ such that both the matrices in (A.21) and (A.22) are invertible for $\lambda = \bar{\lambda}$. Therefore, the matrices

$$A_{42} = A_{42}(\bar{\lambda}) \quad \text{and} \quad D_{32} = D_{32}(\bar{\lambda}) \tag{A.23}$$

are such that (A.12), (A.14) and (A.17) are square and invertible, hence the matrices in (A.2) are square and invertible, as desired. □

The following lemma is used in the proofs of Lemma 4.6 and Lemma 4.10, see Appendix B.4 and Appendix B.7, respectively.

Lemma A.2. *Consider polynomial matrices $G(s)$ and $H(s)$. Suppose that $G(s)$ is row-reduced, that is,*

$$G(s) = D(s)G^h + G^l(s), \tag{A.24}$$

where $D(s)$ is the row-degree matrix of $G(s)$, G^h is a full row rank real matrix, and $G^l(s)$ is a polynomial matrix such that $D(s)^{-1}G^l(s)$ is strictly proper. Furthermore, suppose that

$$\lim_{s\to\infty} D(s)^{-1}(G(s) + H(s)) \tag{A.25}$$

exist and has full row rank. Then

$$N(s)\,(G(s) + H(s)) = G(s)R(s) \tag{A.26}$$

for some proper invertible rational matrix $R(s)$ only if $N(s)$ is unimodular.

Proof. Let

$$\lim_{s\to\infty} D(s)^{-1}(G(s) + H(s)) = \hat{G}^h \tag{A.27}$$

and note that since $\hat{G}^h$ has full row rank, it follows that $D(s)^{-1}(G(s) + H(s))$ and, thus $G(s) + H(s)$, have full row rank. This means that

$$(G(s) + H(s))\,(G(s) + H(s))^\top \tag{A.28}$$

is invertible and (A.26) holds only if

$$N(s) = G(s)R(s)\left(G(s)+H(s)\right)^\top \left(\left(G(s)+H(s)\right)\left(G(s)+H(s)\right)^\top\right)^{-1}. \tag{A.29}$$

Taking the determinant on both sides yields

$$\det N(s) = \frac{\det\left(G(s)R(s)\left(G(s)+H(s)\right)^\top\right)}{\det\left(\left(G(s)+H(s)\right)\left(G(s)+H(s)\right)^\top\right)}. \tag{A.30}$$

Note that we can pre- and post-multiply the numerator and denominator of the latter by $\det D(s)^{-1}$ to obtain

$$\det N(s) = \frac{\det\left(D(s)^{-1}G(s)R(s)\left(\left(G(s)+H(s)\right)\right)^\top D(s)^{-\top}\right)}{\det\left(D(s)^{-1}\left(G(s)+H(s)\right)\left(G(s)+H(s)\right)^\top D(s)^{-\top}\right)}. \tag{A.31}$$

The denominator of the latter converges to

$$\det\left(\hat{G}^h(\hat{G}^h)^\top\right) \neq 0 \tag{A.32}$$

as $s \to \infty$ because of (A.27). Since $R(s)$ is proper, it follows that

$$\lim_{s\to\infty} R(s) = R_\infty, \tag{A.33}$$

whereas

$$\lim_{s\to\infty} D(s)^{-1}G(s) = G^h. \tag{A.34}$$

because $D(s)^{-1}G^l(s)$ is strictly proper. Therefore,

$$\lim_{s\to\infty} \det N(s) = \frac{\det\left(G^h R_\infty(\hat{G}^h)^\top\right)}{\det\left(\hat{G}^h(\hat{G}^h)^\top\right)}, \tag{A.35}$$

which, since $\det N(s)$ is a polynomial, holds if and only if $\det N(s)$ is constant. Furthermore, $G(s)$ has full row rank and $R(s)$ is invertible, hence $G(s)R(s)$ has full row rank and so $N(s)$ must also have full row rank. This implies that $\det N(s) \neq 0$ and, thus, that $N(s)$ is unimodular. □

Appendix B

Proofs

B.1 Proof of Proposition 4.1

The feedback interconnection $\Sigma_1 \leftarrow\!\!\rightarrow \Sigma_2$, as defined in Definition 4.3, is well-posed if and only if

$$\lim_{s\to\infty} I - P(s)^{-1}Q_{\mathrm{i}}(s) \tag{4.21}$$

exists and is invertible.

Proof. We begin by proving sufficiency. Suppose that (4.21) is invertible. Due to Proposition 3.3, this implies that $I-P(s)^{-1}Q_{\mathrm{i}}(s)$ is invertible and its inverse $(I - P(s)^{-1}Q_{\mathrm{i}}(s))^{-1}$ is proper. Since Σ_1 and Σ_2 are in input-output form, it follows that $P(s)^{-1}Q_{\mathrm{e}}(s)$ and $P(s)^{-1}Q_{\mathrm{v}}(s)$ are proper, where $Q_{\mathrm{v}}(s)$ is given by (4.16). This implies that the rational matrix

$$\left(P(s) - Q_{\mathrm{i}}(s)\right)^{-1} Q_{\mathrm{e}}(s) = (I - P(s)^{-1}Q_{\mathrm{i}}(s))^{-1}P(s)^{-1}Q_{\mathrm{e}}(s) \tag{B.1}$$

is proper as a product of proper rational matrices. Similarly, the rational matrix

$$\left(P(s) - Q_{\mathrm{i}}(s)\right)^{-1} Q_{\mathrm{v}}(s) = (I - P(s)^{-1}Q_{\mathrm{i}}(s))^{-1}P(s)^{-1}Q_{\mathrm{v}}(s) \tag{B.2}$$

is also proper, hence $\Sigma_1 \leftarrow\!\!\rightarrow \Sigma_2$ is well-posed.

We proceed by proving necessity. Suppose that $\Sigma_1 \leftarrow\!\!\rightarrow \Sigma_2$ is well-posed. This means that $I - P(s)^{-1}Q_{\mathrm{i}}(s)$ is invertible and $\left(P(s) - Q_{\mathrm{i}}(s)\right)^{-1} Q_{\mathrm{v}}(s)$ is proper. The latter implies that $\left(P(s) - Q_{\mathrm{i}}(s)\right)^{-1} Q_{\mathrm{i}}(s)$ is proper because

$$Q_{\mathrm{i}}(s) = \begin{bmatrix} 0 & Q_{\mathrm{v}}(s) & 0 \end{bmatrix}. \tag{B.3}$$

With this in mind, let

$$R(s) = \left(P(s) - Q_{\mathrm{i}}(s)\right)^{-1} Q_{\mathrm{i}}(s) \tag{B.4}$$

$$= \left(I - P(s)^{-1}Q_{\mathrm{i}}(s)\right)^{-1} P(s)^{-1}Q_{\mathrm{i}}(s), \tag{B.5}$$

so that we can write

$$\left(I - P(s)^{-1}Q_{\mathrm{i}}(s)\right) R(s) = P(s)^{-1}Q_{\mathrm{i}}(s). \tag{B.6}$$

Since $R(s)$ and $P(s)^{-1}Q_{\mathrm{i}}(s)$ are proper it follows that

$$\lim_{s\to\infty} R(s) = R_\infty \quad \text{and} \quad \lim_{s\to\infty} P(s)^{-1}Q_{\mathrm{i}}(s) = T_\infty \tag{B.7}$$

for some real matrices R_∞ and T_∞. Then, taking the limit of (B.6) as $s \to \infty$ yields

$$(I - T_\infty)\, R_\infty = T_\infty. \tag{B.8}$$

The latter implies that $I - T_\infty$ is invertible. Indeed, if x is vector such that

$$x^\top (I - T_\infty) = 0, \tag{B.9}$$

then, due to (B.8), it follows that $x^\top T_\infty = 0$, which we can substitute in (B.9) to obtain $x = 0$. This concludes the proof since (4.21) is equal to $I - T_\infty$. □

B.2 Proof of Proposition 4.2

Suppose that the guarantees Γ_1 and Γ_2 given by (4.2) are such that $G_1(s)$ and $G_2(s)$ are row-reduced. The feedback interconnection $\Gamma_1 \hookleftarrow \Gamma_2$, as defined in Definition 4.5, is well-posed if and only if $D(s)^{-1}H_{\mathrm{e}}(s)$ is proper and

$$\lim_{s\to\infty} D(s)^{-1}\left(G(s) - H_{\mathrm{i}}(s)\right) \tag{4.31}$$

exists and has full row rank, where $D(s)$ is the row-degree matrix of $G(s)$.

Proof. We begin by proving necessity. Suppose that $\Gamma_1 \hookleftarrow \Gamma_2$ is well-posed, that is, there exist input-output systems Σ_1 and Σ_2 such that $\mathfrak{B}(\Sigma_1) \subset \mathfrak{B}(\Gamma_1)$, $\mathfrak{B}(\Sigma_2) \subset \mathfrak{B}(\Gamma_2)$, and the feedback interconnection $\Sigma_1 \hookleftarrow \Sigma_2$, as defined in Definition 4.3, is well-posed. Since $\mathfrak{B}(\Sigma_1) \subset \mathfrak{B}(\Gamma_1)$ and $\mathfrak{B}(\Sigma_2) \subset \mathfrak{B}(\Gamma_2)$, there exist polynomial matrices $M_1(s)$ and $M_2(s)$ such that

$$\begin{bmatrix} G_1(s) & -H_1(s) \end{bmatrix} = M_1(s) \begin{bmatrix} P_1(s) & -Q_1(s) \end{bmatrix}, \tag{B.10}$$

$$\begin{bmatrix} G_2(s) & -H_2(s) \end{bmatrix} = M_2(s) \begin{bmatrix} P_2(s) & -Q_2(s) \end{bmatrix}. \tag{B.11}$$

In particular, this means that the polynomial matrix

$$M(s) = \begin{bmatrix} M_1(s) & 0 \\ 0 & M_2(s) \end{bmatrix} \tag{B.12}$$

is such that

$$G(s) = M(s)P(s), \quad H_{\mathrm{i}}(s) = M(s)Q_{\mathrm{i}}(s), \quad H_{\mathrm{e}}(s) = M(s)Q_{\mathrm{e}}(s). \tag{B.13}$$

Consequently, we have that

$$D(s)^{-1}H_{\mathrm{e}}(s) = D(s)^{-1}M(s)Q_{\mathrm{e}}(s) = D(s)^{-1}G(s)P(s)^{-1}Q_{\mathrm{e}}(s). \tag{B.14}$$

Note that $D(s)^{-1}G(s)$ is proper because $D(s)$ is the row-degree matrix of $G(s)$, whereas $P(s)^{-1}Q_{\mathrm{e}}(s)$ is proper because Σ_1 and Σ_2 are in input-output form. Therefore, $D(s)^{-1}H_{\mathrm{e}}(s)$ is proper as the product of proper rational matrices. On the other hand, we have that

$$D(s)^{-1}\left(G(s) - H_{\mathrm{i}}(s)\right) = D(s)^{-1}M(s)\left(P(s) - Q_{\mathrm{i}}(s)\right) \tag{B.15}$$

$$= D(s)^{-1}G(s)\left(I - P(s)^{-1}Q_{\mathrm{i}}(s)\right). \tag{B.16}$$

Note that

$$D(s) = \begin{bmatrix} D_1(s) & 0 \\ 0 & D_2(s) \end{bmatrix}, \tag{B.17}$$

where $D_1(s)$ and $D_2(s)$ are the row-degree matrices of $G_1(s)$ and $G_2(s)$, respectively. Since $G_1(s)$ and $G_2(s)$ are row-reduced, it follows that $G(s)$ is row-reduced and thus

$$\lim_{s\to\infty} D(s)^{-1}G(s) = G^h \tag{B.18}$$

for some real full row rank matrix G^h. Furthermore, as Σ_1 and Σ_2 are in input-output form, it follows that $P(s)^{-1}Q_{\mathrm{i}}(s)$ is proper and, thus,

$$\lim_{s\to\infty} P(s)^{-1}Q_{\mathrm{i}}(s) = T_\infty \tag{B.19}$$

for some real matrix T_∞. In view of Proposition 4.1 and the assumption that $\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2$ is well-posed, it follows that $I - T_\infty$ is invertible. Consequently, by using (B.16), we obtain

$$\lim_{s\to\infty} D(s)^{-1}\left(G(s) - H_{\mathrm{i}}(s)\right) = G^h(I - T_\infty), \tag{B.20}$$

which has full row rank.

We proceed by proving sufficiency. Suppose that $D(s)^{-1}H_{\mathrm{e}}(s)$ is proper and (4.31) exists and has full row rank. For each $j \in \{1, 2\}$, as $G_j(s)$ is row-reduced, we can write

$$G_j(s) = D_j(s)G_j^h + G_j^l(s), \tag{B.21}$$

where $D_j(s)$ is the row-degree matrix of $G_j(s)$, G_j^h is a real full row rank matrix, and $G_j^l(s)$ is a polynomial matrix such that $D_j(s)^{-1}G_j^h$ is strictly proper. Since $D(s)^{-1}G(s)$ is proper and (4.31) exists, it follows that $D(s)H_{\mathrm{i}}(s)$ is proper. Together with the assumption that $D(s)^{-1}H_{\mathrm{e}}(s)$ is proper, and the fact that (B.17) holds, we have that $D_1(s)^{-1}H_1(s)$ and $D_2(s)^{-1}H_2(s)$ are proper. This means that, for each $j \in \{1, 2\}$, we can write

$$H_j(s) = D_j(s)H_j^h + H_j^l(s), \tag{B.22}$$

for some real matrix H_j^h and a polynomial matrix $H_j^l(s)$ such that $D_j(s)^{-1}H_j^l(s)$ is strictly proper. Now, for each $j \in \{1,2\}$, partition

$$G_j^h = \begin{bmatrix} G_{j1}^h & G_{j2}^h \end{bmatrix} \quad \text{and} \quad H_j^h = \begin{bmatrix} H_{j1}^h & H_{j2}^h \end{bmatrix} \tag{B.23}$$

according to the partition of $G_j(s)$ and $H_j(s)$. Then, we have that

$$\lim_{s\to\infty} D(s)^{-1}\left(G(s) - H_{\mathrm{i}}(s)\right) = \begin{bmatrix} G_{11}^h & G_{12}^h & H_{12}^h & 0 \\ 0 & H_{21}^h & G_{21}^h & G_{22}^h \end{bmatrix} \tag{B.24}$$

has full row rank. Since G_1^h and G_2^h have full row rank as well, Lemma A.1 implies that there exist real matrices $\bar{G}_{11}^h$, $\bar{G}_{12}^h$, $\bar{H}_{12}^h$, $\bar{G}_{21}^h$, $\bar{G}_{22}^h$, and $\bar{H}_{21}^h$ such that the matrices

$$\begin{bmatrix} G_{11}^h & G_{12}^h \\ \bar{G}_{11}^h & \bar{G}_{12}^h \end{bmatrix}, \quad \begin{bmatrix} G_{21}^h & G_{22}^h \\ \bar{G}_{11}^h & \bar{G}_{12}^h \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} G_{11}^h & G_{12}^h & H_{12}^h & 0 \\ \bar{G}_{11}^h & \bar{G}_{12}^h & \bar{H}_{12}^h & 0 \\ 0 & H_{21}^h & G_{21}^h & G_{22}^h \\ 0 & \bar{H}_{21}^h & \bar{G}_{11}^h & \bar{G}_{12}^h \end{bmatrix} \tag{B.25}$$

are square and invertible. With this in mind, let

$$P_1(s) = \begin{bmatrix} D_1(s) & 0 \\ 0 & I \end{bmatrix}\begin{bmatrix} G_{11}^h & G_{12}^h \\ \bar{G}_{11}^h & \bar{G}_{12}^h \end{bmatrix} + \begin{bmatrix} G_1^l(s) \\ 0 \end{bmatrix}, \quad Q_1(s) = \begin{bmatrix} H_{11}(s) & H_{12}(s) \\ 0 & \bar{H}_{12}^h \end{bmatrix},$$
$$P_2(s) = \begin{bmatrix} D_2(s) & 0 \\ 0 & I \end{bmatrix}\begin{bmatrix} G_{21}^h & G_{22}^h \\ \bar{G}_{21}^h & \bar{G}_{22}^h \end{bmatrix} + \begin{bmatrix} G_2^l(s) \\ 0 \end{bmatrix}, \quad Q_2(s) = \begin{bmatrix} H_{21}(s) & H_{22}(s) \\ \bar{H}_{21}^h & 0 \end{bmatrix},$$

and note that $P_1(s)$ and $P_2(s)$ are row-reduced and, thus, invertible due to Proposition 3.8. Then, for each $j \in \{1,2\}$, we have that

$$\begin{bmatrix} G_j(s) & H_j(s) \end{bmatrix} = \begin{bmatrix} I & 0 \end{bmatrix}\begin{bmatrix} P_j(s) & Q_j(s) \end{bmatrix}, \tag{B.26}$$

hence the system

$$\Sigma_j : P_j\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right)y_j = Q_j\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right)u_j \tag{B.27}$$

is such that $\mathfrak{B}(\Sigma_j) \subset \mathfrak{B}(\Gamma_j)$. Furthermore, since $D_1(s)^{-1}H_1(s)$ is proper,

$$\begin{bmatrix} D_1(s) & 0 \\ 0 & I \end{bmatrix}^{-1} Q_1(s) = \begin{bmatrix} D_1(s)^{-1}H_{11}(s) & D_1(s)^{-1}H_{12}(s) \\ 0 & \bar{H}_{12}^h \end{bmatrix} \tag{B.28}$$

is proper, hence, due to Corollary 3.10, $P_1(s)^{-1}Q_1(s)$ is proper and Σ_1 is in input-output form. Similarly, $P_2(s)^{-1}Q_2(s)$ is proper because $D_2(s)^{-1}H_2(s)$ is proper, hence Σ_2 is also in input-output form. The only thing left to show is that $\Sigma_1 \nleftrightarrow \Sigma_2$, as defined in Definition 4.3, is well-posed. To this end, note that

$$I - P(s)^{-1}Q_{\mathrm{i}}(s) = \left(\bar{D}(s)^{-1}P(s)\right)^{-1}\bar{D}(s)^{-1}\left(P(s) - Q_{\mathrm{i}}(s)\right), \tag{B.29}$$

where $\bar{D}(s)$ is the row-degree matrix of $P(s)$, which is given by

$$\bar{D}(s) = \begin{bmatrix} D_1(s) & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & D_2(s) & 0 \\ 0 & 0 & 0 & I \end{bmatrix}. \tag{B.30}$$

As $P_1(s)$ and $P_2(s)$ are row-reduced, we have that $P(s)$ is row-reduced, hence

$$\lim_{s\to\infty} \bar{D}(s)^{-1} P(s) \tag{B.31}$$

is invertible. In view of Proposition 3.3, this means that $(\bar{D}(s)^{-1}P(s))^{-1}$ exists and is proper. In fact, as shown in the proof of Proposition 3.3, we have that

$$\lim_{s\to\infty} \left(\bar{D}(s)^{-1} P(s)\right)^{-1} = \left(\lim_{s\to\infty} \bar{D}(s)^{-1} P(s)\right)^{-1} \tag{B.32}$$

is invertible, which, due to (B.29), implies that

$$\lim_{s\to\infty} I - P(s)^{-1} Q_{\mathrm{i}}(s) \tag{B.33}$$

is invertible if

$$\lim_{s\to\infty} \bar{D}(s)^{-1} \left(P(s) - Q_{\mathrm{i}}(s)\right) \tag{B.34}$$

is invertible. It is straightforward to verify that

$$\lim_{s\to\infty} \bar{D}(s)^{-1} \left(P(s) - Q_{\mathrm{i}}(s)\right) = \begin{bmatrix} G_{11}^h & G_{12}^h & H_{12}^h & 0 \\ \bar{G}_{11}^h & \bar{G}_{12}^h & \bar{H}_{12}^h & 0 \\ 0 & H_{21}^h & G_{21}^h & G_{22}^h \\ 0 & \bar{H}_{21}^h & \bar{G}_{11}^h & \bar{G}_{12}^h \end{bmatrix}, \tag{B.35}$$

which is invertible, hence (B.33) is invertible and, using Proposition 4.1, we conclude that $\Sigma_1 \hookleftarrow \Sigma_2$ is well-posed. □

B.3 Proof of Lemma 4.4

Consider output guarantees Γ and a behaviour $\mathfrak{B}$. If $\mathfrak{B}_{\mathrm{o}}(\Sigma) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma)$ implies $\mathfrak{B}_{\mathrm{o}}(\Sigma) \subset \mathfrak{B}$ for all autonomous Σ, then $\mathfrak{B}_{\mathrm{o}}(\Gamma) \subset \mathfrak{B}$.

Proof. Let Γ and $\mathfrak{B}$ be given by

$$\Gamma : G\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = 0 \quad \text{and} \quad \mathfrak{B} = \left\{ y \in \mathscr{C}_p^\infty \;\middle|\; R\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y = 0 \right\}, \tag{B.36}$$

where $R(s)$ is a polynomial matrix. Because of Remark 3.2, we can assume that $G(s)$ and $R(s)$ have full row rank. In particular, this means that there exists a polynomial matrix $G'(s)$ such that

$$\begin{bmatrix} G(s) \\ G'(s) \end{bmatrix} \tag{B.37}$$

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

$$\Sigma_k : P_k\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right)y = 0, \tag{B.38}$$

is autonomous, where

$$P_k(s) = \begin{bmatrix} I & 0 \\ 0 & s^k I \end{bmatrix}\begin{bmatrix} G(s) \\ G'(s) \end{bmatrix}. \tag{B.39}$$

Furthermore, in view of Proposition 3.13, since

$$G(s) = \begin{bmatrix} I & 0 \end{bmatrix} P_k(s), \tag{B.40}$$

we have that $\mathfrak{B}_{\mathrm{o}}(\Sigma_k) \subset \mathfrak{B}_{\mathrm{o}}(\Gamma)$, which implies that $\mathfrak{B}_{\mathrm{o}}(\Sigma_k) \subset \mathfrak{B}$ by assumption. The latter holds if and only if there exists a polynomial matrix $M_k(s)$ such that

$$R(s) = M_k(s)P_k(s). \tag{B.41}$$

Using (B.39), we find that (B.41) holds if and only if

$$R(s)\begin{bmatrix} G(s) \\ G'(s) \end{bmatrix}^{-1} = M_k(s)\begin{bmatrix} I & 0 \\ 0 & s^k I \end{bmatrix}. \tag{B.42}$$

Note that the left-hand side of (B.42) is independent of k, hence the right-hand side must also be independent of k. Since $M_k(s)$ is a polynomial matrix, this is possible only if

$$M_k(s) = \begin{bmatrix} M_1(s) & 0 \end{bmatrix}, \tag{B.43}$$

for some polynomial matrix $M_1(s)$. Then, (B.42) yields

$$R(s) = \begin{bmatrix} M_1(s) & 0 \end{bmatrix}\begin{bmatrix} G(s) \\ G'(s) \end{bmatrix} = M_1(s)G(s) \tag{B.44}$$

which shows that $\mathfrak{B}_{\mathrm{o}}(\Gamma) \subset \mathfrak{B}$. □

B.4 Proof of Lemma 4.6

Suppose that Γ_1 and Γ_2 are output guarantees, and consider the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$. Then, the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.2 if and only if

$$\mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \hookleftarrow \Gamma_2)) \subset \mathfrak{B}(\mathrm{A}_1 \hookleftarrow \mathrm{A}_2), \tag{4.81}$$

$$\mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \hookleftarrow \Gamma_2)) \subset \mathfrak{B}(\Gamma). \tag{4.82}$$

Proof. We begin by proving necessity. Suppose that $\mathcal{C}$ satisfies Implication 4.2. Let the autonomous systems

$$\Sigma_1 : P_1\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y_1 = 0 \quad \text{and} \quad \Sigma_2 : P_2\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)y_2 = 0, \tag{B.45}$$

be implementations of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and let A be given by (3.73). Then, we have that $\Sigma_1 \hookleftarrow \Sigma_2$ is well-posed and

$$\mathrm{A} \wedge (\Sigma_1 \hookleftarrow \Sigma_2) : \begin{bmatrix} P_1\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) & 0 \\ 0 & P_2\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) \\ 0 & 0 \end{bmatrix} y = \begin{bmatrix} 0 \\ 0 \\ A\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) \end{bmatrix} u, \tag{B.46}$$

which implies that

$$\mathfrak{B}(\mathrm{A} \wedge (\Sigma_1 \hookleftarrow \Sigma_2)) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \times \mathfrak{B}_{\mathrm{o}}(\Sigma_1) \times \mathfrak{B}_{\mathrm{o}}(\Sigma_2). \tag{B.47}$$

In view of Remark 4.5 and the assumption that $\mathcal{C}$ satisfies Implication 4.2, it follows that (4.79) and (4.80) hold. Consequently, we obtain

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \times \mathfrak{B}_{\mathrm{o}}(\Sigma_1) \times \mathfrak{B}_{\mathrm{o}}(\Sigma_2) \subset \mathfrak{B}(\mathrm{A}_1 \hookleftarrow \mathrm{A}_2), \tag{B.48}$$

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \times \mathfrak{B}_{\mathrm{o}}(\Sigma_1) \times \mathfrak{B}_{\mathrm{o}}(\Sigma_2) \subset \mathfrak{B}(\Gamma). \tag{B.49}$$

Due to the Remark 4.3 and the assumption that Γ_1 and Γ_2 are output guarantees, the latter holds for all autonomous Σ_1 and Σ_2 that implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, only if

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_2) \subset \mathfrak{B}(\mathrm{A}_1 \hookleftarrow \mathrm{A}_2), \tag{B.50}$$

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_2) \subset \mathfrak{B}(\Gamma). \tag{B.51}$$

Furthermore, we have that

$$\mathrm{A} \wedge (\Gamma_1 \hookleftarrow \Gamma_2) : \begin{bmatrix} G_1\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) & 0 \\ 0 & G_2\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) \\ 0 & 0 \end{bmatrix} y = \begin{bmatrix} 0 \\ 0 \\ A\big(\frac{\mathrm{d}}{\mathrm{d}t}\big) \end{bmatrix} u, \tag{B.52}$$

and, thus,

$$\mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \hookleftarrow \Gamma_2)) = \mathfrak{B}_{\mathrm{i}}(\mathrm{A}) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_1) \times \mathfrak{B}_{\mathrm{o}}(\Gamma_2). \tag{B.53}$$

Together with (B.50) and (B.51), the latter implies that (4.81) and (4.82) hold.

We proceed by proving sufficiency. Suppose that (4.81) and (4.82) hold. Let Σ_1 and Σ_2 be implementations of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and suppose that $\Sigma_1 \hookleftarrow \Sigma_2$ is well-posed. We will show that

$$\mathfrak{B}(\mathrm{A} \wedge (\Sigma_1 \hookleftarrow \Sigma_2)) \subset \mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \hookleftarrow \Gamma_2)). \tag{B.54}$$

Due to Remark 4.5, (4.81) and (4.82), the latter is sufficient to conclude that $\mathcal{C}$ satisfies Implication 4.2. To this end, let $\Sigma_1 \leftarrow \Sigma_2$ be defined as in Definition 4.3, $\mathrm{A}_1 \leftarrow \mathrm{A}_2$ be defined as in Remark 4.5, and $\Gamma_1 \leftarrow \Gamma_2$ be defined as in Definition 4.5. Note that $H_{\mathrm{i}}(s) = 0$ and $H_{\mathrm{e}}(s) = 0$ because Γ_1 and Γ_2 are output guarantees. On the other hand, since Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$, we have that $\mathfrak{B}(\mathrm{A}_1 \wedge \Sigma_1) \subset \mathfrak{B}(\Gamma_1)$ and $\mathfrak{B}(\mathrm{A}_2 \wedge \Sigma_2) \subset \mathfrak{B}(\Gamma_2)$. In view of Proposition 3.13, this implies that there exist polynomial matrices $T_1(s)$, $M_1(s)$, $T_2(s)$ and $M_2(s)$ such that

$$\begin{bmatrix} G_1(s) & 0 \end{bmatrix} = \begin{bmatrix} T_1(s) & M_1(s) \end{bmatrix} \begin{bmatrix} P_1(s) & -Q_1(s) \\ 0 & -A_1(s) \end{bmatrix}, \tag{B.55}$$

$$\begin{bmatrix} G_2(s) & 0 \end{bmatrix} = \begin{bmatrix} T_2(s) & M_2(s) \end{bmatrix} \begin{bmatrix} P_2(s) & -Q_2(s) \\ 0 & -A_2(s) \end{bmatrix}. \tag{B.56}$$

Consequently, the polynomial matrices

$$T(s) = \begin{bmatrix} T_1(s) & 0 \\ 0 & T_2(s) \end{bmatrix} \quad \text{and} \quad M(s) = \begin{bmatrix} M_1(s) & 0 \\ 0 & M_2(s) \end{bmatrix} \tag{B.57}$$

are such that

$$G(s) = T(s)P(s), \tag{B.58}$$

$$-M(s)A_{\mathrm{i}}(s) = T(s)Q_{\mathrm{i}}(s), \tag{B.59}$$

$$-M(s)A_{\mathrm{e}}(s), = T(s)Q_{\mathrm{e}}(s). \tag{B.60}$$

At the same time, (4.81) holds if and only if there exist polynomial matrices $R_1(s)$ and $R_2(s)$ such that

$$\begin{bmatrix} -A_{\mathrm{i}}(s) & -A_{\mathrm{e}}(s) \end{bmatrix} = \begin{bmatrix} R_1(s) & R_2(s) \end{bmatrix} \begin{bmatrix} G(s) & 0 \\ 0 & -A(s) \end{bmatrix}. \tag{B.61}$$

Now, to show that (B.54) holds, it is enough to show that there exist polynomial matrices $N_1(s)$ and $N_2(s)$ such that

$$\begin{bmatrix} G(s) & 0 \\ 0 & -A(s) \end{bmatrix} = \begin{bmatrix} N_1(s) & N_2(s) \\ 0 & I \end{bmatrix} \begin{bmatrix} P(s) - Q_{\mathrm{i}}(s) & -Q_{\mathrm{e}}(s) \\ 0 & -A(s) \end{bmatrix}. \tag{B.62}$$

With this in mind, (B.58), (B.59) and (B.61) yield

$$\begin{aligned} G(s)\left(I - P(s)^{-1}Q_{\mathrm{i}}(s)\right) &= T(s)\left(P(s) - Q_{\mathrm{i}}(s)\right) \\ &= G(s) + M(s)A_{\mathrm{i}}(s) \\ &= \left(I - M(s)R_1(s)\right)G(s). \end{aligned} \tag{B.63}$$

Because of Remark 3.4, we can assume that $G_1(s)$ and $G_2(s)$ have full row rank, hence $G(s)$ has full row rank as well. Then, due to Proposition 3.8, there

exists a unimodular matrix $U(s)$ such that $\hat{G}(s) = U(s)G(s)$ is row-reduced. We can substitute $G(s)$ with $\hat{G}(s)$ in (B.63) to obtain

$$\hat{G}(s)\left(I - P(s)^{-1}Q_{\mathrm{i}}(s)\right) = U(s)\left(I + M(s)R_1(s)\right)U(s)^{-1}\hat{G}(s), \tag{B.64}$$

where we note that $I - P(s)^{-1}Q_{\mathrm{i}}(s)$ is proper and invertible because $\Sigma_1 \hookleftarrow \Sigma_2$ is well-posed. Therefore, due to Lemma A.2, it follows that

$$U(s)\left(I + M(s)R_1(s)\right)U(s)^{-1} \tag{B.65}$$

is unimodular and, thus, $I + M(s)R_1(s)$ is unimodular as well. Together with (B.63), this implies that

$$N_1(s) = \left(I + M(s)R_1(s)\right)^{-1}T(s) \tag{B.66}$$

is a polynomial matrix such that

$$G(s) = N_1(s)\left(P(s) - Q_{\mathrm{i}}(s)\right). \tag{B.67}$$

Finally, note that (B.60) and (B.61) yield

$$T(s)Q_{\mathrm{e}}(s) = -M(s)A_{\mathrm{e}}(s) = -M(s)R_2(s)A(s), \tag{B.68}$$

hence the polynomial matrix

$$N_2(s) = \left(I + M(s)R_1(s)\right)^{-1}M(s)R_2(s) \tag{B.69}$$

is such that (B.62) holds. This shows that (B.54) holds, which, due to Remark 4.5, (4.81) and (4.82), implies that $\mathcal{C}$ satisfies Implication 4.2. □

B.5 Proof of Lemma 4.8

Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ given by (4.2) are consistent and row-reduced. Consider the partitions in (4.75) and (4.26), and let $D_1(s)$ and $D_2(s)$ be the row-degree matrices of $G_1(s)$ and $G_2(s)$, respectively. Then, the guarantees Γ_1' and Γ_2' given by (4.92) are such that $\Gamma_1' \hookleftarrow \Gamma_2'$ is well-posed if the rational matrices

$$\begin{aligned} &D_1(s)^{-1}\left(H_1(s) - M_1(s)A_1(s)\right), \\ &D_2(s)^{-1}\left(H_2(s) - M_2(s)A_2(s)\right), \end{aligned} \tag{4.95}$$

are proper, and at least one of the following conditions hold:

1. $D_1(s)^{-1}(H_{12}(s) - M_1(s)A_{12}(s))$ is strictly proper;
2. $D_2(s)^{-1}(H_{21}(s) - M_2(s)A_{21}(s))$ is strictly proper.

Proof. Let $G(s)$, $H_{\mathrm{i}}(s)$ and $H_{\mathrm{e}}(s)$ be defined as in Definition 4.5, $A_{\mathrm{i}}(s)$ and $A_{\mathrm{e}}(s)$ be defined as in Remark 4.5, and define

$$M(s) = \begin{bmatrix} M_1(s) & 0 \\ 0 & M_2(s) \end{bmatrix}. \tag{B.70}$$

Note that

$$\Gamma_1' \hookleftarrow \Gamma_2' : \left(G\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) - H_{\mathrm{i}}'\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right)\right) y = H_{\mathrm{e}}'\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u, \tag{B.71}$$

where

$$H_{\mathrm{i}}'(s) = H_{\mathrm{i}}(s) - M(s)A_{\mathrm{i}}(s), \tag{B.72}$$

$$H_{\mathrm{e}}'(s) = H_{\mathrm{e}}(s) - M(s)A_{\mathrm{e}}(s). \tag{B.73}$$

It is easily seen that the row-degree matrix of $G(s)$ is given by

$$D(s) = \begin{bmatrix} D_1(s) & 0 \\ 0 & D_2(s) \end{bmatrix}, \tag{B.74}$$

which, due to (4.95) being proper, implies that $D(s)^{-1}H_{\mathrm{e}}'(s)$ is proper. With this in mind, suppose that the first condition holds, that is,

$$D_1(s)^{-1}(H_{12}(s) - M_1(s)A_{12}(s)) \tag{B.75}$$

is strictly proper. Due to (4.95) being proper, we know that

$$D_2(s)^{-1}(H_{21}(s) - M_2(s)A_{21}(s)) \tag{B.76}$$

is proper, which means that

$$\lim_{s\to\infty} D(s)^{-1}H_{\mathrm{i}}'(s) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & H_{21}^h & 0 & 0 \end{bmatrix}, \tag{B.77}$$

for some real matrix H_{21}^h. On the other hand, since $G_1(s)$ and $G_2(s)$ are row-reduced, it follows that

$$\lim_{s\to\infty} D(s)^{-1}G(s) = \begin{bmatrix} G_{11}^h & G_{12}^h & 0 & 0 \\ 0 & 0 & G_{21}^h & G_{22}^h \end{bmatrix} \tag{B.78}$$

for some real matrices G_{11}^h, G_{12}^h, G_{21}^h, and G_{22}^h such that

$$\begin{bmatrix} G_{11}^h & G_{12}^h \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} G_{21}^h & G_{22}^h \end{bmatrix} \tag{B.79}$$

have full row rank. This implies that

$$\lim_{s\to\infty} D(s)^{-1}(G(s) - H_{\mathrm{i}}'(s)) = \begin{bmatrix} G_{11}^h & G_{12}^h & 0 & 0 \\ 0 & -H_{12}^h & G_{21}^h & G_{22}^h \end{bmatrix} \tag{B.80}$$

has full row rank, hence, by Proposition 4.2, $\Gamma_1' \hookleftarrow \Gamma_2'$ is well-posed. Using a similar argument, we can show that $\Gamma_1' \hookleftarrow \Gamma_2'$ is also well-posed when the second condition holds. □

B.6 Proof of Lemma 4.9

Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are row-reduced and $\Gamma_1 \hookleftarrow \Gamma_2$ is well-posed. Then, the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.2 if and only if

$$\mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \hookleftarrow \Gamma_2)) \subset \mathfrak{B}(\mathrm{A}_1 \hookleftarrow \mathrm{A}_2), \tag{4.97}$$

$$\mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \hookleftarrow \Gamma_2)) \subset \mathfrak{B}(\Gamma). \tag{4.98}$$

Proof. We begin by proving necessity. We will do this by using the ideas from the necessity part of the proof of Theorem 3.3 about contract refinement. Suppose that the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 4.2. Since $\Gamma_1 \hookleftarrow \Gamma_2$ is well-posed, there exist input-output systems Σ_1 and Σ_2 such that $\mathfrak{B}(\Sigma_1) \subset \mathfrak{B}(\Gamma_1)$, $\mathfrak{B}(\Sigma_2) \subset \mathfrak{B}(\Gamma_2)$, and $\Sigma_1 \hookleftarrow \Sigma_2$ is well-posed. Let Σ_1 and Σ_2 be given by (4.1). Then, for each $j \in \{1, 2\}$, there exists a polynomial matrix $T_{1j}(s)$ such that

$$\begin{bmatrix} G_j(s) & -H_j(s) \end{bmatrix} = T_{1j}(s) \begin{bmatrix} P_j(s) & -Q_j(s) \end{bmatrix}, \tag{B.81}$$

Since $\mathcal{C}_j = (\mathrm{A}_j, \Gamma_j)$ is row-reduced, we have that $G_j(s)$ is row-reduced. This means that $G_j(s)$ has full row rank, and since $G_j(s) = T_{1j}(s)P_j(s)$ and $P_j(s)$ is invertible, it follows that $T_{1j}(s)$ must have full row rank as well. Consequently, there exists a polynomial matrix $T_{j2}(s)$ such that

$$T_j(s) = \begin{bmatrix} T_{1j}(s) \\ T_{2j}(s) \end{bmatrix} \tag{B.82}$$

is invertible, which implies that

$$T_{j,k}(s) = \begin{bmatrix} T_{1j}(s) \\ s^k T_{2j}(s) \end{bmatrix} \tag{B.83}$$

is invertible for all nonnegative integers k. Let

$$P_{j,k}(s) = T_{j,k}(s)P_j(s), \quad Q_{j,k}(s) = T_{j,k}(s)Q_j(s). \tag{B.84}$$

Note that $P_{j,k}(s)$ is invertible, and

$$P_{j,k}(s)^{-1}Q_{j,k} = P_j(s)^{-1}Q_j(s) \tag{B.85}$$

is proper. Moreover,

$$\begin{bmatrix} G_j(s) & -H_j(s) \end{bmatrix} = \begin{bmatrix} I & 0 \end{bmatrix} \begin{bmatrix} P_{j,k}(s) & Q_{j,k}(s) \end{bmatrix}, \tag{B.86}$$

hence the system

$$\Sigma_{j,k} : P_{j,k}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) y_j = Q_{j,k}\left(\tfrac{\mathrm{d}}{\mathrm{d}t}\right) u_j \tag{B.87}$$

is in input-output form and such that $\mathfrak{B}(\Sigma_{j,k}) \subset \mathfrak{B}(\Gamma_j)$. Clearly, this implies that $\mathfrak{B}(\mathrm{A}_j \wedge \Sigma_{j,k}) \subset \mathfrak{B}(\Gamma_j)$ as well, hence $\Sigma_{j,k}$ is an implementation of $\mathcal{C}_j$.

With this in mind, note that

$$\Sigma_{1,k} \hookleftarrow \Sigma_{2,k} : T_k\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)\left(P\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) - Q_{\mathrm{i}}\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big)\right) y = T_k\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) Q_{\mathrm{e}}\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) u, \tag{B.88}$$

where $P(s)$, $Q_{\mathrm{i}}(s)$ and $Q_{\mathrm{e}}(s)$ are defined as in Definition 4.3, and

$$T_k(s) = \begin{bmatrix} T_{1,k}(s) & 0 \\ 0 & T_{2,k}(s) \end{bmatrix}. \tag{B.89}$$

In view of Proposition 4.1, $\Sigma_{1,k} \hookleftarrow \Sigma_{2,k}$ is well-posed if and only if

$$\lim_{s\to\infty} I - \left(T_k(s)P(s)\right)^{-1} T_k(s) Q_{\mathrm{i}}(s) = \lim_{s\to\infty} I - P(s)^{-1} Q_{\mathrm{i}}(s) \tag{B.90}$$

exists and is invertible, which is the case because $\Sigma_1 \hookleftarrow \Sigma_2$ is well-posed. Therefore, for all nonnegative integers k, we have that $\Sigma_{1,k}$ and $\Sigma_{2,k}$ implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and $\Sigma_{1,k} \hookleftarrow \Sigma_{2,k}$ is well-posed, hence

$$\mathfrak{B}(\mathrm{A} \wedge (\Sigma_{1,k} \hookleftarrow \Sigma_{2,k})) \subset \mathfrak{B}(\mathrm{A}_1 \hookleftarrow \mathrm{A}_2), \tag{B.91}$$

$$\mathfrak{B}(\mathrm{A} \wedge (\Sigma_{1,k} \hookleftarrow \Sigma_{2,k})) \subset \mathfrak{B}(\Gamma), \tag{B.92}$$

because $\mathcal{C}$ satisfies Implication 4.2, see Remark 4.5. We will show that (B.92) holds for all nonnegative integers k only if (4.98) holds. To this end, let

$$\mathrm{A} : 0 = \bar{A}\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) u \quad \text{and} \quad \Gamma : \bar{G}\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) y = \bar{H}\big(\tfrac{\mathrm{d}}{\mathrm{d}t}\big) u, \tag{B.93}$$

where $\bar{A}(s)$, $\bar{G}(s)$ and $\bar{H}(s)$ are polynomial matrices. Note that (B.92) holds if and only if there exists polynomial matrices $N_k(s)$ and $M_k(s)$ such that

$$\begin{bmatrix} \bar{G}(s) & -\bar{H}(s) \end{bmatrix} = \begin{bmatrix} N_k(s) & M_k(s) \end{bmatrix} \begin{bmatrix} T_k(s)\left(P(s) - Q_{\mathrm{i}}(s)\right) & -T_k(s) Q_{\mathrm{e}}(s) \\ 0 & -\bar{A}(s) \end{bmatrix}. \tag{B.94}$$

In particular, we have that $N_k(s)$ is such that

$$\bar{G}(s) = N_k(s) T_k(s) \left(P(s) - Q_{\mathrm{i}}(s)\right). \tag{B.95}$$

Note that $P(s) - Q_{\mathrm{i}}(s)$ is invertible because $\Sigma_1 \hookleftarrow \Sigma_2$ is well-posed, while

$$T_k(s) = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & s^k I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & s^k I \end{bmatrix} T_0(s), \tag{B.96}$$

where $T_0(s)$ is invertible. Therefore, (B.95) holds if and only if

$$\bar{G}(s)\left(P(s) - Q_{\mathrm{i}}(s)\right)^{-1} T_0(s)^{-1} = N_k(s) \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & s^k I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & s^k I \end{bmatrix} \tag{B.97}$$

Note that the left-hand side of the latter is independent of k, hence the right-hand side must be independent of k as well. This is the case if and only if

$$N_k(s) = \begin{bmatrix} N_1(s) & 0 & N_3(s) & 0 \end{bmatrix} \tag{B.98}$$

for some polynomial matrices $N_1(s)$ and $N_3(s)$. In particular, we obtain

$$N_k(s)T_k(s) = \begin{bmatrix} N_1(s) & N_3(s) \end{bmatrix} \begin{bmatrix} T_{11}(s) & 0 \\ 0 & T_{12}(s) \end{bmatrix}. \tag{B.99}$$

In view of (B.81), it follows that

$$N_k(s)T_k(s)P(s) = \begin{bmatrix} N_1(s) & N_3(s) \end{bmatrix} G(s), \tag{B.100}$$

$$N_k(s)T_k(s)Q_{\mathrm{i}}(s) = \begin{bmatrix} N_1(s) & N_3(s) \end{bmatrix} H_{\mathrm{i}}(s), \tag{B.101}$$

$$N_k(s)T_k(s)Q_{\mathrm{e}}(s) = \begin{bmatrix} N_1(s) & N_3(s) \end{bmatrix} H_{\mathrm{e}}(s), \tag{B.102}$$

where $G(s)$, $H_{\mathrm{i}}(s)$ and $H_{\mathrm{e}}(s)$ are defined as in Definition 4.5. Now, let

$$\bar{N}(s) = \begin{bmatrix} N_1(s) & N_3(s) \end{bmatrix}, \tag{B.103}$$

and note that, for some arbitrary positive integer k, (B.94) yields

$$\begin{bmatrix} \bar{G}(s) & -\bar{H}(s) \end{bmatrix} = \begin{bmatrix} \bar{N}(s) & M_k(s) \end{bmatrix} \begin{bmatrix} G(s) - H_{\mathrm{i}}(s) & -H_{\mathrm{e}}(s) \\ 0 & -\bar{A}(s) \end{bmatrix}, \tag{B.104}$$

which shows that (4.98) holds, as desired. Using the same ideas, we can show that (B.91) holds for all nonnegative integers k only if (4.97) holds.

We proceed by proving sufficiency. Suppose that (4.97) and (4.98) hold. Let Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and suppose that $\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2$ is well-posed. Due to Lemma 4.10, if follows that (4.99) holds. Consequently (4.97) and (4.98) imply that (4.79) and (4.80) hold, which shows that $\mathcal{C}$ satisfies Implication 4.2. □

B.7 Proof of Lemma 4.10

Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are row-reduced, $\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2$ is well-posed, and (4.97) holds. Then

$$\mathfrak{B}(\mathrm{A} \wedge (\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2)) \subset \mathfrak{B}(\mathrm{A} \wedge (\Gamma_1 \leftarrow\!\!\shortmid \Gamma_2)) \tag{4.99}$$

for all implementations Σ_1 and Σ_2 of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, such that $\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2$ is well-posed.

Proof. Suppose that Σ_1 and Σ_2 implement $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and that $\Sigma_1 \leftarrow\!\!\shortmid \Sigma_2$ is well-posed. For each $j \in \{1, 2\}$, let Σ_j be given by (4.1). Since Σ_j

implements $\mathcal{C}_j$, we have that $\mathfrak{B}(\mathrm{A}_j \wedge \Sigma_j) \subset \mathfrak{B}(\Gamma_j)$, which holds if and only if there exist polynomial matrices $T_j(s)$ and $M_j(s)$ such that

$$\begin{bmatrix} G_j(s) & -H_j(s) \end{bmatrix} = \begin{bmatrix} T_j(s) & M_j(s) \end{bmatrix} \begin{bmatrix} P_j(s) & -Q_j(s) \\ 0 & -A_j(s) \end{bmatrix}. \tag{B.105}$$

We can rewrite the latter to obtain

$$\begin{bmatrix} G_j(s) & -H_j(s) + M_j(s)A_j(s) \end{bmatrix} = T_j(s) \begin{bmatrix} P_j(s) & -Q_j(s) \end{bmatrix}. \tag{B.106}$$

Consequently, the polynomial matrices

$$T(s) = \begin{bmatrix} T_1(s) & 0 \\ 0 & T_2(s) \end{bmatrix} \quad \text{and} \quad M(s) = \begin{bmatrix} M_1(s) & 0 \\ 0 & M_2(s) \end{bmatrix} \tag{B.107}$$

are such that

$$G(s) = T(s)P(s), \tag{B.108}$$
$$H_{\mathrm{i}}(s) - M(s)A_{\mathrm{i}}(s) = T(s)Q_{\mathrm{i}}(s), \tag{B.109}$$
$$H_{\mathrm{e}}(s) - M(s)A_{\mathrm{e}}(s) = T(s)Q_{\mathrm{e}}(s), \tag{B.110}$$

where $G(s)$, $H_{\mathrm{i}}(s)$ and $H_{\mathrm{e}}(s)$ are defined as in Definition 4.5, $P(s)$, $Q_{\mathrm{i}}(s)$ and $Q_{\mathrm{e}}(s)$ are defined as in Definition 4.3, and $A_{\mathrm{i}}(s)$ and $A_{\mathrm{e}}(s)$ are defined as in Remark 4.5. Let A and Γ be given by (B.93). Note that (4.97) holds if and only if there exist polynomial matrices $R_1(s)$ and $R_2(s)$ such that

$$\begin{bmatrix} -A_{\mathrm{i}}(s) & -A_{\mathrm{e}}(s) \end{bmatrix} = \begin{bmatrix} R_1(s) & R_2(s) \end{bmatrix} \begin{bmatrix} G(s) - H_{\mathrm{i}}(s) & -H_{\mathrm{e}}(s) \\ 0 & -\bar{A}(s) \end{bmatrix}. \tag{B.111}$$

In particular, this means that

$$-A_{\mathrm{i}}(s) = R_1(s) \left(G(s) - H_{\mathrm{i}}(s) \right). \tag{B.112}$$

Now, to show that (4.99) holds, it is sufficient to show that there exist polynomial matrices $N_1(s)$ and $N_2(s)$ such that

$$\begin{bmatrix} G(s) - H_{\mathrm{i}}(s) & -H_{\mathrm{e}}(s) \\ 0 & -\bar{A}(s) \end{bmatrix} = \begin{bmatrix} N_1(s) & N_2(s) \\ 0 & I \end{bmatrix} \begin{bmatrix} P(s) - Q_{\mathrm{i}}(s) & -Q_{\mathrm{e}}(s) \\ 0 & -\bar{A}(s) \end{bmatrix}. \tag{B.113}$$

To this end, due to (B.108) and (B.109), we have that

$$\begin{aligned} G(s) - H_{\mathrm{i}}(s) + M(s)A_{\mathrm{i}}(s) &= T(s) \left(P(s) - Q_{\mathrm{i}}(s) \right) \\ &= G(s) \left(I - P(s)^{-1} Q_{\mathrm{i}}(s) \right). \end{aligned} \tag{B.114}$$

On the other hand, due to (B.112), we have that

$$G(s) - H_{\mathrm{i}}(s) + M(s)A_{\mathrm{i}}(s) = \left(I - M(s)R_1(s) \right) \left(G(s) - H_{\mathrm{i}}(s) \right), \tag{B.115}$$

hence

$$(I - M(s)R_1(s))\,(G(s) - H_{\mathrm{i}}(s)) = G(s)\left(I - P(s)^{-1}Q_{\mathrm{i}}(s)\right). \tag{B.116}$$

Note that, due to Proposition 4.1, $I - P(s)^{-1}Q_{\mathrm{i}}(s)$ is proper and invertible because $\Sigma_1 \leftarrow\!\!\shortmid\; \Sigma_2$ is well-posed. Since the contracts $\mathcal{C}_1$ and $\mathcal{C}_2$ are row-reduced, it follows that the polynomial matrices $G_1(s)$, $G_2(s)$ and, thus, $G(s)$ are row-reduced. Furthermore, as $\Gamma_1 \leftarrow\!\!\shortmid\; \Gamma_2$ is well-posed, Proposition 4.2 implies that

$$\lim_{s\to\infty} D(s)^{-1}\,(G(s) - H_{\mathrm{i}}(s)) \tag{B.117}$$

has full row rank, where $D(s)$ is the row-degree matrix of $G(s)$. Therefore, we can use Lemma A.2 and (B.116) to conclude that $I - M(s)R_1(s)$ is unimodular. In view of (B.116), this means that

$$N_1(s) = (I - M(s)R_1(s))^{-1}\,T(s) \tag{B.118}$$

is a polynomial matrix such that

$$G(s) - H_{\mathrm{i}}(s) = N_1(s)\,(P(s) - Q_{\mathrm{i}}(s)). \tag{B.119}$$

Now, from (B.111) it follows that

$$A_{\mathrm{e}}(s) = R_1(s)H_{\mathrm{e}}(s) + R_2(s)\bar{A}(s), \tag{B.120}$$

which we can combine with (B.110) to obtain

$$\begin{aligned} T(s)Q_{\mathrm{e}}(s) &= H_{\mathrm{e}}(s) - M(s)A_{\mathrm{e}}(s) \\ &= (I - M(s)R_1(s))\,H_{\mathrm{e}}(s) - M(s)R_2(s)\bar{A}(s). \end{aligned} \tag{B.121}$$

This implies that the polynomial matrix

$$N_2(s) = (I - MR_1(s))^{-1}\,M(s)R_2(s) \tag{B.122}$$

is such that

$$-H_{\mathrm{e}}(s) = -N_1(s)Q_{\mathrm{e}}(s) + N_2(s)\bar{A}(s), \tag{B.123}$$

which, together with (B.119) implies that (B.113) and, thus, (4.99) hold. □

B.8 Proof of Theorem 4.5

Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are consistent. Then, $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$ if and only if

$$(0, y_1) \in \mathfrak{B}(\Gamma_1) \quad \Longrightarrow \quad y_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2), \tag{4.117}$$

Furthermore, if $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$, then the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ exist and is given by

$$\mathcal{C}_1 \to \mathcal{C}_2 = (\mathrm{A}_{12}, \Gamma_1 \to \Gamma_2), \tag{4.118}$$

where A_{12} is such that

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{12}) = \mathfrak{B}_{\mathrm{i}}((\mathrm{A}_1 \to \mathrm{A}_2) \wedge (\Gamma_1 \to \Gamma_2)), \tag{4.119}$$

that is, A_{12} is obtained by eliminating y from $(\mathrm{A}_1 \to \mathrm{A}_2) \wedge (\Gamma_1 \to \Gamma_2)$.

Proof. Since $\mathcal{C}_1$ and $\mathcal{C}_2$ are consistent, due to Lemma 3.18, we can assume that $\mathcal{C}_1$ and $\mathcal{C}_2$ are row-reduced without loss of generality. Suppose that u_{12}, y_{11}, u_{22} and y_{21} in (4.8) are void so that the feedback interconnection reduces to the series interconnection. As the series interconnection is always well-posed, it follows that $\mathcal{C}_1$ is feedback compatible with $\mathcal{C}_2$. Then, due to Lemma 4.7 there exist guarantees Γ_1' and Γ_2' such that $\Gamma_1' \hookleftarrow \Gamma_2'$ is well-posed and the contracts $\mathcal{C}_1' = (\mathrm{A}_1, \Gamma_1')$ and $\mathcal{C}_2' = (\mathrm{A}_2, \Gamma_2')$ are equivalent to $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. It is easily seen that $\mathcal{C}_1'$ and $\mathcal{C}_2'$ are also row-reduced. Now, due to Theorem 4.3, $\mathcal{C}_1'$ is feedback composable to $\mathcal{C}_2'$ if and only if

$$(0, y) \in \mathfrak{B}(\Gamma_1' \hookleftarrow \Gamma_2') \quad \Longrightarrow \quad (0, y) \in \mathfrak{B}(\mathrm{A}_1 \hookleftarrow \mathrm{A}_2). \tag{B.124}$$

Since the series interconnection reduces to the feedback interconnection, $\mathcal{C}_1'$ is feedback composable to $\mathcal{C}_2'$ if and only if $\mathcal{C}_1'$ is series composable to $\mathcal{C}_2'$, which, due to (B.124), is the case if and only if

$$(0, y) \in \mathfrak{B}(\Gamma_1' \to \Gamma_2') \quad \Longrightarrow \quad (0, y) \in \mathfrak{B}(\mathrm{A}_1 \to \mathrm{A}_2). \tag{B.125}$$

On the other hand, since $\mathcal{C}_1'$ and $\mathcal{C}_2'$ are equivalent to $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, $\mathcal{C}_1'$ is series composable to $\mathcal{C}_2'$ if and only if $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$. Therefore, it is sufficient to show that (B.125) holds if and only if (4.117) holds.

To this end, suppose that (B.125) holds and let $(0, y_1) \in \mathfrak{B}(\Gamma_1)$. Since $0 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$, it follows that $(0, y_1) \in \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1)$. In view of Corollary 3.21 and the fact that $\mathcal{C}_1$ is equivalent to $\mathcal{C}_1'$, it follows that $(0, y_1) \in \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1')$ and, thus, $(0, y_1) \in \mathfrak{B}(\Gamma_1')$. Since $\mathcal{C}_2'$ is row-reduced, for all u_2, there exists y_2 such that $(u_2, y_2) \in \mathfrak{B}(\Gamma_2')$. Therefore, there exists y_2 such that $(y_1, y_2) \in \mathfrak{B}(\Gamma_2')$. This implies that $(0, y) \in \mathfrak{B}(\Gamma_1' \to \Gamma_2')$, hence $(0, y) \in \mathfrak{B}(\mathrm{A}_1 \to \mathrm{A}_2)$ due to (B.125). As the latter holds if and only if $y_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$, this shows that (4.117) holds.

To show the converse, suppose that (4.117) holds. Let $(0, y) \in \mathfrak{B}(\Gamma_1' \to \Gamma_2')$ and note that $(0, y_1) \in \mathfrak{B}(\Gamma_1')$. But $0 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1)$, hence $(0, y_1) \in \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1')$ and, thus, $(0, y_1) \in \mathfrak{B}(\mathrm{A}_1 \wedge \Gamma_1)$ because $\mathcal{C}_1'$ is equivalent to $\mathcal{C}_1$. Consequently, $(0, y_1) \in \mathfrak{B}(\Gamma_1)$, which implies that $y_1 \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$ due to (4.117). As the latter holds if and only if $(0, y) \in \mathfrak{B}(\mathrm{A}_1 \to \mathrm{A}_2)$, this shows that (B.125) holds.

Now, suppose that $\mathcal{C}_1$ is series composable to $\mathcal{C}_2$. Then $\mathcal{C}_1'$ is feedback composable to $\mathcal{C}_2'$ and, due to Theorem 4.3,

$$\mathcal{C}_1' \leftarrow \mathcal{C}_2' = (\mathrm{A}_{12}, \Gamma_1' \leftarrow \Gamma_2'), \tag{B.126}$$

where

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{12}) = \mathfrak{B}((\mathrm{A}_1 \leftarrow \mathrm{A}_2) \wedge (\Gamma_1' \leftarrow \Gamma_2')). \tag{B.127}$$

Since the series interconnection reduces to the feedback interconnection, the feedback composition reduces to the series composition. In particular,

$$\mathcal{C}_1' \rightarrow \mathcal{C}_2' = (\mathrm{A}_{12}, \Gamma_1' \rightarrow \Gamma_2'), \tag{B.128}$$

where A_{12} is such that

$$\mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{12}) = \mathfrak{B}_{\mathrm{i}}((\mathrm{A}_1 \rightarrow \mathrm{A}_2) \wedge (\Gamma_1' \rightarrow \Gamma_2')). \tag{B.129}$$

Note that

$$(\mathrm{A}_1 \rightarrow \mathrm{A}_2) \wedge (\Gamma_1' \rightarrow \Gamma_2') = (\mathrm{A}_1 \wedge \Gamma_1') \rightarrow (\mathrm{A}_2 \wedge \Gamma_2'), \tag{B.130}$$

hence, due to Proposition 4.3 and Corollary 3.21, (B.129) holds if and only if (4.119) holds. Since $\mathcal{C}_1'$ and $\mathcal{C}_2'$ are equivalent to $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$ exists and is given by $\mathcal{C}_1' \rightarrow \mathcal{C}_2'$. Therefore, it is sufficient to show that $\mathcal{C}_1' \rightarrow \mathcal{C}_2'$ is equivalent to the contract $\mathcal{C}_1 \rightarrow \mathcal{C}_2$, as defined in (4.118). Due to Corollary 3.21, this is the case if and only if

$$\mathfrak{B}(\mathrm{A}_{12} \wedge (\Gamma_1' \rightarrow \Gamma_2')) = \mathfrak{B}(\mathrm{A}_{12} \wedge (\Gamma_1 \rightarrow \Gamma_2)). \tag{B.131}$$

With this in mind, let $(u, y) \in \mathfrak{B}(\mathrm{A}_{12} \wedge (\Gamma_1' \rightarrow \Gamma_2'))$. The latter holds if and only if $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{12})$, $(u, y) \in \mathfrak{B}(\Gamma_1' \rightarrow \Gamma_2')$. In view of (B.129), there exist y' such that $(u, y') \in \mathfrak{B}(\mathrm{A}_1 \rightarrow \mathrm{A}_2)$ and $(u, y') \in \mathfrak{B}(\Gamma_1' \rightarrow \Gamma_2')$. This implies that $(0, y - y') \in \mathfrak{B}(\Gamma_1' \rightarrow \Gamma_2')$, hence $(0, y - y') \in \mathfrak{B}(\mathrm{A}_1 \rightarrow \mathrm{A}_2)$ due to (B.124). This means that $(u, y) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \rightarrow \mathrm{A}_2)$ and, thus,

$$(u, y) \in \mathfrak{B}((\mathrm{A}_1 \rightarrow \mathrm{A}_2) \wedge (\Gamma_1' \rightarrow \Gamma_2')). \tag{B.132}$$

Due to (B.130), Proposition 4.3 and Corollary 3.21, the latter is equivalent to

$$(u, y) \in \mathfrak{B}((\mathrm{A}_1 \rightarrow \mathrm{A}_2) \wedge (\Gamma_1 \rightarrow \Gamma_2)). \tag{B.133}$$

In particular, we obtain $(u, y) \in \mathfrak{B}(\Gamma_1 \rightarrow \Gamma_2)$. Since $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{12})$, it follows that $(u, y) \in \mathfrak{B}(\mathrm{A}_{12} \wedge (\Gamma_1 \rightarrow \Gamma_2))$.

To show the converse, let $(u, y) \in \mathfrak{B}(\mathrm{A}_{12} \wedge (\Gamma_1 \rightarrow \Gamma_2))$. The latter holds if and only if $u \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_{12})$, $(u, y) \in \mathfrak{B}(\Gamma_1 \rightarrow \Gamma_2)$. In view of (4.119), there exist y' such that $(u, y') \in \mathfrak{B}(\mathrm{A}_1 \rightarrow \mathrm{A}_2)$ and $(u, y') \in \mathfrak{B}(\Gamma_1' \rightarrow \Gamma_2')$. This implies that $(0, y - y') \in \mathfrak{B}(\Gamma_1 \rightarrow \Gamma_2)$, hence, in particular, that $(0, y_1 - y_1') \in \mathfrak{B}(\Gamma_1)$. Due to (4.117), it follows that $y_1 - y_1' \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_2)$, hence $(0, y - y') \in \mathfrak{B}(\mathrm{A}_1 \rightarrow \mathrm{A}_2)$. Consequently, we obtain $(u, y) \in \mathfrak{B}_{\mathrm{i}}(\mathrm{A}_1 \rightarrow \mathrm{A}_2)$, which implies that (B.133) and, thus, (B.132) hold. This yields $(u, y) \in \mathfrak{B}(\mathrm{A}_{12} \wedge (\Gamma_1' \rightarrow \Gamma_2'))$, which shows (B.131) holds. Therefore, $\mathcal{C}_1' \rightarrow \mathcal{C}_2'$ is equivalent to $\mathcal{C}_1 \rightarrow \mathcal{C}_2$ and the latter is indeed the series composition of $\mathcal{C}_1$ to $\mathcal{C}_2$. □

B.9 Proof of Lemma 5.6

Suppose that the subspaces $\bar{\mathcal{R}} \subset \mathcal{R}$ satisfy

$$A'\mathcal{R} \subset \mathcal{R} + \operatorname{im} B' + \operatorname{im} G', \tag{5.58}$$

$$A'\left(\bar{\mathcal{R}} \cap \ker C'\right) \subset \bar{\mathcal{R}} + \operatorname{im} G', \tag{5.59}$$

where A', B', C' and G' are matrices of appropriate dimensions. Then, there exist matrices K', M', L' and N such that

$$(A' + G'K' + B'M')\mathcal{R} \subset \mathcal{R}, \tag{5.60}$$

$$(A' + G'K' - L'C')\bar{\mathcal{R}} \subset \bar{\mathcal{R}}, \tag{5.61}$$

$$(A' + G'K' + B'NC')\bar{\mathcal{R}} \subset \mathcal{R}. \tag{5.62}$$

Furthermore, if R is a matrix whose columns form a basis for $\mathcal{R}$, and $R^\dagger$ is such that $R^\dagger R = I$, then the matrices

$$K = R^\dagger(A' + G'K' - B'NC' + B'M' - L'C')R, \tag{5.63}$$

$$L = R^\dagger(B'N + L'), \tag{5.64}$$

$$M = (M' - NC')R, \tag{5.65}$$

are such that the subspace

$$\mathcal{S}' = \left\{(x + \bar{x}, w) \;\middle|\; x = Rw, \bar{x} \in \bar{\mathcal{R}}\right\} \tag{5.66}$$

satisfies

$$\begin{bmatrix} A' + B'NC' & B'M \\ LC' & K \end{bmatrix}\mathcal{S}' \subset \mathcal{S}' + \operatorname{im}\begin{bmatrix} G' \\ 0 \end{bmatrix}. \tag{5.67}$$

Proof. We will first show that there exists a matrix K' such that

$$(A' + G'K')\mathcal{R} \subset \mathcal{R} + \operatorname{im} B', \tag{B.134}$$

$$(A' + G'K')\left(\bar{\mathcal{R}} \cap \ker C'\right) \subset \bar{\mathcal{R}} \tag{B.135}$$

Let $r_1, \ldots, r_k$ be a basis for $\bar{\mathcal{R}} \cap \ker C'$ and extend it to a basis $r_1, \ldots, r_l$ for $\mathcal{R}$, where $l \geq k$. This is possible because $\bar{\mathcal{R}} \subset \mathcal{R}$. Now, due to (5.59), there exist $d_1, \ldots, d_k$ such that

$$A'r_i + G'd_i \in \bar{\mathcal{R}}, \quad i \in \{1, \ldots, k\} \tag{B.136}$$

Furthermore, due to (5.58), there exist $d_{k+1}, \ldots, d_l$ such that

$$A'r_i + G'd_i \in \mathcal{R} + \operatorname{im} B', \quad i \in \{k+1, \ldots, l\}. \tag{B.137}$$

Let K' be a matrix such that

$$K'r_i = d_i, \quad i \in \{1, \ldots, l\}. \tag{B.138}$$

Then (B.136) yields

$$(A' + G'K')r_i \in \bar{\mathcal{R}}, \quad i \in \{1, \dots, k\} \tag{B.139}$$

and thus (B.135) holds. On the other hand, since $\bar{\mathcal{R}} \subset \mathcal{R} + \operatorname{im} B'$, we have that (B.136) and (B.137) yield

$$(A' + G'K')r_i \in \mathcal{R} + \operatorname{im} B', \quad i \in \{1, \dots, l\}, \tag{B.140}$$

and thus (B.134) holds. Due to [68, Theorem 4.2], (B.134) implies that there exists a matrix M' such that (5.60) holds. Similarly, due to [68, Theorem 5.5], (B.135) implies that there exists a matrix L' such that (5.61) holds. On the other hand, (B.134) and (B.135) show that $(\bar{\mathcal{R}}, \mathcal{R})$ are a $(C', A'+G'K', B')$-pair, see [68, Definition 6.1], hence, due to [68, Lemma 6.3], there exists a matrix N such that (5.62) holds.

The only thing left to show is that (5.67) holds. To this end, let $(x + \bar{x}, w) \in \mathcal{S}'$, that is, $x = Rw$ and $\bar{x} \in \bar{\mathcal{R}}$. Note that (5.67) holds if there exist $x', \bar{x}', w'$ and d such that $(x' + \bar{x}', w') \in \mathcal{S}'$, that is, $x' = Rw'$ and $\bar{x}' \in \bar{\mathcal{R}}$, and

$$\begin{bmatrix} A' + B'NC' & B'M \\ LC' & K \end{bmatrix} \begin{bmatrix} x + \bar{x} \\ w \end{bmatrix} = \begin{bmatrix} x' + \bar{x}' \\ w' \end{bmatrix} + \begin{bmatrix} G' \\ 0 \end{bmatrix} d, \tag{B.141}$$

With this in mind, let

$$w' = LC'(x + \bar{x}) + Kw. \tag{B.142}$$

Using (5.64) and then (5.63), we obtain

$$\begin{aligned} LC'x &= R^{\dagger}(B'NC' + L'C')Rw \\ &= R^{\dagger}(A' + G'K' + B'M')x - Kw, \end{aligned} \tag{B.143}$$

which implies that we can write

$$w' = R^{\dagger}\big((A' + G'K' + B'M')x + (B'NC' + L'C')\bar{x}\big). \tag{B.144}$$

Since $x \in \mathcal{R}$, (5.60) yields

$$(A' + G'K' + B'M')x \in \mathcal{R}. \tag{B.145}$$

Moreover, since $\bar{x} \in \bar{\mathcal{R}}$, (5.61) and (5.62) yield

$$(A' + G'K' - L'C')\bar{x} \in \bar{\mathcal{R}} \subset \mathcal{R}, \tag{B.146}$$

$$(A' + G'K' + B'NC')\bar{x} \in \mathcal{R}, \tag{B.147}$$

and taking their difference yields

$$(B'NC + L'C')\bar{x} \in \mathcal{R}. \tag{B.148}$$

Let

$$x' = Rw' \tag{B.149}$$

Since $RR^{\dagger}z = z$ for all $z \in \mathcal{R}$, (B.144), (B.145) and (B.148) yield

$$x' = (A' + G'K' + B'M')x + (B'NC' + L'C')\bar{x}. \tag{B.150}$$

On the other hand, (5.65) yields

$$B'Mw = (B'M' - B'NC')x \tag{B.151}$$

which implies that

$$(A' + B'NC')x + B'Mw = (A' + B'M')x. \tag{B.152}$$

In view of (B.146), we have that

$$\bar{x}' = (A' + G'K' - L'C')\bar{x} \tag{B.153}$$

is such that $\bar{x}' \in \bar{\mathcal{R}}$. Furthermore, we can write

$$(A' + B'NC')\bar{x} = \bar{x}' + (B'NC' + L'C')\bar{x} - G'K'\bar{x}. \tag{B.154}$$

Now, due to (B.150), (B.152) and (B.154), it follows that

$$d = -K'(x + \bar{x}) \tag{B.155}$$

is such that

$$(A' + B'NC')(x + \bar{x}) + B'Mw = x' + \bar{x}' + Gd, \tag{B.156}$$

Finally, this implies that (B.141) holds with $x' = Rw'$ and $\bar{x}' \in \bar{\mathcal{R}}$, which shows that (5.67) holds. □

B.10 Proof of Theorem 5.2

The contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ is consistent if and only if there exist subspaces $\mathcal{R} \subset \mathcal{X}_a \times \mathcal{X}_g$ and $\bar{\mathcal{R}} \subset \mathcal{X}_a \times \mathcal{X}_g$ such that $\bar{\mathcal{R}} \subset \mathcal{R}$ and the following conditions are satisfied:

1. $\mathcal{R}$ is such that $\pi_{\mathcal{X}_a}(\mathcal{R}) = \mathcal{V}_a$ and

$$\begin{bmatrix} A_a & 0 \\ 0 & A_g \end{bmatrix}\mathcal{R} \subset \mathcal{R} + \mathrm{im}\begin{bmatrix} G_a & 0 \\ 0 & G_g \end{bmatrix}, \tag{5.68}$$

$$\mathcal{R} \subset \ker \begin{bmatrix} C_a & -C_g^u \\ H_a & 0 \\ 0 & H_g \end{bmatrix}. \tag{5.69}$$

2. $\bar{\mathcal{R}}$ is such that $\pi_{\mathcal{X}_a}(\bar{\mathcal{R}}) = \mathcal{V}_a$ and

$$\begin{bmatrix} A_a & 0 \\ 0 & A_g \end{bmatrix} \left(\bar{\mathcal{R}} \cap \ker \begin{bmatrix} C_a & 0 \end{bmatrix}\right) \subset \bar{\mathcal{R}} + \operatorname{im} \begin{bmatrix} G_a & 0 \\ 0 & G_g \end{bmatrix}, \tag{5.70}$$

$$\begin{bmatrix} \operatorname{im} G_a \cap \mathcal{V}_a \\ 0 \end{bmatrix} \subset \bar{\mathcal{R}} + \operatorname{im} \begin{bmatrix} 0 \\ G_g \end{bmatrix}, \tag{5.71}$$

$$\bar{\mathcal{R}} \subset \ker \begin{bmatrix} 0 & -C_g^y \end{bmatrix}. \tag{5.72}$$

Proof. We begin by proving necessity. Suppose that $\mathcal{C}$ is consistent. In view of Theorem 5.1, this implies that there exists a system Σ of the form (5.42) such that $\mathsf{A} \wedge \Sigma \preccurlyeq \Gamma$. Consequently, due to Proposition 5.1, there exists a subspace $\mathcal{S} \subset \mathcal{X}_a \times \mathcal{X} \times \mathcal{X}_g$ such that $\pi_{\mathcal{X}_a \times \mathcal{X}}(\mathcal{S}) = \mathcal{V}_a \times \mathcal{X}$ and

$$\begin{bmatrix} A_a & 0 & 0 \\ BC_a & A & 0 \\ 0 & 0 & A_g \end{bmatrix} \mathcal{S} \subset \mathcal{S} + \operatorname{im} \begin{bmatrix} G_a & 0 & 0 \\ 0 & G & 0 \\ 0 & 0 & G_g \end{bmatrix}, \tag{B.157}$$

$$\begin{bmatrix} \operatorname{im} \begin{bmatrix} G_a & 0 \\ 0 & G \\ & 0 \end{bmatrix} \cap (\mathcal{V}_a \times \mathcal{X}) \end{bmatrix} \subset \mathcal{S} + \operatorname{im} \begin{bmatrix} 0 \\ 0 \\ G_g \end{bmatrix}, \tag{B.158}$$

$$\mathcal{S} \subset \ker \begin{bmatrix} C_a & 0 & -C_g^u \\ 0 & C & -C_g^y \\ H_a & 0 & 0 \\ 0 & 0 & H_g \end{bmatrix}. \tag{B.159}$$

It is fairly straightforward to verify that $\mathcal{R} = \pi_{\mathcal{X}_a \times \mathcal{X}_g}(\mathcal{S})$ satisfies (5.68) and (5.69). On the other hand, the subspace

$$\bar{\mathcal{R}} = \{(x_a, x_g) \mid (x_a, 0, x_g) \in \mathcal{S}\} \tag{B.160}$$

satisfies (5.70), (5.71) and (5.72). Since $\pi_{\mathcal{X}_a \times \mathcal{X}}(\mathcal{S}) = \mathcal{V}_a \times \mathcal{X}$, it follows that $\pi_{\mathcal{X}_a}(\bar{\mathcal{R}}) = \pi_{\mathcal{X}_a}(\mathcal{R}) = \mathcal{V}_a$. We also have that $\bar{\mathcal{R}} \subset \mathcal{R}$, hence the proposed $\bar{\mathcal{R}}$ and $\mathcal{R}$ satisfy the conditions in Theorem 5.2 and we have proven necessity.

We proceed by proving sufficiency. We will do this by using Lemma 5.6. Suppose that the subspaces $\bar{\mathcal{R}} \subset \mathcal{R} \subset \mathcal{X}_a \times \mathcal{X}_g$ satisfy the conditions in Theorem 5.2. Let $B' = 0$ and

$$A' = \begin{bmatrix} A_a & 0 \\ 0 & A_g \end{bmatrix}, \quad G' = \begin{bmatrix} G_a & 0 \\ 0 & G_g \end{bmatrix}, \quad C' = \begin{bmatrix} C_a & 0 \end{bmatrix}, \tag{B.161}$$

and note that (5.68) and (5.70) yield (5.58) and (5.59), respectively. Since $B' = 0$, the matrices M', N and, hence, M, in Lemma 5.6 can be taken to be zero. Consequently, the matrices K and L defined in Lemma 5.6 are such that the subspace

$$\mathcal{S}' = \left\{ \begin{bmatrix} x_a + \bar{x}_a \\ x_g + \bar{x}_g \\ x \end{bmatrix} \;\middle|\; \begin{bmatrix} x_a \\ x_g \end{bmatrix} = Rx, \; \begin{bmatrix} \bar{x}_a \\ \bar{x}_g \end{bmatrix} \in \bar{\mathcal{R}} \right\}, \tag{B.162}$$

where the columns of R form a basis for $\mathcal{R}$, satisfies

$$\begin{bmatrix} A_a & 0 & 0 \\ 0 & A_g & 0 \\ LC_a & 0 & K \end{bmatrix} \mathcal{S}' \subset \mathcal{S}' + \operatorname{im} \begin{bmatrix} G_a & 0 \\ 0 & G_g \\ 0 & 0 \end{bmatrix} \tag{B.163}$$

Now, we can partially define a system Σ as in (5.42) by taking

$$A = K, \quad B = L, \quad G = 0. \tag{B.164}$$

Note that, due to (B.163), the subspace

$$\mathcal{S} = \{(x_a, x, x_g) \mid (x_a, x_g, x) \in \mathcal{S}'\} \tag{B.165}$$

satisfies (B.157). Furthermore, as $\pi_{\mathcal{X}_a}(\bar{\mathcal{R}}) = \mathcal{V}_a$ and x is free in $\mathcal{S}'$, it follows that $\pi_{\mathcal{X}_a \times \mathcal{X}}(\mathcal{S}') = \mathcal{V}_a \times \mathcal{X}$ and thus

$$\pi_{\mathcal{X}_a \times \mathcal{X}}(\mathcal{S}) = \mathcal{V}_a \times \mathcal{X}. \tag{B.166}$$

On the other hand, due to (5.71), for all d_a such that $G_a d_a \in \mathcal{V}_a$, there exists d_g such that $(G_a d_a, G_g d_g) \in \bar{\mathcal{R}}$, which implies that $(G_a d_a, 0, G_g d_g) \in \mathcal{S}$ and thus (B.158) holds. Finally, let

$$C = \begin{bmatrix} 0 & C_g^y \end{bmatrix} R \tag{B.167}$$

and take $(x_a + \bar{x}_a, x, x_g + \bar{x}_g) \in \mathcal{S}$. Note that

$$Cx = \begin{bmatrix} 0 & C_g^y \end{bmatrix} Rx = C_g^y x_g = C_g^y (x_g + \bar{x}_g), \tag{B.168}$$

where we used (5.72) for the last equality. Since $\bar{\mathcal{R}} \subset \mathcal{R}$, it follows that $(x_a + \bar{x}_a, x_g + \bar{x}_g) \in \mathcal{R}$, hence (B.168) and (5.69) yield

$$\begin{bmatrix} C_a & 0 & -C_g^u \\ 0 & C & -C_g^y \\ H_a & 0 & 0 \\ 0 & 0 & H_g \end{bmatrix} \begin{bmatrix} x_a + \bar{x}_a \\ x \\ x_g + \bar{x}_g \end{bmatrix} = 0, \tag{B.169}$$

which shows that (B.159) holds as well. Therefore, due to Proposition 5.1, the system Σ as in (5.42) is such that $\mathsf{A} \wedge \Sigma \preccurlyeq \Gamma$. Theorem 5.1 then implies that Σ is an implementation of $\mathcal{C}$ and we conclude that $\mathcal{C}$ is consistent. □

B.11 Proof of Lemma 5.8

We start by showing necessity. Suppose that $\bar{\mathcal{R}} \subset \mathcal{R}$ satisfies the second condition in Theorem 5.2. Due to Lemma 5.7, this means that $\bar{\mathcal{R}}$ satisfies (5.74) as well. Since $\pi_{\mathcal{X}_a}(\bar{\mathcal{R}}) = \mathcal{V}_a$, there exist matrices $\bar{R}_g$ and $\hat{R}_g^0$ such that

$$\bar{\mathcal{R}} = \operatorname{im} \begin{bmatrix} V_a & 0 \\ \bar{R}_g & \hat{R}_g^0 \end{bmatrix}. \tag{B.170}$$

Consequently $(x_a, x_g) \in \bar{\mathcal{R}} \cap \ker \begin{bmatrix} C_a & 0 \end{bmatrix}$ if and only if

$$\begin{bmatrix} x_a \\ x_g \end{bmatrix} = \begin{bmatrix} V_a & 0 \\ \bar{R}_g & \hat{R}_g^0 \end{bmatrix} \begin{bmatrix} z \\ z_0 \end{bmatrix} \tag{B.171}$$

where z is such that $C_a V_a z = 0$ and z_0 is arbitrary. Since $C_a V_a z = 0$ if and only if $z \in \operatorname{im} C_a^{\mathcal{V}}$, it follows that

$$\bar{\mathcal{R}} \cap \ker \begin{bmatrix} C_a & 0 \end{bmatrix} = \operatorname{im} \begin{bmatrix} V_a C_a^{\mathcal{V}} \\ \bar{R}_g C_a^{\mathcal{V}} \end{bmatrix} + \operatorname{im} \begin{bmatrix} 0 \\ \hat{R}_g^0 \end{bmatrix}, \tag{B.172}$$

Using the latter, we see that (5.74) holds if and only if

$$\begin{bmatrix} A_a + G_a F_a & 0 \\ 0 & A_g \end{bmatrix} \operatorname{im} \begin{bmatrix} 0 \\ \hat{R}_g^0 \end{bmatrix} \subset \operatorname{im} \begin{bmatrix} V_a & 0 \\ \bar{R}_g & \hat{R}_g^0 \end{bmatrix} + \operatorname{im} \begin{bmatrix} 0 \\ G_g \end{bmatrix}, \tag{B.173}$$

$$\begin{bmatrix} A_a + G_a F_a & 0 \\ 0 & A_g \end{bmatrix} \operatorname{im} \begin{bmatrix} V_a C_a^{\mathcal{V}} \\ \bar{R}_g C_a^{\mathcal{V}} \end{bmatrix} \subset \operatorname{im} \begin{bmatrix} V_a & 0 \\ \bar{R}_g & \hat{R}_g^0 \end{bmatrix} + \operatorname{im} \begin{bmatrix} 0 \\ G_g \end{bmatrix}. \tag{B.174}$$

It is easily seen that (B.173) holds if and only if

$$A_g \operatorname{im} \hat{R}_g^0 \subset \operatorname{im} \hat{R}_g^0 + \operatorname{im} G_g. \tag{B.175}$$

At the same time, as $\bar{\mathcal{R}} \subset \mathcal{R}$ and (5.72) holds, we have that

$$\operatorname{im} \begin{bmatrix} 0 \\ \hat{R}_g^0 \end{bmatrix} \subset \ker \begin{bmatrix} R_a^{\perp} & R_g^{\perp} \\ 0 & -C_g^y \end{bmatrix}, \tag{B.176}$$

which holds if and only if

$$\operatorname{im} \hat{R}_g^0 \subset \ker \begin{bmatrix} R_g^{\perp} \\ -C_g^y \end{bmatrix}. \tag{B.177}$$

Then, (B.175) and (B.177) imply that $\operatorname{im} \hat{R}_g^0 \subset \bar{\mathcal{R}}_g^0$, hence there exists a matrix T such that

$$\hat{R}_g^0 = \bar{R}_g^0 T. \tag{B.178}$$

On the other hand, (B.174) holds if and only if there exist matrices U, X' and Y such that

$$(A_a + G_a F_a) V_a C_a^{\mathcal{V}} = V_a U \tag{B.179}$$

$$A_g \bar{R}_g C_a^{\mathcal{V}} = \bar{R}_g U + \hat{R}_g^0 X' + G_g Y. \tag{B.180}$$

The first equation yields

$$U = V_a^{\dagger} (A_a + G_a F_a) V_a C_a^{\mathcal{V}}, \tag{B.181}$$

which we can substitute in the second equation to obtain

$$A_g\bar{R}_gC_a^{\mathcal{V}} = \bar{R}_gV_a^{\dagger}(A_a + G_aF_a)V_aC_a^{\mathcal{V}} + \hat{R}_g^0X' + G_gY. \tag{B.182}$$

Note that the latter is equivalent to (5.81) with $X = TX'$. Next, from (5.71) it follows that

$$\operatorname{im}\begin{bmatrix} G_a^{\mathcal{V}} \\ 0 \end{bmatrix} \subset \operatorname{im}\begin{bmatrix} V_a & 0 \\ \bar{R}_g & \hat{R}_g^0 \end{bmatrix} + \operatorname{im}\begin{bmatrix} 0 \\ G_g \end{bmatrix}, \tag{B.183}$$

hence there exist matrices U', W' and Z such that

$$G_a^{\mathcal{V}} = V_aU' \tag{B.184}$$

$$0 = \bar{R}_gU' + \hat{R}_g^0W' + G_gZ. \tag{B.185}$$

Again, the first equation yields

$$U' = V_a^{\dagger}G_a^{\mathcal{V}}, \tag{B.186}$$

which we substitute in the second equation to obtain

$$0 = \bar{R}_gV_a^{\dagger}G_a^{\mathcal{V}} + \hat{R}_g^0W' + G_gZ. \tag{B.187}$$

Note that the latter is equivalent to (5.82) with $W = TW'$. Finally, as $\bar{\mathcal{R}} \subset \mathcal{R}$ and (5.72) holds, we get

$$\operatorname{im}\begin{bmatrix} V_a \\ \bar{R}_g \end{bmatrix} \subset \ker\begin{bmatrix} R_a^{\perp} & R_g^{\perp} \\ 0 & -C_y^g \end{bmatrix}, \tag{B.188}$$

which is equivalent to (5.83). This concludes the proof as we have shown that there exist matrices $\bar{R}_g$, W, X, Y and Z such that (5.81), (5.82) and (5.83) hold.

We now turn to proving sufficiency. Suppose that there exist matrices $\bar{R}_g$, W, X, Y and Z such that (5.81), (5.82) and (5.83) hold. Let $\bar{\mathcal{R}}$ be given by (5.84) and note that

$$\bar{\mathcal{R}} \cap \ker\begin{bmatrix} C_a & 0 \end{bmatrix} = \operatorname{im}\begin{bmatrix} V_aC_a^{\mathcal{V}} \\ \bar{R}_gC_a^{\mathcal{V}} \end{bmatrix} + \operatorname{im}\begin{bmatrix} 0 \\ \bar{R}_g^0 \end{bmatrix} \tag{B.189}$$

similarly to (B.172). Now, since $\operatorname{im}\bar{R}_g^0 = \bar{\mathcal{R}}_{g'}^0$ (5.80) yields

$$\operatorname{im}\begin{bmatrix} 0 \\ A_g\bar{R}_g^0 \end{bmatrix} \subset \operatorname{im}\begin{bmatrix} 0 \\ R_g^0 \end{bmatrix} + \operatorname{im}\begin{bmatrix} 0 \\ G_g \end{bmatrix}, \tag{B.190}$$

which implies that

$$\begin{bmatrix} A_a + G_aF_a & 0 \\ 0 & A_g \end{bmatrix}\operatorname{im}\begin{bmatrix} 0 \\ \bar{R}_g^0 \end{bmatrix} \subset \bar{\mathcal{R}} + \operatorname{im}\begin{bmatrix} 0 \\ G_g \end{bmatrix}. \tag{B.191}$$

Let U be as in (B.181). Since $\operatorname{im} V_a C_a^{\mathcal{V}} \subset \mathcal{V}_a$, (5.73) implies that

$$\operatorname{im}(A_a + G_a F_a) V_a C_a^{\mathcal{V}} \subset \mathcal{V}_a. \tag{B.192}$$

Consequently, we obtain

$$V_a U = (A_a + G_a F_a) V_a C_a^{\mathcal{V}}, \tag{B.193}$$

where we used the fact that $V_a V_a^{\dagger} z = z$ for all $z \in \mathcal{V}_a$. Then (B.193) and (5.81) can be written as

$$\begin{bmatrix} A_a + G_a F_a & 0 \\ 0 & A_g \end{bmatrix} \begin{bmatrix} V_a C_a^{\mathcal{V}} \\ \bar{R}_g C_a^{\mathcal{V}} \end{bmatrix} = \begin{bmatrix} V_a & 0 \\ \bar{R}_g & \bar{R}_g^0 \end{bmatrix} \begin{bmatrix} U \\ X \end{bmatrix} + \begin{bmatrix} 0 \\ G_g \end{bmatrix} Y, \tag{B.194}$$

from which we conclude that

$$\begin{bmatrix} A_a + G_a F_a & 0 \\ 0 & A_g \end{bmatrix} \operatorname{im} \begin{bmatrix} V_a C_a^{\mathcal{V}} \\ \bar{R}_g C_a^{\mathcal{V}} \end{bmatrix} \subset \bar{\mathcal{R}} + \operatorname{im} \begin{bmatrix} 0 \\ G_g \end{bmatrix}. \tag{B.195}$$

In view of (B.189), (B.191) and (B.194) imply that (5.74) holds. Next, let U' be as in (B.186) and note that $V_a U' = G_a^{\mathcal{V}}$ because $\operatorname{im} G_A^{\mathcal{V}} \subset \mathcal{V}_a$. Therefore, we can use (5.82) to write

$$\begin{bmatrix} G_a^{\mathcal{V}} \\ 0 \end{bmatrix} = \begin{bmatrix} V_a & 0 \\ \bar{R}_g & \bar{R}_g^0 \end{bmatrix} \begin{bmatrix} U' \\ W \end{bmatrix} + \begin{bmatrix} 0 \\ G_g \end{bmatrix} Z, \tag{B.196}$$

which implies that

$$\operatorname{im} \begin{bmatrix} G_a^{\mathcal{V}} \\ 0 \end{bmatrix} \subset \bar{\mathcal{R}} + \operatorname{im} \begin{bmatrix} 0 \\ G_g \end{bmatrix} \tag{B.197}$$

and thus (5.71) holds by definition of $G_a^{\mathcal{V}}$. Finally, in view of (5.80), we have that

$$\operatorname{im} \begin{bmatrix} 0 \\ \bar{R}_g^0 \end{bmatrix} \subset \ker \begin{bmatrix} R_a^{\perp} & R_g^{\perp} \\ 0 & -C_g^y \end{bmatrix}. \tag{B.198}$$

Together with (5.83), the latter implies that

$$\bar{\mathcal{R}} \subset \ker \begin{bmatrix} R_a^{\perp} & R_g^{\perp} \\ 0 & -C_g^y \end{bmatrix}, \tag{B.199}$$

hence $\bar{\mathcal{R}} \subset \mathcal{R}$ and (5.72) holds. In other words, we have shown that $\bar{\mathcal{R}}$ satisfies the second condition in Theorem 5.2, which concludes the proof.

B.12 Proof of Theorem 5.3

There exists a controller C such that P $\wedge$ C implements $\mathcal{C} = (\mathrm{A}, \Gamma)$ if and only if there exist subspaces $\mathcal{R} \subset \mathcal{X}_a \times \mathcal{X}_p \times \mathcal{X}_g$ and $\mathcal{R} \subset \mathcal{X}_a \times \mathcal{X}_p \times \mathcal{X}_g$ such that $\bar{\mathcal{R}} \subset \mathcal{R}$ and the following conditions are satisfied:

1. $\mathcal{R}$ is such that $\pi_{\mathcal{X}_a \times \mathcal{X}_p}(\mathcal{R}) = \mathcal{V}_a \times \mathcal{X}_p$ and

$$\begin{bmatrix} A_a & 0 & 0 \\ B_p^u C_a & A_p & 0 \\ 0 & 0 & A_g \end{bmatrix} \mathcal{R} \subset \mathcal{R} + \operatorname{im} \begin{bmatrix} 0 & G_a & 0 \\ B_p^v & 0 & 0 \\ 0 & 0 & G_g \end{bmatrix}, \tag{5.88}$$

$$\mathcal{R} \subset \ker \begin{bmatrix} C_a & 0 & -C_g^u \\ 0 & C_p^y & -C_g^y \\ H_a & 0 & 0 \\ 0 & 0 & H_g \end{bmatrix}. \tag{5.89}$$

2. $\bar{\mathcal{R}}$ is such that $\pi_{\mathcal{X}_a \times \mathcal{X}_p}(\bar{\mathcal{R}}) = \mathcal{V}_a \times \mathcal{X}_p$ and

$$\begin{bmatrix} A_a & 0 & 0 \\ B_p^u C_a & A_p & 0 \\ 0 & 0 & A_g \end{bmatrix} \left(\bar{\mathcal{R}} \cap \ker \begin{bmatrix} 0 & C_p^z & 0 \end{bmatrix}\right) \subset \bar{\mathcal{R}} + \operatorname{im} \begin{bmatrix} G_a & 0 \\ 0 & 0 \\ 0 & G_g \end{bmatrix}, \tag{5.90}$$

$$\begin{bmatrix} \operatorname{im} G_a \cap \mathcal{V}_a \\ 0 \\ 0 \end{bmatrix} \subset \bar{\mathcal{R}} + \operatorname{im} \begin{bmatrix} 0 \\ 0 \\ G_g \end{bmatrix}. \tag{5.91}$$

Proof. We begin by proving necessity. Suppose that C is such that P∧C implements $\mathcal{C}$. Due to Theorem 5.1, this implies that A∧(P∧C) $\preccurlyeq \Gamma$. Then, there exists a full simulation relation of A∧(P∧C) by Γ, which, due to Proposition 5.1, is a subspace $\mathcal{S} \subset \mathcal{X}_a \times \mathcal{X}_p \times \mathcal{W} \times \mathcal{X}_g$ such that $\pi_{\mathcal{X}_a \times \mathcal{X}_p \times \mathcal{W}}(\mathcal{S}) = \mathcal{V}_a \times \mathcal{X}_p \times \mathcal{W}$ and

$$\begin{bmatrix} A_a & 0 & 0 & 0 \\ B_p^u C_a & A_p + B_p^v N C_p^z & B_p^v M & 0 \\ 0 & L C_p^z & K & 0 \\ 0 & 0 & 0 & A_g \end{bmatrix} \mathcal{S} \subset \mathcal{S} + \operatorname{im} \begin{bmatrix} G_a & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & G_g \end{bmatrix}, \tag{B.200}$$

$$\begin{bmatrix} \operatorname{im} G_a \cap \mathcal{V}_a \\ 0 \\ 0 \\ 0 \end{bmatrix} \subset \mathcal{S} + \operatorname{im} \begin{bmatrix} 0 \\ 0 \\ 0 \\ G_g \end{bmatrix}, \tag{B.201}$$

$$\mathcal{S} \subset \ker \begin{bmatrix} C_a & 0 & 0 & -C_g^u \\ 0 & C_p^y & 0 & -C_g^y \\ H_a & 0 & 0 & 0 \\ 0 & 0 & 0 & H_g \end{bmatrix}. \tag{B.202}$$

Analogously to the proof of Theorem 5.2, we take

$$\mathcal{R} = \pi_{\mathcal{X}_a \times \mathcal{X}_p \times \mathcal{X}_g}(\mathcal{S}), \tag{B.203}$$

$$\bar{\mathcal{R}} = \{(x_a, x_p, x_g) \mid (x_a, x_p, 0, x_g) \in \mathcal{S}\}. \tag{B.204}$$

As $\pi_{\mathcal{X}_a \times \mathcal{X}_p \times \mathcal{W}}(\mathcal{S}) = \mathcal{V}_a \times \mathcal{X}_p \times \mathcal{W}$, we have that $\pi_{\mathcal{X}_a \times \mathcal{X}_p}(\mathcal{R}) = \mathcal{V}_a \times \mathcal{X}_p$ and $\pi_{\mathcal{X}_a \times \mathcal{X}_p}(\bar{\mathcal{R}}) = \mathcal{V}_a \times \mathcal{X}_p$. Moreover, it is straightforward to show that (B.200) implies (5.88) and (5.90), (B.201) implies (5.91), and (B.202) implies (5.91).

We proceed by proving sufficiency. We will do this with Lemma 5.6. Let

$$A' = \begin{bmatrix} A_a & 0 & 0 \\ B_p^u C_a & A_p & 0 \\ 0 & 0 & A_g \end{bmatrix}, \quad B' = \begin{bmatrix} 0 \\ B_p^v \\ 0 \end{bmatrix}, \tag{B.205}$$

$$C' = \begin{bmatrix} 0 & C_p^z & 0 \end{bmatrix}, \qquad G' = \begin{bmatrix} G_a & 0 \\ 0 & 0 \\ 0 & G_g \end{bmatrix}, \tag{B.206}$$

Then (5.88) and (5.90) yield (5.58) and (5.59), respectively. Consequently, the matrices K, L, M and N defined in Lemma 5.6 are such that the subspace

$$\mathcal{S}' = \left\{ \begin{bmatrix} x_a + \bar{x}_a \\ x_p + \bar{x}_p \\ x_g + \bar{x}_g \\ w \end{bmatrix} \;\middle|\; \begin{bmatrix} x_a \\ x_p \\ x_g \end{bmatrix} = Rw, \; \begin{bmatrix} \bar{x}_a \\ \bar{x}_p \\ \bar{x}_g \end{bmatrix} \in \bar{\mathcal{R}} \right\} \tag{B.207}$$

satisfies (5.67). Therefore, the subspace

$$\mathcal{S} = \{ (x_a, x_p, w, x_g) \mid (x_a, x_p, x_g, w) \in \mathcal{S}' \} \tag{B.208}$$

satisfies (B.200). Moreover, we have that $\pi_{\mathcal{X}_a \times \mathcal{X}_p}(\bar{\mathcal{R}}) = \mathcal{V}_a \times \mathcal{X}_p$ and w is free in $\mathcal{S}'$, hence $\pi_{\mathcal{X}_a \times \mathcal{X}_p \times \mathcal{W}}(\mathcal{S}') = \mathcal{V}_a \times \mathcal{X}_p \times \mathcal{W}$ and, thus,

$$\pi_{\mathcal{X}_a \times \mathcal{X}_p \times \mathcal{W}}(\mathcal{S}) = \mathcal{V}_a \times \mathcal{X}_p \times \mathcal{W}. \tag{B.209}$$

Finally, we have that (5.91) implies (B.201), and (5.89) implies (B.202). Indeed, due to (5.91), for all d_a such that $G_a d_a \in \mathcal{V}$, there exists d_g such that $(G_a d_a, 0, G_g d_g) \in \bar{\mathcal{R}}$, which implies that $(G_a d_a, 0, 0, G_g d_g) \in \mathcal{S}$, by definition of $\mathcal{S}$. On the other hand, since $\bar{\mathcal{R}} \subset \mathcal{R}$, (5.89) implies that

$$\begin{bmatrix} x_a + \bar{x}_a \\ x_p + \bar{x}_p \\ w \\ x_g + \bar{x}_g \end{bmatrix} \in \ker \begin{bmatrix} C_a & 0 & 0 & -C_g^u \\ 0 & C_p^y & 0 & -C_g^y \\ H_a & 0 & 0 & 0 \\ 0 & 0 & 0 & H_g \end{bmatrix}, \tag{B.210}$$

if $(x_a, x_p, x_g) \in \mathcal{R}$ and $(\bar{x}_a, \bar{x}_p, \bar{x}_g) \in \bar{\mathcal{R}}$, hence (B.202) holds by definition of $\mathcal{S}$. □

B.13 Proof of Lemma 5.9

Suppose that the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ is consistent. Then there exists a system Σ that implements $\mathcal{C}$ and is such that

$$\mathrm{E} \wedge \Gamma \preccurlyeq \mathrm{E} \wedge \Sigma \tag{5.119}$$

for all environments E compatible with $\mathcal{C}$.

Proof. Let A and Γ be given by (5.45) and (5.46), respectively. Furthermore, let the subspaces $\mathcal{R}$ and $\bar{\mathcal{R}}$, and the matrices A, B and C be constructed as in Algorithm 1 or, equivalently, as in the proof of Theorem 5.2. Let R be a matrix whose columns form a basis for $\mathcal{R}$, and let $R^\dagger$ be a matrix such that $R^\dagger R = I$. Recall that such a matrix $R^\dagger$ exists because R has full column rank. Consider the system Σ given by (5.42), where G is a matrix whose columns form a basis for the subspace

$$R^\dagger \left(\operatorname{im} \begin{bmatrix} 0 \\ G_g \end{bmatrix} \cap \mathcal{R} \right). \tag{B.211}$$

We will show that Σ is an implementation of $\mathcal{C}$ by showing that the subspace $\mathcal{S} \subset \mathcal{X}_a \times \mathcal{X} \times \mathcal{X}_g$ given by

$$\mathcal{S} = \left\{ (x_a + \bar{x}_a, x, x_g + \bar{x}_g) \;\middle|\; Rx = \begin{bmatrix} x_a \\ x_g \end{bmatrix},\ \begin{bmatrix} \bar{x}_a \\ \bar{x}_g \end{bmatrix} \subset \bar{\mathcal{R}} \right\} \tag{B.212}$$

is a full simulation relation of A $\wedge$ Σ by Γ. To this end, in the proof of Theorem 5.2, we already showed that $\mathcal{S}$ is such that

$$\begin{bmatrix} A_a & 0 & 0 \\ BC_a & A & 0 \\ 0 & 0 & A_g \end{bmatrix} \mathcal{S} \subset \mathcal{S} + \operatorname{im} \begin{bmatrix} G_a & 0 \\ 0 & 0 \\ 0 & G_g \end{bmatrix}, \tag{B.213}$$

$$\begin{bmatrix} \operatorname{im} G_a \cap \mathcal{V}_a \\ 0 \\ 0 \end{bmatrix} \subset \mathcal{S} + \operatorname{im} \begin{bmatrix} 0 \\ 0 \\ G_g \end{bmatrix}, \tag{B.214}$$

$$\mathcal{S} \subset \ker \begin{bmatrix} C_a & 0 & -C_g^u \\ 0 & C & -C_g^y \\ H_a & 0 & 0 \\ 0 & 0 & H_g \end{bmatrix}. \tag{B.215}$$

and $\pi_{\mathcal{X}_a \times \mathcal{X}}(\mathcal{S}) = \mathcal{V}_a \times \mathcal{X}$. Therefore, we only need to show that

$$\operatorname{im} \begin{bmatrix} 0 \\ G \\ 0 \end{bmatrix} \subset \mathcal{S} + \operatorname{im} \begin{bmatrix} 0 \\ 0 \\ G_g \end{bmatrix} \tag{B.216}$$

in order to conclude that $\mathcal{S}$ is indeed a full simulation relation of A $\wedge$ Σ by Γ.

With this in mind, let $d \in \mathcal{D}$ and note that, by definition of G, there exists $d_g \in \mathcal{D}_g$ such that $(0, G_g d_g) \in \mathcal{R}$ and

$$Gd = R^\dagger \begin{bmatrix} 0 \\ G_g d_g \end{bmatrix}. \tag{B.217}$$

Since $RR^\dagger z = z$ for all $z \in \mathcal{R}$, it follows that

$$RGd = \begin{bmatrix} 0 \\ G_g d_g \end{bmatrix}, \tag{B.218}$$

hence $(0, Gd, G_g d_g) \in \mathcal{S}$ and, thus, (B.216) holds. Therefore, $\mathcal{S}$ is a full simulation relation of $\mathrm{A} \wedge \Sigma$ by Γ, hence $\mathrm{A} \wedge \Sigma \preccurlyeq \Gamma$, which, due to Theorem 5.1, implies that Σ implements $\mathcal{C}$.

Now, in order to show that (5.119) holds, consider an environment E of the form (5.43) that is compatible with $\mathcal{C}$, that is, $\mathrm{E} \preccurlyeq \mathrm{A}$. Let $\mathcal{S}_{ea}$ be a full simulation relation of E by A. We will show that $\mathrm{E} \wedge \Gamma \preccurlyeq \mathrm{E} \wedge \Sigma$ by showing that the subspace $\mathcal{S}_{gs} \subset \mathcal{X}_a \times \mathcal{X}_g \times \mathcal{X}_a \times \mathcal{X}$ given by

$$\mathcal{S}_{gs} = \{(x_e, x_g, x_e, x) \mid \exists x_a \in \mathcal{X}_a \text{ s.t. } (x_e, x_a) \in \mathcal{S}_{ea},\ (x_a, x, x_g) \in \mathcal{S}\} \tag{B.219}$$

is a full simulation relation of $\mathrm{E} \wedge \Gamma$ by $\mathrm{E} \wedge \Sigma$. To this end, we need to show that

$$\begin{bmatrix} A_e & 0 & 0 & 0 \\ 0 & A_g & 0 & 0 \\ 0 & 0 & A_e & 0 \\ 0 & 0 & BC_e & A \end{bmatrix} \mathcal{S}_{gs} \subset \mathcal{S}_{gs} + \operatorname{im} \begin{bmatrix} G_e & 0 & 0 & 0 \\ 0 & G_g & 0 & 0 \\ 0 & 0 & G_e & 0 \\ 0 & 0 & 0 & G \end{bmatrix}, \tag{B.220}$$

$$\begin{bmatrix} \operatorname{im} \begin{bmatrix} G_e & 0 \\ 0 & G_g \end{bmatrix} \cap \mathcal{V}_{eg} \\ 0 \\ 0 \end{bmatrix} \subset \mathcal{S}_{gs} + \operatorname{im} \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ G_e & 0 \\ 0 & G \end{bmatrix}, \tag{B.221}$$

$$\mathcal{S}_{gs} \subset \ker \begin{bmatrix} C_e & 0 & -C_e & 0 \\ 0 & C_g^y & 0 & -C \\ H_e & 0 & 0 & 0 \\ 0 & H_g & 0 & 0 \\ C_e & -C_g^u & 0 & 0 \\ 0 & 0 & H_e & 0 \end{bmatrix}, \tag{B.222}$$

and $\pi_{\mathcal{X}_e \times \mathcal{X}_g}(\mathcal{S}_{gs}) = \mathcal{V}_{eg}$, where $\mathcal{V}_{eg}$ is the consistent subspace of $\mathrm{E} \wedge \Gamma$.

We will first show that (B.220) and (B.222) hold. Let $(x_e, x_g, x_e, x) \in \mathcal{S}_{gs}$, that is, $(x_e, x_a) \in \mathcal{S}_{ea}$ and $(x_a, x, x_g) \in \mathcal{S}$ for some $x_a \in \mathcal{X}_a$. Let $d_e \in \mathcal{D}_e$ be such that $A_e x_e + G_e d_e \in \mathcal{V}_e$. As $\mathcal{S}_{ea}$ is a simulation relation, it follows that there exists $d_a \in \mathcal{D}_a$ such that

$$(A_e x_e + G_e d_e, A_a x_a + G_a d_a) \in \mathcal{S}_{ea}. \tag{B.223}$$

This means that $A_a x_a + G_a d_a \in \mathcal{V}_a$, hence there exists $d_g \in \mathcal{D}_g$ such that

$$(A_a x_a + G_a d_a, Ax + BC_a x_a, A_g x_g + G_g d_g) \in \mathcal{S} \tag{B.224}$$

because $\mathcal{S}$ is a simulation relation. Since $(x_e, x_a) \in \mathcal{S}_{ea}$, it follows that

$$C_e x_e = C_a x_a, \quad H_e x_e = 0, \quad 0 = H_a x_a, \tag{B.225}$$

hence, in particular, we can replace $C_a x_a$ by $C_e x_e$ in (B.224) to obtain

$$(A_a x_a + G_a d_a, Ax + BC_e x_e, A_g x_g + G_g d_g) \in \mathcal{S}. \tag{B.226}$$

Together with (B.223), this implies that

$$(A_e x_e + G_e d_e, A_g x_g + G_g d_g, A_e x_e + G_e d_e, Ax + BC_e x_e) \in \mathcal{S}_{gs}, \tag{B.227}$$

which shows that (B.220) holds. On the other hand, we have that

$$C_a x_a = C_g^u x_g, \quad Cx = C_g^y x_g, \quad H_g x_g = 0, \tag{B.228}$$

since $(x_a, x, x_g) \in \mathcal{S}$. Together with (B.225), this implies that (B.222) holds.

Next, we will show that $\pi_{\mathcal{X}_e \times \mathcal{X}_g}(\mathcal{S}_{gs}) = \mathcal{V}_{eg}$. As explained in Remark 5.1, since $\mathcal{S}_{gs}$ satisfies (B.220) and (B.222), it follows that $\pi_{\mathcal{X}_e \times \mathcal{X}_g}(\mathcal{S}_{gs}) \subset \mathcal{V}_{eg}$. To show the converse, let $(x_e, x_g) \in \mathcal{V}_{eg}$. This yields $x_e \in \mathcal{V}_e$, hence there exists $x_a \in \mathcal{X}_a$ such that $(x_e, x_a) \in \mathcal{S}_{ea}$, which, in turn, yields $x_a \in \mathcal{V}_a$. Consequently, for any $x' \in \mathcal{X}$, there exists $x'_g \in \mathcal{V}_g$ such that $(x_a, x', x'_g) \in \mathcal{S}$ and, thus,

$$(x_e, x'_g, x_e, x') \in \mathcal{S}_{gs}. \tag{B.229}$$

Since $\pi_{\mathcal{X}_e \times \mathcal{X}_g}(\mathcal{S}_{gs}) \subset \mathcal{V}_{eg}$, it follows that $(x_e, x'_g) \in \mathcal{V}_{eg}$, hence $(0, x_g - x'_g) \in \mathcal{V}_{eg}$ by linearity. We claim that $(0, x_g - x'_g) \in \mathcal{R}$. To see this, note that the consistent subspace $\mathcal{V}_{eg}$ is such that the subspace $\mathcal{V}_{0g} \subset \mathcal{X}_g$ given by

$$\mathcal{V}_{0g} = \{ x_g \mid (0, x_g) \in \mathcal{V}_{eg} \} \tag{B.230}$$

satisfies

$$A_g \mathcal{V}_{0g} \subset \mathcal{V}_{0g} + \operatorname{im} G_g, \quad \mathcal{V}_{0g} \subset \ker \begin{bmatrix} -C_g^u \\ H_g \end{bmatrix}, \tag{B.231}$$

hence the subspace $\{0\} \times \mathcal{V}_{0g} \subset \mathcal{X}_a \times \mathcal{X}_g$ satisfies

$$\begin{bmatrix} A_a & 0 \\ 0 & A_g \end{bmatrix} (\{0\} \times \mathcal{V}_{0g}) \subset (\{0\} \times \mathcal{V}_{0g}) + \operatorname{im} \begin{bmatrix} G_a & 0 \\ 0 & G_g \end{bmatrix}, \tag{B.232}$$

$$\{0\} \times \mathcal{V}_{0g} \subset \ker \begin{bmatrix} C_a & -C_g^u \\ H_a & 0 \\ 0 & H_g \end{bmatrix}. \tag{B.233}$$

Since $\mathcal{R}$ is the largest such subspace, it follows that $\{0\} \times \mathcal{V}_{0g} \subset \mathcal{R}$. Therefore, $(0, x_g - x'_g) \in \mathcal{V}_{eg}$ implies that $(0, x_g - x'_g) \in \mathcal{R}$, which, in turn, implies that there exists $x'' \in \mathcal{X}$ such that

$$Rx'' = \begin{bmatrix} 0 \\ x_g - x'_g \end{bmatrix}. \tag{B.234}$$

This means that $(0, x'', x_g - x'_g) \in \mathcal{S}$, and, since $(0,0) \in \mathcal{S}_{ea}$, we obtain

$$(0, x_g - x'_g, 0, x'') \in \mathcal{S}_{gs}. \tag{B.235}$$

Together with (B.229), this implies that

$$(x_e, x_g, x_e, x' + x'') \in \mathcal{S}_{gs}, \tag{B.236}$$

which shows that $(x_e, x_g) \in \pi_{\mathcal{X}_e \times \mathcal{X}_g}(\mathcal{S}_{gs})$ and, thus, $\pi_{\mathcal{X}_e \times \mathcal{X}_g}(\mathcal{S}_{gs}) = \mathcal{V}_{eg}$.

Finally, we will show that (B.221) holds. Let $d_e \in \mathcal{D}_e$ and $d_g \in \mathcal{D}_g$ be such that $(G_e d_e, G_g d_g) \in \mathcal{V}_{eg}$. In particular, this means that $G_e d_e \in \mathcal{V}_e$, hence there exists $d_a \in \mathcal{D}_a$ such that $(G_e d_e, G_a d_a) \in \mathcal{S}_{ea}$. But then $G_a d_a \in \mathcal{V}_a$, hence there exists $d'_g \in \mathcal{D}_g$ such that $(G_a d_a, 0, G_g d'_g) \in \mathcal{S}$. Consequently, we have that

$$(G_e d_e, G_g d'_g, G_e d_e, 0) \in \mathcal{S}_{gs}, \tag{B.237}$$

which implies that $(G_e d_e, G_g d'_g) \in \mathcal{V}_{eg}$. Then, $(0, G_g(d_g - d'_g)) \in \mathcal{V}_{eg}$ by linearity, hence, as shown earlier, $(0, G_g(d_g - d'_g)) \in \mathcal{R}$. By definition of G, there exists $d \in \mathcal{D}$ such that

$$Gd = R^\dagger \begin{bmatrix} 0 \\ G_g(d_g - d'_g) \end{bmatrix}. \tag{B.238}$$

Since $RR^\dagger z = z$ for all $z \in \mathcal{R}$, it follows that

$$RGd = \begin{bmatrix} 0 \\ G_g(d_g - d'_g) \end{bmatrix}, \tag{B.239}$$

and, thus, $(0, Gd, G_g(d_g - d'_g)) \in \mathcal{S}$. Together with (B.237), this implies that

$$(G_e d_e, G_g d_g, G_e d_e, Gd) \in \mathcal{S}_{gs}, \tag{B.240}$$

which shows that (B.221) holds. In conclusion, we have shown that $\mathcal{S}_{gs}$ is a full simulation relation of $\mathrm{E} \wedge \Gamma$ by $\mathrm{E} \wedge \Sigma$, hence $\mathrm{E} \wedge \Gamma \preccurlyeq \mathrm{E} \wedge \Sigma$, as desired. □

B.14 Proof of Lemma 5.10

Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are consistent. Then, the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 5.1 if and only if

$$\hat{\mathrm{A}} \preccurlyeq \mathrm{A}_1, \tag{5.129}$$

$$\hat{\mathrm{A}} \wedge \hat{\Gamma}_1 \preccurlyeq \mathrm{A}_2, \tag{5.130}$$

$$\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2) \preccurlyeq \Gamma, \tag{5.131}$$

where $\hat{\mathrm{A}}$ is obtained from A by relabelling u to u_1, and $\hat{\Gamma}_1$ is obtained from Γ_1 by relabelling y_1 to u_2.

Proof. We begin by proving necessity. Suppose that $\mathcal{C} = (\mathrm{A}, \Gamma)$ satisfies Implication 5.1, where A and Γ are given by (5.45) and (5.46), respectively. Since $\mathcal{C}_1$ and $\mathcal{C}_2$ are consistent, due to Lemma 5.9, there exist systems Σ_1 and Σ_2 that implement $\mathcal{C}_1$ and $\mathcal{C}_1$, respectively, and are such that

$$\mathrm{E}_1 \wedge \Gamma_1 \preccurlyeq \mathrm{E}_1 \wedge \Sigma_1 \quad \text{and} \quad \mathrm{E}_2 \wedge \Gamma_2 \preccurlyeq \mathrm{E}_2 \wedge \Sigma_2 \tag{B.241}$$

for all environments E_1 and E_2 compatible with $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Our goal is to show that Σ_1 and Σ_2 are such that

$$\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2) \preccurlyeq \mathrm{A} \wedge (\Sigma_1 \to \Sigma_2). \tag{B.242}$$

To this end, we will first show that $\hat{\mathrm{A}} \preccurlyeq \mathrm{A}_1$. Note that (5.126) and (5.127) hold because $\mathcal{C}$ satisfies Implication 5.1. Let $\mathcal{S} \subset \mathcal{X}_a \times \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_{a_1} \times \mathcal{X}_{a_2}$ be a full simulation relation of $\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2)$ by $\mathrm{A}_1 \to \mathrm{A}_2$, and let

$$\mathcal{S}_1 = \pi_{\mathcal{X}_a \times \mathcal{X}_{a_1}}(\mathcal{S}). \tag{B.243}$$

We claim that $\mathcal{S}_1$ is a full simulation relation of $\hat{\mathrm{A}}$ by A_1. Note that the consistent subspace of $\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2)$ is $\mathcal{V}_a \times \mathcal{X}_1 \times \mathcal{X}_2$, hence

$$\pi_{\mathcal{X}_a}(\mathcal{S}_1) = \pi_{\mathcal{X}_a}(\mathcal{S}) = \mathcal{V}_a \tag{B.244}$$

because $\mathcal{S}$ is a full simulation relation. Let $(x_a, x_{a_1}) \in \mathcal{S}_1$ and $d_a \in \mathcal{D}_a$ be such that $A_a x_a + G_a d_a \in \mathcal{V}_a$. By definition of $\mathcal{S}_1$, there exist $x_1 \in \mathcal{X}_1$, $x_2 \in \mathcal{X}_2$ and $x_{a_2} \in \mathcal{X}_{a_2}$ such that $(x_a, x_1, x_2, x_{a_1}, x_{a_2}) \in \mathcal{S}$. Recall the dynamics of the interconnections $\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2)$ and $\mathrm{A}_1 \to \mathrm{A}_2$ from (5.124) and (5.125). Due to Proposition 5.2, since $\mathcal{S}$ is a simulation relation and

$$(A_a x_a + G_a d_a, A_1 x_1 + B_1 C_a x_a, A_2 x_2 + B_2 C_2 x_2) \in \mathcal{V}_a \times \mathcal{X}_1 \times \mathcal{X}_2, \tag{B.245}$$

there exist $d_{a_1} \in \mathcal{D}_{a_1}$ and $d_{a_2} \in \mathcal{D}_{a_2}$ such that

$$\begin{bmatrix} A_a x_a + G_a d_a \\ A_1 x_1 + B_1 C_a x_a \\ A_2 x_2 + B_2 C_2 x_2 \\ A_{a_1} x_{a_1} + G_{a_1} d_{a_1} \\ A_{a_2} x_{a_2} + G_{a_2} d_{a_2} \end{bmatrix} \in \mathcal{S}. \tag{B.246}$$

Furthermore, we have that

$$C_a x_a = C_{a_1} x_{a_1}, \quad H_a x_a = 0, \quad 0 = H_{a_1} x_{a_1}. \tag{B.247}$$

In particular, (B.246) implies that $(A_a x_a + G_a d_a, A_{a_1} x_{a_1} + G_{a_1} d_{a_1}) \in \mathcal{S}_1$, which, together with (B.244), (B.247) and Proposition 5.2, shows that $\mathcal{S}_1$ is a full simulation relation of $\hat{\mathrm{A}}$ by A_1, that is, $\hat{\mathrm{A}} \preccurlyeq \mathrm{A}_1$, as desired.

Next, we will show that $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1 \preccurlyeq \mathrm{A}_2$. Since $\hat{\mathrm{A}} \preccurlyeq \mathrm{A}_1$, it follows that $\hat{\mathrm{A}}$ is an environment compatible with $\mathcal{C}_1$, and, thus, (B.241) yields

$$\hat{\mathrm{A}} \wedge \Gamma_1 \preccurlyeq \hat{\mathrm{A}} \wedge \Sigma_1. \tag{B.248}$$

Recall that $\hat{\Gamma}_1$ is obtained from Γ_1 by relabelling the output y_1 to u_2. Let $\hat{\Sigma}_1$ be obtained from Σ_1 in the same way. As it is simply a matter of relabelling, $\hat{\mathrm{A}} \wedge \Gamma_1 \preccurlyeq \hat{\mathrm{A}} \wedge \Sigma_1$ is equivalent to

$$\hat{\mathrm{A}} \wedge \hat{\Gamma}_1 \preccurlyeq \hat{\mathrm{A}} \wedge \hat{\Sigma}_1. \tag{B.249}$$

Therefore, by transitivity of simulation, it is enough to show that

$$\hat{\mathrm{A}} \wedge \hat{\Sigma}_1 \preccurlyeq \mathrm{A}_2. \tag{B.250}$$

in order to conclude that $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1 \preccurlyeq \mathrm{A}_2$. With this in mind, consider the subspace

$$\mathcal{S}_2 = \pi_{\mathcal{X}_a \times \mathcal{X}_1 \times \mathcal{X}_{a_2}}(\mathcal{S}). \tag{B.251}$$

We will show that $\mathcal{S}_2$ is a full simulation relation of $\hat{\mathrm{A}} \wedge \hat{\Sigma}_1$ by A_2. Here, simulation is with respect to shared output u_2, see Remark 5.5. Note that

$$\pi_{\mathcal{X}_a \times \mathcal{X}_1}(\mathcal{S}_2) = \pi_{\mathcal{X}_a \times \mathcal{X}_1}(\mathcal{S}) = \mathcal{V}_a \times \mathcal{X}_1. \tag{B.252}$$

because the consistent subspace of $\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2)$ is $\mathcal{V}_a \times \mathcal{X}_1 \times \mathcal{X}_2$ and $\mathcal{S}$ is a full simulation relation. Next, let $(x_a, x_1, x_{a_2}) \in \mathcal{S}_2$, $d_a \in \mathcal{D}_a$ and $d_1 \in \mathcal{D}_1$ be such that

$$(A_a x_a + G_a d_a, A_1 x_1 + B_1 C_a x_a + G_1 d_1) \in \mathcal{V}_a \times \mathcal{X}_1 \tag{B.253}$$

By definition of $\mathcal{S}_2$, there exist $x_2 \in \mathcal{X}_2$ and $x_{a_1} \in \mathcal{X}_{a_1}$ such that

$$(x_a, x_1, x_2, x_{a_1}, x_{a_2}) \in \mathcal{S}. \tag{B.254}$$

Recall the dynamics of $\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2)$ and $\mathrm{A}_1 \to \mathrm{A}_2$ from (5.124) and (5.125). Due to Proposition 5.2, since $\mathcal{S}$ is a full simulation relation and

$$(A_a x_a + G_a d_a, A_1 x_1 + B_1 C_a x_a + G_1 d_1, A_2 x_2 + B_2 C_2 x_2) \in \mathcal{V}_a \times \mathcal{X}_1 \times \mathcal{X}_2, \tag{B.255}$$

there exist $d_{a_1} \in \mathcal{D}_{a_1}$ and $d_{a_2} \in \mathcal{D}_{a_2}$ such that

$$\begin{bmatrix} A_a x_a + G_a d_a \\ A_1 x_1 + B_1 C_a x_a + G_1 d_1 \\ A_2 x_2 + B_2 C_2 x_2 \\ A_{a_1} x_{a_1} + G_{a_1} d_{a_1} \\ A_{a_2} x_{a_2} + G_{a_2} d_{a_2} \end{bmatrix} \in \mathcal{S}. \tag{B.256}$$

Furthermore, we have that

$$C_1 x_1 = C_{a_2} x_{a_2}, \quad H_a x_a = 0, \quad 0 = H_{a_2} x_{a_2}. \tag{B.257}$$

Consequently, (B.256) implies that

$$\begin{bmatrix} A_a x_a + G_a d_a \\ A_1 x_1 + B_1 C_a x_a + G_1 d_1 \\ A_{a_2} x_{a_2} + G_{a_2} d_{a_2} \end{bmatrix} \in \mathcal{S}_2, \tag{B.258}$$

which, together with (B.252), (B.257) and Proposition 5.2, shows that $\mathcal{S}_2$ is indeed a full simulation relation of $\hat{\mathrm{A}} \wedge \hat{\Sigma}_1$ by A_2, that is, $\hat{\mathrm{A}} \wedge \hat{\Sigma}_1 \preccurlyeq \mathrm{A}_2$. In view of (B.249), it follows that $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1 \preccurlyeq \mathrm{A}_2$, as desired.

We are now ready to show that (B.242) holds. Since $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1 \preccurlyeq \mathrm{A}_2$, it follows that $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1$ is an environment compatible with $\mathcal{C}_2$ that has an extra output u_1. In view of Remark 5.17, we still have that (B.241) yields

$$(\hat{\mathrm{A}} \wedge \hat{\Gamma}_1) \wedge \Gamma_2 \preccurlyeq (\hat{\mathrm{A}} \wedge \hat{\Gamma}_1) \wedge \Sigma_2. \tag{B.259}$$

Since $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1 \preccurlyeq \hat{\mathrm{A}} \wedge \hat{\Sigma}_1$, Lemma 5.5 implies that

$$(\hat{\mathrm{A}} \wedge \hat{\Gamma}_1) \wedge \Sigma_2 \preccurlyeq (\hat{\mathrm{A}} \wedge \hat{\Sigma}_1) \wedge \Sigma_2, \tag{B.260}$$

see Remark 5.11. Together with (B.259), the latter implies that

$$(\hat{\mathrm{A}} \wedge \hat{\Gamma}_1) \wedge \Gamma_2 \preccurlyeq (\hat{\mathrm{A}} \wedge \hat{\Sigma}_1) \wedge \Sigma_2 \tag{B.261}$$

because simulation is transitive. Recall the dynamics of $\Gamma_1 \to \Gamma_2$ given by (5.128) and note that

$$(\hat{\mathrm{A}} \wedge \hat{\Gamma}_1) \wedge \Gamma_2 : \begin{cases} \begin{bmatrix} \dot{x}_a \\ \dot{x}_{g_1} \\ \dot{x}_{g_2} \end{bmatrix} = \begin{bmatrix} A_a & 0 & 0 \\ 0 & A_{g_1} & 0 \\ 0 & 0 & A_{g_2} \end{bmatrix} \begin{bmatrix} x_a \\ x_{g_1} \\ x_{g_2} \end{bmatrix} + \begin{bmatrix} G_a & 0 & 0 \\ 0 & G_{g_1} & 0 \\ 0 & 0 & G_{g_2} \end{bmatrix} \begin{bmatrix} d_a \\ d_{g_1} \\ d_{g_2} \end{bmatrix}, \\ u_1 = \begin{bmatrix} C_a & 0 & 0 \end{bmatrix} \begin{bmatrix} x_a \\ x_{g_1} \\ x_{g_2} \end{bmatrix} \\ \begin{bmatrix} u_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} 0 & C^y_{g_1} & 0 \\ 0 & 0 & C^y_{g_2} \end{bmatrix} \begin{bmatrix} x_a \\ x_{g_1} \\ x_{g_2} \end{bmatrix}, \\ 0 = \begin{bmatrix} H_a & 0 & 0 \\ 0 & H_{g_1} & 0 \\ 0 & 0 & H_{g_2} \\ C_a & -C^u_{g_1} & 0 \\ 0 & C^y_{g_1} & C^u_{g_2} \end{bmatrix} \begin{bmatrix} x_a \\ x_{g_1} \\ x_{g_2} \end{bmatrix}. \end{cases} \tag{B.262}$$

It is easily seen that $\mathrm{A}\wedge(\Gamma_1 \to \Gamma_2)$ is obtained from $(\hat{\mathrm{A}}\wedge\hat{\Gamma}_1)\wedge\Gamma_2$ by relabelling u_1 and u and u_2 to y_1. Since $\mathrm{A}\wedge(\Sigma_1 \to \Sigma_2)$ is obtained from $(\hat{\mathrm{A}}\wedge\hat{\Sigma}_1)\wedge\Sigma_2$ in the same way, (B.261) implies that (B.242) holds. Finally, (B.242) and (5.127) yield (5.131) by transitivity, which concludes the proof since we already showed that (5.129) and (5.130) hold.

We proceed by proving sufficiency. Suppose that (5.129), (5.130) and (5.131) hold. We will first show that

$$\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2) \preccurlyeq \mathrm{A}_1 \to \mathrm{A}_2. \tag{B.263}$$

Let $\mathcal{S}_1$ be a full simulation relation of $\hat{\mathrm{A}}$ by A_1, let $\mathcal{S}_2$ be a full simulation relation of $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1$ by A_2, and let $\mathcal{V}_{ag}$ be the consistent subspace of $\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2)$. We will show that the subspace $\mathcal{S} \subset \mathcal{X}_a \times \mathcal{X}_{g_1} \times \mathcal{X}_{g_2} \times \mathcal{X}_{a_1} \times \mathcal{X}_{a_2}$ given by

$$\mathcal{S} = \left\{ \begin{bmatrix} x_a \\ x_{g_1} \\ x_{g_2} \\ x_{a_1} \\ x_{a_2} \end{bmatrix} \;\middle|\; \begin{bmatrix} x_a \\ x_{g_1} \\ x_{g_2} \end{bmatrix} \in \mathcal{V}_{ag},\ \begin{bmatrix} x_a \\ x_{a_1} \end{bmatrix} \in \mathcal{S}_1,\ \begin{bmatrix} x_a \\ x_{g_1} \\ x_{a_2} \end{bmatrix} \in \mathcal{S}_2 \right\} \tag{B.264}$$

is a full simulation relation of $\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2)$ by $\mathrm{A}_1 \to \mathrm{A}_2$. First, recall that $(\hat{\mathrm{A}} \wedge \hat{\Gamma}_1) \wedge \Gamma_2$ is obtained from $\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2)$ by relabelling u to u_1 and y_1 to u_2, hence $\mathcal{V}_{ag}$ is also the consistent subspace of $(\hat{\mathrm{A}} \wedge \hat{\Gamma}_1) \wedge \Gamma_2$. Since $\mathcal{C}_2$ is consistent, we have that $\mathrm{A}_2 \preccurlyeq \Gamma_2$, which implies that $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1 \preccurlyeq \Gamma_2$ due to (5.130) and transitivity. Therefore, due to Remark 5.6, $\mathcal{V}_{ag}$ is the largest simulation relation of $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1$ by Γ_2, and, thus,

$$\mathcal{V}_{ag_1} = \pi_{\mathcal{X}_a \times \mathcal{X}_{g_1}}(\mathcal{V}_{ag}) \tag{B.265}$$

is the consistent subspace of $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1$. With this in mind, we claim that

$$\pi_{\mathcal{X}_a \times \mathcal{X}_{g_1} \times \mathcal{X}_{g_2}}(\mathcal{S}) = \mathcal{V}_{ag}. \tag{B.266}$$

To see this, first note that $\pi_{\mathcal{X}_a \times \mathcal{X}_{g_1} \times \mathcal{X}_{g_2}}(\mathcal{S}) \subset \mathcal{V}_{ag}$ by definition of $\mathcal{S}$. To show the converse, let $(x_a, x_{g_1}, x_{g_2}) \in \mathcal{V}_{ag}$. Then, (B.265) yields $(x_a, x_{g_1}) \in \mathcal{V}_{ag_1}$, hence there exists $x_{a_2} \in \mathcal{X}_{a_2}$ such that $(x_a, x_{g_1}, x_{a_2}) \in \mathcal{S}_2$ because $\mathcal{S}_2$ is a full simulation relation. Furthermore, since $\mathcal{V}_{ag_1} \subset \mathcal{V}_a \times \mathcal{V}_{g_1}$, we have that $x_a \in \mathcal{V}_a$ and, thus, there exists $x_{a_1} \in \mathcal{X}_{a_1}$ such that $(x_a, x_{a_1}) \in \mathcal{S}_1$ because $\mathcal{S}_1$ is a full simulation relation. This implies that $(x_a, x_{g_1}, x_{g_2}, x_{a_1}, x_{a_2}) \in \mathcal{S}$, which shows that (B.266) holds.

Now, let $(x_a, x_{g_1}, x_{g_2}, x_{a_1}, x_{a_2}) \in \mathcal{S}$, $d_a \in \mathcal{D}_a$, $d_{g_1} \in \mathcal{D}_{g_1}$ and $d_{g_2} \in \mathcal{D}_{g_2}$ be such that

$$(A_a x_a + G_a d_a, A_{g_1} x_{g_1} + G_{a_1} d_{a_1}, A_{g_2} x_{g_2} + G_{g_2} d_{g_2}) \in \mathcal{V}_{ag}. \tag{B.267}$$

By definition of $\mathcal{S}$, we have that $(x_a, x_{g_1}, x_{g_2}) \in \mathcal{V}_{ag}$, hence

$$\begin{aligned} &C_a x_a = C^u_{g_1} x_{g_1}, \qquad && C^y_{g_1} x_{g_1} = C^u_{g_2} x_{g_2}, \\ &H_a x_a = 0, && H_{g_1} x_{g_1} = 0, \qquad && H_{g_2} x_{g_2} = 0. \end{aligned} \tag{B.268}$$

We also have that $(x_a, x_{g_1}, x_{a_2}) \in \mathcal{S}_2$, hence

$$\begin{aligned} &C_a x_a = C^u_{g_1} x_{g_1}, \qquad && C^y_{g_1} x_{g_1} = C_{a_2} x_{a_2}, \\ &H_a x_a = 0, && H_{g_1} x_{g_1} = 0, \qquad && 0 = H_{a_2} x_{a_2}. \end{aligned} \tag{B.269}$$

Furthermore, (B.265) and (B.267) yield

$$(A_a x_a + G_a d_a, A_{g_1} x_{g_1} + G_{a_1} d_{a_1}) \in \mathcal{V}_{ag_1}, \tag{B.270}$$

which, due to Proposition 5.2, implies that there exist $d_{a_2} \in \mathcal{D}_{a_2}$ such that

$$(A_a x_a + G_a d_a, A_{g_1} x_{g_1} + G_{g_1} d_{g_1}, A_{a_2} x_{a_2} + G_{a_2} d_{a_2}) \in \mathcal{S}_2. \tag{B.271}$$

On the other hand, we also have that $(x_a, x_{a_1}) \in \mathcal{S}_1$, hence

$$C_a x_a = C_{a_1} x_{a_1}, \quad H_a x_a = 0, \quad 0 = H_{a_1} x_{a_1}. \tag{B.272}$$

Furthermore, (B.265) yields $A_a x_a + G_a d_a \in \mathcal{V}_a$, which, due to Proposition 5.2, implies that there exist $d_{a_1} \in \mathcal{D}_{a_1}$ such that

$$(A_a x_a + G_a d_a, A_{a_1} x_{a_1} + G_{a_1} d_{a_1}) \in \mathcal{S}_1. \tag{B.273}$$

Now, (B.267), (B.271) and (B.273) imply that

$$\begin{bmatrix} A_a x_a + G_a d_a \\ A_{g_1} x_{g_1} + G_{g_1} d_{g_1} \\ A_{g_2} x_{g_2} + G_{g_2} d_{g_2} \\ A_{a_1} x_{a_1} + G_{a_1} d_{a_1} \\ A_{a_2} x_{a_2} + G_{a_2} d_{a_2} \end{bmatrix} \in \mathcal{S}, \tag{B.274}$$

which, due to Proposition 5.2 and the equalities between (B.267) and (B.273), shows that $\mathcal{S}$ is a simulation relation of $\mathrm{A} \wedge (\Gamma_1 \to \Gamma_2)$ by $\mathrm{A}_1 \to \mathrm{A}_2$. Furthermore, since (B.266) holds, $\mathcal{S}$ is a full simulation relation and, thus, (B.263) holds.

We finally turn to showing that $\mathcal{C}$ satisfies Implication 5.1. Let Σ_1 and Σ_2 be implementations of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. We will first show that

$$\mathrm{A} \wedge (\Sigma_1 \to \Sigma_2) \preccurlyeq \mathrm{A} \wedge (\Gamma_1 \to \Gamma_2). \tag{B.275}$$

Then, the proof will follow from (B.263), (5.131) and the fact that simulation is transitive. With this in mind, (5.129) implies that $\hat{\mathrm{A}}$ is compatible with $\mathcal{C}_1$,

hence $\hat{\mathrm{A}} \wedge \Sigma_1 \preccurlyeq \Gamma_1$ and, thus, $\hat{\mathrm{A}} \wedge \Sigma_1 \preccurlyeq \hat{\mathrm{A}} \wedge \Gamma_1$ due to Remark 5.9. By relabelling y_1 to u_2, we obtain $\hat{\mathrm{A}} \wedge \hat{\Sigma}_1 \preccurlyeq \hat{\mathrm{A}} \wedge \hat{\Gamma}_1$, hence $\hat{\mathrm{A}} \wedge \hat{\Sigma}_1 \preccurlyeq \mathrm{A}_2$ by transitivity and (5.130). Consequently, $\hat{\mathrm{A}} \wedge \hat{\Sigma}_1$ is an environment compatible with $\mathcal{C}_2$, which, due to Remark 5.9, implies that

$$(\hat{\mathrm{A}} \wedge \hat{\Sigma}_1) \wedge \Sigma_2 \preccurlyeq (\hat{\mathrm{A}} \wedge \hat{\Sigma}_1) \wedge \Gamma_2. \tag{B.276}$$

At the same time, due to Proposition 5.4 and Remark 5.7, we have that

$$(\hat{\mathrm{A}} \wedge \hat{\Sigma}_1) \wedge \Gamma_2 \preccurlyeq (\hat{\mathrm{A}} \wedge \hat{\Gamma}_1) \wedge \Gamma_2 \tag{B.277}$$

and, thus,

$$(\hat{\mathrm{A}} \wedge \hat{\Sigma}_1) \wedge \Sigma_2 \preccurlyeq (\hat{\mathrm{A}} \wedge \hat{\Gamma}_1) \wedge \Gamma_2 \tag{B.278}$$

by transitivity. Finally, by relabelling u_1 to u and u_2 to y_1, we obtain (B.275), which, together with (B.263) and (5.131), implies that (5.126) and (5.127) hold because simulation is transitive. This shows that $\mathcal{C}$ satisfies Implication 5.1. □

B.15 Proof of Lemma 5.11

Suppose that the contracts $\mathcal{C}_1 = (\mathrm{A}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathrm{A}_2, \Gamma_2)$ are consistent, and consider the contract $\mathcal{C} = (\mathrm{A}, \Gamma)$. Let $\hat{\Gamma}_1$ be obtained from Γ_1 by relabelling y_1 to u_2, and let $\hat{\mathrm{A}}$ be obtained from A by relabelling u to u_1. Then, A is such that

$$\hat{\mathrm{A}} \preccurlyeq \mathrm{A}_1 \quad \text{and} \quad \hat{\mathrm{A}} \wedge \hat{\Gamma}_1 \preccurlyeq \mathrm{A}_2 \tag{5.132}$$

if and only if

$$\hat{\mathrm{A}} \preccurlyeq \mathrm{A}_1 \wedge \hat{\Gamma}_1 \wedge \mathrm{A}_2 \quad \text{and} \quad \hat{\Gamma}_1^0 \preccurlyeq \mathrm{A}_2, \tag{5.133}$$

where $\hat{\Gamma}_1^0$ is obtained from $\hat{\Gamma}_1$ by setting $u_1 = 0$.

Proof. We begin by proving necessity. Suppose that (5.132) holds. Since $\mathcal{C}_1$ is consistent, due to Remark 5.13, it follows that $\mathrm{A}_1 \preccurlyeq \Gamma_1$. Since simulation is transitive, we obtain $\hat{\mathrm{A}} \preccurlyeq \Gamma_1$ and, thus, $\hat{\mathrm{A}} \preccurlyeq \hat{\Gamma}_1$ after relabelling y_1 to u_2. Therefore, due to Remark 5.6, the consistent subspace $\mathcal{V}_{ag_1}$ of $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1$ is the largest simulation relation of $\hat{\mathrm{A}}$ by $\hat{\Gamma}_1$. In particular, this implies that

$$\begin{bmatrix} \operatorname{im} G_a \cap \mathcal{V}_a \\ 0 \end{bmatrix} \subset \mathcal{V}_{ag_1} + \operatorname{im} \begin{bmatrix} 0 \\ G_{g_1} \end{bmatrix} \quad \text{and} \quad \pi_{\mathcal{X}_a}(\mathcal{V}_{ag_1}) = \mathcal{V}_a, \tag{B.279}$$

where $\mathcal{V}_a$ is the consistent subspace of A. Let $\mathcal{S}$ be a full simulation relation of $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1$ by A_2. Therefore, due to Proposition 5.1, we have that

$$\begin{bmatrix} A_a & 0 & 0 \\ 0 & A_{g_1} & 0 \\ 0 & 0 & A_{a_2} \end{bmatrix} \mathcal{S} \subset \mathcal{S} + \operatorname{im} \begin{bmatrix} G_a & 0 & 0 \\ 0 & G_{g_1} & 0 \\ 0 & 0 & G_{a_2} \end{bmatrix}, \tag{B.280}$$

$$\begin{bmatrix} \operatorname{im} \begin{bmatrix} G_a & 0 \\ 0 & G_{g_1} \\ & 0 \end{bmatrix} \cap \mathcal{V}_{ag_1} \end{bmatrix} \subset \mathcal{S} + \operatorname{im} \begin{bmatrix} 0 \\ 0 \\ G_{a_2} \end{bmatrix}, \tag{B.281}$$

$$\mathcal{S} \subset \begin{bmatrix} 0 & C^y_{g_2} & -C_{a_2} \\ H_a & 0 & 0 \\ 0 & H_{g_1} & 0 \\ C_a & -C^u_{g_1} & 0 \\ 0 & 0 & H_{a_2} \end{bmatrix}. \tag{B.282}$$

Due to (B.279), (B.281) implies that

$$\begin{bmatrix} \operatorname{im} G_a \cap \mathcal{V}_a \\ 0 \\ 0 \end{bmatrix} \subset \mathcal{S} + \operatorname{im} \begin{bmatrix} 0 & 0 \\ G_{g_1} & 0 \\ 0 & G_{a_2} \end{bmatrix}, \tag{B.283}$$

which, together with (B.280), (B.282) and Proposition 5.1, implies that $\mathcal{S}$ is a simulation relation of $\hat{\mathrm{A}}$ by $\hat{\Gamma}_1 \wedge \mathrm{A}_2$. Furthermore, we have that

$$\pi_{\mathcal{X}_a}(\mathcal{S}) = \pi_{\mathcal{X}_a}\left(\pi_{\mathcal{X}_a \times \mathcal{X}_{g_1}}(\mathcal{S})\right) = \pi_{\mathcal{X}_a}(\mathcal{V}_{ag_1}) = \mathcal{V}_a, \tag{B.284}$$

hence $\mathcal{S}$ is a full simulation relation and, thus, $\hat{\mathrm{A}} \preccurlyeq \hat{\Gamma}_1 \wedge \mathrm{A}_2$. Since we also have that $\hat{\mathrm{A}} \preccurlyeq \mathrm{A}_1$, Proposition 5.4 yields

$$\hat{\mathrm{A}} \preccurlyeq \mathrm{A}_1 \wedge (\hat{\Gamma}_1 \wedge \mathrm{A}_2), \tag{B.285}$$

where we used the fact that $\hat{\mathrm{A}} \sim \hat{\mathrm{A}} \wedge \hat{\mathrm{A}}$.

On the other hand, we can show that the subspace $\mathcal{S}^0 \subset \mathcal{X}_{g_1} \times \mathcal{X}_{a_2}$ given by

$$\mathcal{S}^0 = \{(x_{g_1}, x_{a_2}) \mid (0, x_{g_1}, x_{a_2}) \in \mathcal{S}\} \tag{B.286}$$

is a full simulation relation of $\hat{\Gamma}^0_1$ by A_2. To see this, first note that (B.280), (B.282) and (B.283) yield

$$\begin{bmatrix} A_{g_1} & 0 \\ 0 & A_{a_2} \end{bmatrix} \mathcal{S}^0 \subset \mathcal{S}^0 + \operatorname{im} \begin{bmatrix} G_{g_1} & 0 \\ 0 & G_{a_2} \end{bmatrix}, \tag{B.287}$$

$$\begin{bmatrix} \operatorname{im} G_{g_1} \cap \mathcal{V}^0_{ag_1} \\ 0 \end{bmatrix} \subset \mathcal{S}^0 + \operatorname{im} \begin{bmatrix} 0 \\ G_{a_2} \end{bmatrix}, \tag{B.288}$$

$$\mathcal{S}^0 \subset \begin{bmatrix} C^y_{g_2} & -C_{a_2} \\ H_{g_1} & 0 \\ -C^u_{g_1} & 0 \\ 0 & H_{a_2} \end{bmatrix}, \tag{B.289}$$

where the subspace $\mathcal{V}^0_{ag_1} \subset \mathcal{X}_{g_1}$ is given by

$$\mathcal{V}^0_{ag_1} = \{ x_{g_1} \mid (0, x_{g_1}) \in \mathcal{V}_{ag_1} \}. \tag{B.290}$$

Therefore, due to Proposition 5.1, $\mathcal{S}^0$ is a simulation relation of $\hat{\Gamma}^0_1$ by A_2 if

$$\mathcal{V}^0_{ag_1} = \mathcal{V}^0_{g_1}, \tag{B.291}$$

where $\mathcal{V}^0_{g_1}$ is the consistent subspace of $\hat{\Gamma}^0_1$. With this in mind, note that $\mathcal{V}_{ag_1}$ is the largest subspace such that

$$\begin{bmatrix} A_a & 0 \\ 0 & A_{g_1} \end{bmatrix} \mathcal{V}_{ag_1} \subset \mathcal{V}_{ag_1} + \operatorname{im} \begin{bmatrix} G_a & 0 \\ 0 & G_{g_1} \end{bmatrix}, \tag{B.292}$$

$$\mathcal{V}_{ag_1} \subset \ker \begin{bmatrix} H_a & 0 \\ 0 & H_{g_1} \\ C_a & -C^u_{g_1} \end{bmatrix}, \tag{B.293}$$

hence $\mathcal{V}^0_{ag_1}$ is such that

$$A_{g_1} \mathcal{V}^0_{ag_1} \subset \mathcal{V}^0_{ag_1} + \operatorname{im} G_{g_1} \quad \text{and} \quad \mathcal{V}^0_{ag_1} \subset \ker \begin{bmatrix} H_{g_1} \\ C^u_{g_1} \end{bmatrix}. \tag{B.294}$$

Since $\mathcal{V}^0_{g_1}$ is the *largest* subspace such that

$$A_{g_1} \mathcal{V}^0_{g_1} \subset \mathcal{V}^0_{g_1} + \operatorname{im} G_{g_1} \quad \text{and} \quad \mathcal{V}^0_{g_1} \subset \ker \begin{bmatrix} H_{g_1} \\ C^u_{g_1} \end{bmatrix}, \tag{B.295}$$

it follows that $\mathcal{V}^0_{ag_1} \subset \mathcal{V}^0_{g_1}$. Furthermore, we have that

$$\begin{bmatrix} A_a & 0 \\ 0 & A_{g_1} \end{bmatrix} \big(\{0\} \times \mathcal{V}^0_{g_1} \big) \subset \big(\{0\} \times \mathcal{V}^0_{g_1} \big) + \operatorname{im} \begin{bmatrix} G_a & 0 \\ 0 & G_{g_1} \end{bmatrix} \tag{B.296}$$

$$\{0\} \times \mathcal{V}^0_{g_1} \subset \ker \begin{bmatrix} H_a & 0 \\ 0 & H_{g_1} \\ C_a & -C^u_{g_1} \end{bmatrix}, \tag{B.297}$$

hence $\{0\} \times \mathcal{V}^0_{g_1} \subset \mathcal{V}_{ag_1}$ and, thus, $\mathcal{V}^0_{g_1} \subset \mathcal{V}^0_{ag_1}$. This shows that (B.291) holds and $\mathcal{S}^0$ is indeed a simulation relation of $\hat{\Gamma}^0_1$ by A_2. Furthermore, since

$$\pi_{\mathcal{X}_{g_1}}(\mathcal{S}_0) = \big\{ x_{g_1} \,\big|\, (0, x_{g_1}) \in \pi_{\mathcal{X}_a \times \mathcal{X}_{g_1}}(\mathcal{S}) \big\} \tag{B.298}$$

and $\mathcal{S}$ is a full simulation relation of $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1$ by A_2, it follows that

$$\pi_{\mathcal{X}_{g_1}}(\mathcal{S}_0) = \{ x_{g_1} \mid (0, x_{g_1}) \in \mathcal{V}_{ag_1} \} = \mathcal{V}^0_{ag_1} = \mathcal{V}^0_{g_1}, \tag{B.299}$$

hence $\mathcal{S}^0$ is a full simulation relation of $\hat{\Gamma}^0_1$ by A_2. This implies that $\hat{\Gamma}^0_1 \preccurlyeq \mathrm{A}_2$ and, thus, (5.133) holds.

We proceed by proving necessity. Suppose that (5.133) holds. Due to Proposition 5.4, it follows that $\hat{\mathrm{A}} \preccurlyeq \mathrm{A}_1$ and $\hat{\mathrm{A}} \preccurlyeq \hat{\Gamma}_1 \wedge \mathrm{A}_2$. Therefore, we only need to show that $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1 \preccurlyeq \mathrm{A}_2$. To this end, let $\mathcal{S}'$ be a full simulation relation of $\hat{\mathrm{A}}$ by $\hat{\Gamma}_1 \wedge \mathrm{A}_2$. In particular, this means that $\mathcal{S}'$ satisfies (B.280), (B.282) and (B.283) with $\mathcal{S}$ replaced by $\mathcal{S}'$. On the other hand, let $\mathcal{S}^0$ be a full simulation relation of $\hat{\Gamma}_1^0$ by A_2. This means that $\mathcal{S}^0$ satisfies (B.287), (B.289) and

$$\begin{bmatrix} \operatorname{im} G_{g_1} \cap \mathcal{V}_{g_1}^0 \\ 0 \end{bmatrix} \subset \mathcal{S}^0 + \operatorname{im} \begin{bmatrix} 0 \\ G_{a_2} \end{bmatrix}. \tag{B.300}$$

It is easily seen that $\{0\} \times \mathcal{S}^0$ satisfies (B.280) and (B.282) with $\mathcal{S}$ replaced by $\{0\} \times \mathcal{S}^0$, hence the subspace

$$\mathcal{S} = \mathcal{S}' + (\{0\} \times \mathcal{S}^0) \tag{B.301}$$

also satisfies (B.280) and (B.282). Note that $\mathcal{S}$ would be a simulation relation of $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1$ by A_2 if (B.281) holds.

To show this, let $d_a \in \mathcal{D}_a$ and $d_{g_1} \in \mathcal{D}_{g_1}$ be such that $(G_a d_a, G_{g_1} d_{g_1}) \in \mathcal{V}_{ag_1}$. Since $\mathcal{V}_{ag_1} \subset \mathcal{V}_a \times \mathcal{V}_{g_1}$, where $\mathcal{V}_{g_1}$ is the consistent subspace of $\hat{\Gamma}_1$, it follows that $G_a d_a \in \mathcal{V}_a$. Therefore, as $\mathcal{S}'$ satisfies (B.283) with $\mathcal{S}$ replaced by $\mathcal{S}'$, there exist $d'_{g_1} \in \mathcal{D}_{g_1}$ and $d'_{a_2} \in \mathcal{D}_{a_2}$ such that

$$(G_a d_a, G_{g_1} d'_{g_1}, G_{a_2} d'_{a_2}) \in \mathcal{S}' \subset \mathcal{S}. \tag{B.302}$$

As explained in Remark 5.1, since $\mathcal{S}$ satisfies (B.280) and (B.282), it follows that $\pi_{\mathcal{X}_a \times \mathcal{X}_{g_1}}(\mathcal{S}) \subset \mathcal{V}_{ag_1}$, hence $(G_a d_a, G_{g_1} d'_{g_1}) \in \mathcal{V}_{ag_1}$ and, thus,

$$(0, G_{g_1}(d_{g_1} - d'_{g_1})) \in \mathcal{V}_{ag_1} \tag{B.303}$$

by linearity. Recall that the subspace $\mathcal{V}_{ag_1}^0$ in (B.290) is such that $\mathcal{V}_{ag_1}^0 \subset \mathcal{V}_{g_1}^0$. This implies that $G_{g_1}(d_{g_1} - d'_{g_1}) \in \mathcal{V}_{g_1}^0$, hence, due to (B.300), there exists $d''_{a_2} \in \mathcal{D}_{a_2}$ such that $(G_{g_1}(d_{g_1} - d'_{g_1}), G_{a_2} d''_{a_2}) \in \mathcal{S}_0$ and, thus,

$$(0, G_{g_1}(d_{g_1} - d'_{g_1}), G_{a_2} d''_{a_2}) \in \{0\} \times \mathcal{S}^0 \subset \mathcal{S}. \tag{B.304}$$

In view of (B.302), we obtain

$$(G_a d_a, G_{g_1} d_{g_1}, G_{a_2}(d'_{a_2} + d''_{a_2})) \in \mathcal{S}, \tag{B.305}$$

which implies that $\mathcal{S}$ satisfies (B.281). Together with (B.280) and (B.282), this shows that $\mathcal{S}$ is a simulation relation of $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1$ by A_2.

We can show that $\mathcal{V}_{ag1} \subset \pi_{\mathcal{X}_a \times \mathcal{X}_{g_1}}(\mathcal{S})$ using a similar argument. Namely, if $(x_a, x_{g_1}) \in \mathcal{V}_{ag_1}$, then $x_a \in \mathcal{V}_a$ and, thus, there exist $x'_{g_1} \in \mathcal{X}_{g_1}$ and $x'_{a_2} \in \mathcal{X}_{a_2}$ such that $(x_a, x'_{g_1}, x'_{a_2}) \in \mathcal{S}' \subset \mathcal{S}$. This yields $(0, x_{g_1} - x'_{g_1}) \in \mathcal{V}_{ag_1}$, which implies that $x_{g_1} - x'_{g_1} \in \mathcal{V}_{g_1}^0$. Therefore, there exists $x''_{a_2} \in \mathcal{X}_{a_2}$ such that $(x_{g_1} - x'_{g_1}, x''_{a_2}) \in \mathcal{S}^0$ and, thus, $(x_a, x_{g_1}, x'_{a_2} + x''_{a_2}) \in \mathcal{S}$. This shows that $\mathcal{V}_{ag_1} \subset$

$\pi_{\mathcal{X}_a \times \mathcal{X}_{g_1}}(\mathcal{S})$. We already have that $\pi_{\mathcal{X}_a \times \mathcal{X}_{g_1}}(\mathcal{S}) \subset \mathcal{V}_{ag_1}$ because $\mathcal{S}$ satisfies (B.280) and (B.282), see Remark 5.1. This shows that $\mathcal{S}$ is a *full* simulation relation of $\hat{\mathrm{A}} \wedge \hat{\Gamma}_1$ by A_2, and we conclude that (5.132) holds. □

Bibliography

[1] E. A. Lee, "Cyber physical systems: Design challenges," in *IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing*, pp. 363–369, 2008.

[2] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, "Cyber-physical systems: A new frontier," in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, pp. 1–9, 2008.

[3] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Design Automation Conference*, pp. 731–736, 2010.

[4] R. Poovendran, K. Sampigethaya, S. K. S. Gupta, I. Lee, K. V. Prasad, D. Corman, and J. L. Paunicka, "Special issue on cyber-physical systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 6–12, 2012.

[5] J. C. Willems, "Dissipative dynamical systems part I: General theory," *Archive for Rational Mechanics and Analysis*, vol. 45, no. 5, pp. 321–351, 1972.

[6] R. Sepulchre, M. Janković, and P. V. Kokotović, *Constructive Nonlinear Control*. Springer London, 1997.

[7] M. Arcak, C. Meissen, and A. Packard, *Networks of Dissipative Systems*. Springer International Publishing, 2016.

[8] A. J. van der Schaft, *L_2-Gain and Passivity Techniques in Nonlinear Control*. Springer International Publishing, 2017.

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

[10] P. Tabuada, *Verification and Control of Hybrid Systems: A Symbolic Approach*. Springer US, 2009.

[11] C. Belta, B. Yordanov, and E. A. Gol, *Formal Methods for Discrete-Time Dynamical Systems*, vol. 89 of *Studies in Systems, Decision and Control*. Springer-Verlag GmbH, 2017.

[12] J. Willems, "On interconnections, control, and feedback," *IEEE Transactions on Automatic Control*, vol. 42, no. 3, pp. 326–339, 1997.

[13] M. Belur and H. Trentelman, "Stabilization, pole placement, and regular implementability," *IEEE Transactions on Automatic Control*, vol. 47, no. 5, pp. 735–744, 2002.

[14] A. J. van der Schaft, "Achievable behavior of general systems," *Systems & Control Letters*, vol. 49, no. 2, pp. 141–149, 2003.

[15] A. A. Julius and A. J. van der Schaft, "Bisimulation as congruence in the behavioral setting," in *Proceedings of the IEEE Conference on Decision and Control*, pp. 814–819, 2005.

[16] A. A. Julius, J. W. Polderman, and A. van der Schaft, "Parametrization of the regular equivalences of the canonical controller," *IEEE Transactions on Automatic Control*, vol. 53, no. 4, pp. 1032–1036, 2008.

[17] P. Tabuada, "Controller synthesis for bisimulation equivalence," *Systems & Control Letters*, vol. 57, no. 6, pp. 443–452, 2008.

[18] H. Vinjamoor and A. J. van der Schaft, "Asymptotic achievability for linear time invariant state space systems," in *Proceedings of the IEEE Conference on Decision and Control*, 2010.

[19] H. Vinjamoor and A. J. van der Schaft, "The achievable dynamics via control by interconnection," *IEEE Transactions on Automatic Control*, vol. 56, no. 5, pp. 1110–1117, 2011.

[20] H. Vinjamoor and A. van der Schaft, "What can the canonical controller in principle tell us?," *Systems & Control Letters*, vol. 60, no. 8, pp. 644–649, 2011.

[21] N. Y. Megawati and A. van der Schaft, "Abstraction and control by interconnection of linear systems: A geometric approach," *Systems & Control Letters*, vol. 105, pp. 27–33, 2017.

[22] S. Wang and C. Desoer, "The exact model matching of linear multivariable systems," *IEEE Transactions on Automatic Control*, vol. 17, no. 3, pp. 347–349, 1972.

[23] B. Moore and L. Silverman, "Model matching by state feedback and dynamic compensation," *IEEE Transactions on Automatic Control*, vol. 17, no. 4, pp. 491–497, 1972.

[24] W. A. Wolovich, *Linear Multivariable Systems*. Springer New York, 1974.

[25] V. Kučera and E. C. Toledo, "A review of stable exact model matching by state feedback," in *Mediterranean Conference on Control and Automation*, pp. 85–90, 2014.

[26] A. Morse, "Structure and design of linear model following systems," *IEEE Transactions on Automatic Control*, vol. 18, no. 4, pp. 346–354, 1973.

[27] D. D. Šiljak, "Decentralized control of complex systems," in *Mathematics in Science and Engineering*, Academic Press, 1991.

[28] M. Rotkowitz and S. Lall, "A characterization of convex problems in decentralized control," *IEEE Transactions on Automatic Control*, vol. 51, no. 2, pp. 274–286, 2006.

[29] L. Bakule, "Decentralized control: An overview," *Annual Reviews in Control*, vol. 32, no. 1, pp. 87–98, 2008.

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

[31] B. Meyer, *Touch of Class: Learning to Program Well with Objects and Contracts*. Springer Berlin Heidelberg, 2009.

[32] C. A. R. Hoare, "An axiomatic basis for computer programming," *Communincations of the ACM*, vol. 12, p. 576–580, oct 1969.

[33] R. W. Floyd, "Assigning meanings to programs," in *Program Verification: Fundamental Issues in Computer Science* (T. R. Colburn, J. H. Fetzer, and T. L. Rankin, eds.), pp. 65–81, Springer Netherlands, 1993.

[34] C. Jones, "Specification and design of (parallel) programs.," in *Proceedings of IFIP Congress*, vol. 83, pp. 321–332, 1983.

[35] L. de Alfaro and T. A. Henzinger, "Interface automata," in *Proceedings of the joint 8th European Software Engineering Conference and 9th ACM SIGSOFT International Symposium on Foundations of Software Engineering*, pp. 109–120, ACM, 2001.

[36] L. de Alfaro and T. A. Henzinger, "Interface theories for component-based design," in *Embedded Software* (T. A. Henzinger and C. M. Kirsch, eds.), pp. 148–165, Springer Berlin Heidelberg, 2001.

[37] A. Chakrabarti, L. de Alfaro, T. A. Henzinger, and F. Y. C. Mang, "Synchronous and bidirectional component interfaces," in *Computer Aided Verification* (E. Brinksma and K. G. Larsen, eds.), pp. 414–427, Springer Berlin Heidelberg, 2002.

[38] L. de Alfaro and T. A. Henzinger, "Interface-based design," in *Engineering Theories of Software Intensive Systems* (M. Broy, J. Grünbauer, D. Harel, and T. Hoare, eds.), pp. 83–104, Springer Netherlands, 2005.

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

[40] A. Davare, D. Densmore, L. Guo, R. Passerone, A. L. Sangiovanni-Vincentelli, A. Simalatsar, and Q. Zhu, "metroII: A design environment for cyber-physical systems," *ACM Transactions on Embedded Computing Systems*, vol. 12, no. 1s, 2013.

[41] P. Nuzzo, H. Xu, N. Ozay, J. B. Finn, A. L. Sangiovanni-Vincentelli, R. M. Murray, A. Donzé, and S. A. Seshia, "A contract-based methodology for aircraft electric power system design," *IEEE Access*, vol. 2, pp. 1–25, 2014.

[42] P. Nuzzo and A. Sangiovanni-Vincentelli, "Let's get physical: Computer science meets systems," in *From Programs to Systems. The Systems Perspective in Computing*, pp. 193–208, Springer Berlin Heidelberg, 2014.

[43] P. Nuzzo, A. L. Sangiovanni-Vincentelli, D. Bresolin, L. Geretti, and T. Villa, "A platform-based design methodology with contracts and related tools for the design of cyber-physical systems," *Proceedings of the IEEE*, vol. 103, pp. 2104–2132, nov 2015.

[44] P. Nuzzo and A. L. Sangiovanni-Vincentelli, "Hierarchical system design with vertical contracts," in *Principles of Modeling: Essays Dedicated to Edward A. Lee on the Occasion of His 60th Birthday* (M. Lohstroh, P. Derler, and M. Sirjani, eds.), pp. 360–382, Springer, Cham, 2018.

[45] P. Nuzzo, M. Lora, Y. A. Feldman, and A. L. Sangiovanni-Vincentelli, "CHASE: Contract-based requirement engineering for cyber-physical system design," in *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 839–844, 2018.

[46] A. Benveniste, B. Caillaud, D. Nickovic, R. Passerone, J.-B. Raclet, P. Reinkemeier, A. Sangiovanni-Vincentelli, W. Damm, T. A. Henzinger, and K. G. Larsen, *Contracts for System Design*. Foundations and Trends in Electronic Design Automation, Now Publishers, 2018.

[47] E. S. Kim, M. Arcak, and S. A. Seshia, "A small gain theorem for parametric assume-guarantee contracts," in *Proceedings of the 20th International Conference on Hybrid Systems: Computation and Control*, pp. 207–216, 2017.

[48] M. Al Khatib and M. Zamani, "Controller synthesis for interconnected systems using parametric assume-guarantee contracts," in *Proceedings of the American Control Conference*, pp. 5419–5424, 2020.

[49] 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 Transactions on Control of Network Systems*, vol. 8, no. 1, pp. 487–499, 2021.

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

[51] A. Saoud, A. Girard, and L. Fribourg, "Contract based design of symbolic controllers for interconnected multiperiodic sampled-data systems," in *Proceedings of the IEEE Conference on Decision and Control*, pp. 773–779, 2018.

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

[53] D. Zonetti, A. Saoud, A. Girard, and L. Fribourg, "A symbolic approach to voltage stability and power sharing in time-varying DC microgrids," in *Proceedings of the European Control Conference*, pp. 903–909, 2019.

[54] I. D. Loreto, A. Borri, and M. D. Di Benedetto, "An assume-guarantee approach to sampled-data quantized glucose control," in *Proceedings of the IEEE Conference on Decision and Control*, pp. 3401–3406, 2020.

[55] A. Saoud, A. Girard, and L. Fribourg, "Assume-guarantee contracts for continuous-time systems," *Automatica*, vol. 134, p. 109910, 2021.

[56] M. Sharf, B. Besselink, A. Molin, Q. Zhao, and K. H. Johansson, "Assume/guarantee contracts for dynamical systems: Theory and computational tools," in *Proceedings of the 7th IFAC Conference on Analysis and Design of Hybrid Systems*, pp. 25–30, 2021.

[57] A. Eqtami and A. Girard, "A quantitative approach on assume-guarantee contracts for safety of interconnected systems," in *Proceedings of the European Control Conference*, pp. 536–541, 2019.

[58] B. Besselink, K. H. Johansson, and A. J. van der Schaft, "Contracts as specifications for dynamical systems in driving variable form," in *Proceedings of the European Control Conference*, pp. 263–268, 2019.

[59] K. Ghasemi, S. Sadraddini, and C. Belta, "Compositional synthesis via a convex parameterization of assume-guarantee contracts," in *Proceedings of the International Conference on Hybrid Systems: Computation and Control*, pp. 1–10, 2020.

[60] F. Kerber and A. van der Schaft, "Assume-guarantee reasoning for linear dynamical systems," in *Proceedings of the European Control Conference*, pp. 5015–5020, 2009.

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

[62] F. Kerber and A. J. van der Schaft, "Decentralized control using compositional analysis techniques," in *Proceedings of the IEEE Conference on Decision and Control and European Control Conference*, pp. 2699–2704, 2011.

[63] J. W. Polderman and J. C. Willems, *Introduction to Mathematical Systems Theory*. Springer-Verlag New York, 1998.

[64] G. J. Pappas, "Bisimilar linear systems," *Automatica*, vol. 39, p. 2035–2047, Dec. 2003.

[65] A. J. van der Schaft, "Equivalence of dynamical systems by bisimulation," *IEEE Transactions on Automatic Control*, vol. 49, no. 12, pp. 2160–2172, 2004.

[66] R. Milner, *Communication and Concurrency*. Prentice Hall International Series in Computer Science, Prentice Hall, 1995.

[67] G. Basile and G. Marro, *Controlled and Conditioned Invariants in Linear System Theory*. Prentice Hall, Englewood Cliffs, USA, 1992.

[68] H. L. Trentelman, A. A. Stoorvogel, and M. L. J. Hautus, *Control theory for linear systems*. London: Springer-Verlag, 2001.

[69] B. M. Shali, A. J. van der Schaft, and B. Besselink, "Behavioural contracts for linear dynamical systems: input assumptions and output guarantees," in *Proceedings of the European Control Conference*, pp. 564–569, 2021.

[70] B. M. Shali, A. J. van der Schaft, and B. Besselink, "Behavioural assume-guarantee contracts for linear dynamical systems," in *Proceedings of the IEEE Conference on Decision and Control*, pp. 2002–2007, 2021.

[71] J. C. Willems, "Models for dynamics," in *Dynamics Reported: A Series in Dynamical Systems and Their Applications* (U. Kirchgraber and H. O. Walther, eds.), pp. 171–269, Vieweg+Teubner Verlag, 1989.

[72] J. Willems, "Paradigms and puzzles in the theory of dynamical systems," *IEEE Transactions on Automatic Control*, vol. 36, no. 3, pp. 259–294, 1991.

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

[74] T. Kaczorek, *Polynomial and Rational Matrices*. Springer-Verlag London, 2007.

[75] T. Kailath, *Linear Systems*. Information and System Sciences Series, Prentice-Hall, 1980.

[76] J. G. Forney, "Minimal bases of rational vector spaces, with applications to multivariable linear systems," *SIAM Journal on Control*, vol. 13, pp. 493–520, 1975.

[77] J. C. Willems, "Input-output and state-space representations of finite-dimensional linear time-invariant systems," *Linear Algebra and its Applications*, vol. 50, pp. 581–608, 1983.

[78] J. W. Polderman, "A new and simple proof of the equivalence theorem for behaviors," *Systems & Control Letters*, vol. 41, no. 3, pp. 223–224, 2000.

[79] A. Julius, J. Willems, M. Belur, and H. Trentelman, "The canonical controllers and regular interconnection," *Systems & Control Letters*, vol. 54, no. 8, pp. 787–797, 2005.

[80] C. Praagman, H. L. Trentelman, and R. Z. Yoe, "On the parametrization of all regularly implementing and stabilizing controllers," *SIAM Journal on Control and Optimization*, vol. 45, no. 6, pp. 2035–2053, 2007.

[81] H. Trentelman and S. Fiaz, "On regular implementability using controllers with a priori input/output structure," in *Proceedings of the IEEE Conference on Decision and Control*, pp. 464–469, 2007.

[82] J. Wilkening and J. Yu, "A local construction of the Smith normal form of a matrix polynomial," *Journal of Symbolic Computation*, vol. 46, no. 1, pp. 1–22, 2011.

[83] B. M. Shali, A. van der Schaft, and B. Besselink, "Composition of behavioural assume-guarantee contracts," *IEEE Transactions on Automatic Control*, pp. 1–16, 2022.

[84] K. Zhou, J. C. Doyle, and K. Glover, *Robust and Optimal Control*. Prentice Hall, 1996.

[85] B. M. Shali, H. M. Heidema, A. J. van der Schaft, and B. Besselink, "Series composition of simulation-based assume-guarantee contracts for linear dynamical systems," in *Proceedings of the IEEE Conference on Decision and Control*, pp. 2204–2209, 2022.

[86] W. M. Wonham, *Linear Multivariable Control: A Geometric Approach*. Springer US, 1979.

[87] A. van der Schaft, "Equivalence of hybrid dynamical systems," in *Proceedings of the 16th International Symposium on Mathematical Theory of Networks and Systems, Leuven, Belgium*, 2004.

[88] N. Y. Megawati and A. van der Schaft, "Bisimulation equivalence of differential-algebraic systems," *International Journal of Control*, vol. 91, no. 1, pp. 45–56, 2016.

[89] A. Girard and G. Pappas, "Approximate bisimulations for constrained linear systems," in *Proceedings of the IEEE Conference on Decision and Control*, pp. 4700–4705, 2005.

[90] A. Girard and G. Pappas, "Approximate bisimulations for nonlinear dynamical systems," in *Proceedings of the IEEE Conference on Decision and Control*, pp. 684–689, 2005.

[91] A. Girard and G. J. Pappas, "Approximation metrics for discrete and continuous systems," *IEEE Transactions on Automatic Control*, vol. 52, no. 5, pp. 782–798, 2007.

[92] A. Girard and G. J. Pappas, "Approximate bisimulation: A bridge between computer science and control theory," *European Journal of Control*, vol. 17, no. 5, pp. 568–578, 2011.

[93] A. Pirastehzad, A. van der Schaft, and B. Besselink, "A notion of system comparison," *arXiv e-prints*, p. arXiv:2303.11015, 2023.

Summary

Modern engineering systems, such as intelligent transportation systems, smart grids, smart manufacturing systems, etc., often comprise a large number of interconnected components. The design requirements for the components of such systems are becoming increasingly complex. Consequently, the development of components usually requires specialized expertise and is, thus, handled by different (independent) teams. But independent teams seldom have the facilities to collaborate effectively, which can cause long and costly delays. This can be avoided by adopting a method for specifying design requirements that is inherently modular, i.e., that allows components to be considered independently. One such method is based on using so-called contracts, first introduced in the field of computer science. While contract theories have been developed for various system classes, these are generally restricted to systems with discrete variables evolving in discrete time.

Motivated by this, in this thesis, we develop a contract theory for a class of dynamical control systems with continuous variables in continuous time. In particular, we introduce assume-guarantee contracts for linear dynamical systems with inputs and outputs. These contracts are defined as a pair of linear systems called assumptions and guarantees, and they serve as specifications for components through two aspects. First, the assumptions capture the expected dynamics of the environment in which the component operates, thus leading to a class of compatible environments. Second, the guarantees capture the required dynamics of the component when interconnected with a compatible environment, thus leading to a class of implementations. Formally, the classes of compatible environments and implementations are obtained by system comparison with the assumptions and guarantees. In this thesis, we consider two methods for system comparison, namely, behavioural inclusion and simulation, and we develop a contract theory using each.

We begin by developing a contract theory using behavioural inclusion as a method for system comparison. In particular, we introduce notions of implementation, refinement, and conjunction, which allow us to express, compare, and combine specifications using contracts. We characterize these notions in terms of behavioural inclusions and provide algorithms for their verification. In the same vein, we consider the problem of designing an implementation

for a given contract. We provide algorithmically verifiable necessary and sufficient conditions under which an implementation exists, and we provide a systematic procedure for its construction when it exists. Subsequently, we introduce two notions of contract composition. Loosely speaking, the composition of two contracts is such that the interconnection of any of their implementations is guaranteed to implement their composition. Together with the notion of refinement, such a notion of composition enables the independent design of components within interconnected systems. With this in mind, we consider two notions of composition based on two types of system interconnections, namely, series and feedback. For each type, we provide algorithmically verifiable necessary and sufficient conditions under which the composition exists, and we provide an explicit expression for it when it exists.

Although the contract theory based on behavioural inclusion is supported by algorithms for verification, these are not necessarily efficient. To address this issue, we develop a contract theory based on simulation instead of behavioural inclusion as a method for system comparison. Simulation is supported by efficient algorithms for verification based on the (controlled) invariant subspace algorithm. Furthermore, its connection to geometric control theory allows us to use a multitude of tools and techniques in tackling problems related to contract-based design. Encouraged by this, we again introduce notions of implementation, refinement, and series composition. All of these notions are defined and characterized in terms of simulation conditions, which can be verified efficiently. We also consider the problems of constructing an implementation for a given contract and constructing a controller that turns a given plant system into an implementation of a given contract. First, we find necessary and sufficient conditions under which a given contract has an implementation, and we provide a systematic procedure for its construction when it exists. Then, using similar ideas, we find necessary and sufficient conditions under which there exists a controller that turns a given plant system into an implementation of a given contract, and we provide a systematic procedure for the construction of an appropriate controller when it exists. The latter is demonstrated with a simple vehicle following example.

Samenvatting

Moderne technologische systemen, zoals intelligente transportsystemen, slimme energienetwerken,slimme productiesystemen, etc., bestaan vaak uit vele onderling verbonden componenten. De ontwerpeisen voor de componenten van zulke systemen worden steeds complexer. Als gevolg daarvan vereist de ontwikkeling van deze componenten gespecialiseerde expertise en wordt daarom vaak uitgevoerd door verschillende (onafhankelijke) teams. Deze onafhankelijke teams hebben echter zelden de middelen om effectief samen te werken, wat kan leiden tot aanzienlijke en kostbare vertragingen. Dit kan worden voorkomen door het aannemen van een ontwikkel-methode die intrinsiek modulair is, d.w.z., een methode waarmee componenten onafhankelijk van elkaar kunnen worden beschouwd. Een dergelijke methode is gebaseerd op het gebruik van zogenaamde contracten, oorspronkelijk geïntroduceerd in het vakgebied van de informatica. Hoewel er al verscheidene contracttheorieën zijn ontwikkeld voor verschillende systeemklassen, zijn deze doorgaans beperkt tot systemen met discrete variabelen die zich discreet in de tijd ontwikkelen.

Hierdoor geïnspireerd ontwikkelen we in dit proefschrift een contracttheorie voor een klasse van dynamische regelsystemen in continue tijd, met continue variabelen. In het bijzonder introduceren we aanname-garantie contracten voor lineaire dynamische systemen met in- en uitgangen. Deze contracten worden gedefinieerd als een tweetal lineaire systemen, genaamd aannames en garanties, en ze dienen als specificaties voor componenten via twee aspecten. Ten eerste leggen de aannames de verwachte dynamica van de omgeving vast waarin de component opereert, wat leidt tot een klasse van compatibele omgevingen. Ten tweede leggen de garanties de vereiste dynamica van de component vast wanneer deze is verbonden met een compatibele omgeving, wat leidt tot een klasse van implementaties. Formeel worden de klassen van compatibele omgevingen en implementaties verkregen door systemen te vergelijken met de aannames en garanties. In dit proefschrift beschouwen we twee methoden voor systeemvergelijking, namelijk gedragsinclusie en simulatie, en we ontwikkelen een contracttheorie voor beide methoden.

We beginnen met het ontwikkelen van een contracttheorie met behulp van gedragsinclusie als methode voor systeemvergelijking. In het bijzonder

introduceren we begrippen als implementatie, verfijning en conjunctie, die ons in staat stellen om specificaties te beschrijven, vergelijken en combineren met behulp van contracten. We karakteriseren deze begrippen in termen van gedragsinclusies, en geven algoritmes voor hun verificatie. Verder onderzoeken we het probleem van het ontwerpen van een implementatie voor een gegeven contract. We bieden algoritmisch verifieerbare noodzakelijke en voldoende voorwaarden voor het bestaan van een implementatie, en we geven een systematische procedure voor de constructie ervan wanneer deze bestaat. Ook introduceren we het begrip van contractcompositie. Kort gezegd, de compositie van twee contracten is zodanig dat de interconnectie van hun implementaties gegarandeerd leidt tot een implementatie van hun compositie, onafhankelijk van de keuze van implementatie. Samen met de notie van verfijning maakt een dergelijke notie van compositie het onafhankelijk ontwerpen van componenten binnen gekoppelde systemen mogelijk. Met het oog hierop overwegen we dan twee vormen van compositie, gebaseerd op twee types gekoppelde systemen, namelijk serie- en terugkoppeling. Voor elk type bieden we algoritmisch verifieerbare, noodzakelijke en voldoende voorwaarden waaronder de compositie bestaat, en bieden we een expliciete uitdrukking ervoor wanneer deze bestaat.

Hoewel de contracttheorie gebaseerd op gedragsinclusie wordt ondersteund door algoritmen voor verificatie, zijn deze niet noodzakelijkerwijs efficiënt. Om dit probleem aan te pakken, ontwikkelen we een contracttheorie met behulp van simulatie in plaats van gedragsinclusie als methode voor systeemvergelijking. Simulatie wordt ondersteund door efficiënte algoritmen voor verificatie op basis van het (stuur-)invariante deelruimte-algoritme. Bovendien stelt de verbinding met de geometrische regeltechniek ons in staat om een veelvond aan methoden en technieken die daar zijn ontwikkeld te gebruiken voor het oplossen van problemen gerelateerd aan contractgebaseerd ontwerpen. Hierdoor geïnspireerd introduceren we opnieuw de begrippen van implementatie, verfijning en seriecompositie. Al deze begrippen worden gedefinieerd en gekarakteriseerd in termen van simulatievoorwaarden, die efficiënt kunnen worden geverifieerd. Verder beschouwen we ook de problemen van het construeren van een implementatie voor een gegeven contract en het construeren van een regelaar die een gegeven ongeregeld systeem omzet in een implementatie van een gegeven contract. Allereerst vinden we noodzakelijke en voldoende voorwaarden waaronder een gegeven contract een implementatie heeft, en bieden een systematische procedure voor de constructie ervan wanneer deze bestaat. Vervolgens, door gebruik te maken van vergelijkbare ideeën, vinden we noodzakelijke en voldoende voorwaarden waaronder een regelaar bestaat die een gegeven ongeregeld systeem omzet in een implementatie van een gegeven contract, en bieden we een systematische procedure voor het construeren van een geschikte regelaar wanneer deze bestaat. Dit laatste wordt gedemonstreerd aan de hand van een eenvoudig voorbeeld van voertuigen die elkaar volgen.