Compositional analysis and control of dynamical systems

Kerber, Florian Josef

1

Introduction

1.1. Motivation and setting

The goal of this thesis is to develop concepts and tools for compositional analysis and control of interconnected dynamical systems. We extend notions and techniques well established in computer science and apply them to dynamical systems commonly considered in systems theory and control. Our approach provides insights in various areas. Explicit connections are made with classical compositional analysis techniques in systems and control such as passivity theory and with decentralized control.

1.1.1. Compositional modeling and analysis techniques

Complexity is one of the key problems when analyzing engineering and IT processes. Many applications consist of a large number of subsystems interacting with each other, take as typical examples chemical reactors or finite element models in fluid and solid mechanics. In computer science, a similar problem is concurrency, i.e. the simultaneous execution of multiple processes e.g. in a shared memory or a network control system.

Example 1.1. A multi-product batch process is a chemical plant that processes raw materials to obtain multiple product substances. The main process units of such a batch process are the reactors where the raw materials are processed by mixing, heating, reacting with each other, etc. Both the raw materials and the products are stored in tanks. Tanks and reactors are connected through pipes. The process can be controlled by operating valves and pumps regulating the in- and outflow of tanks and reactors which are monitored by sensors, e.g. for water levels, temperature or other physical quantities. Figure 1.1 depicts a model of a two-product batch process. The storage tanks for the raw materials are modeled as subsystems $\Sigma_{P_i}, i = 1, 2, 3$, of the global plant. Each tank is controlled by pumps and valves represented by the controller systems $\Sigma_{C_i}, i = 1, 2, 3$, which are in turn interconnected with each other. Furthermore, the plant consists of two reactors, denoted by Σ_{P_4} and Σ_{P_5}, which are controlled by Σ_{C_4} and Σ_{C_5}, respectively. The product tanks

are represented as the components Σ_{P_6} and Σ_{P_7}. The pipes between tanks and reactors determine the interconnection structure of the plant. The external variables $e_i, z_i, i \in \{1, 3, 6, 7\}$ can be thought of as in- and outflows of raw materials and products, respectively. Without specifying the dynamics of the

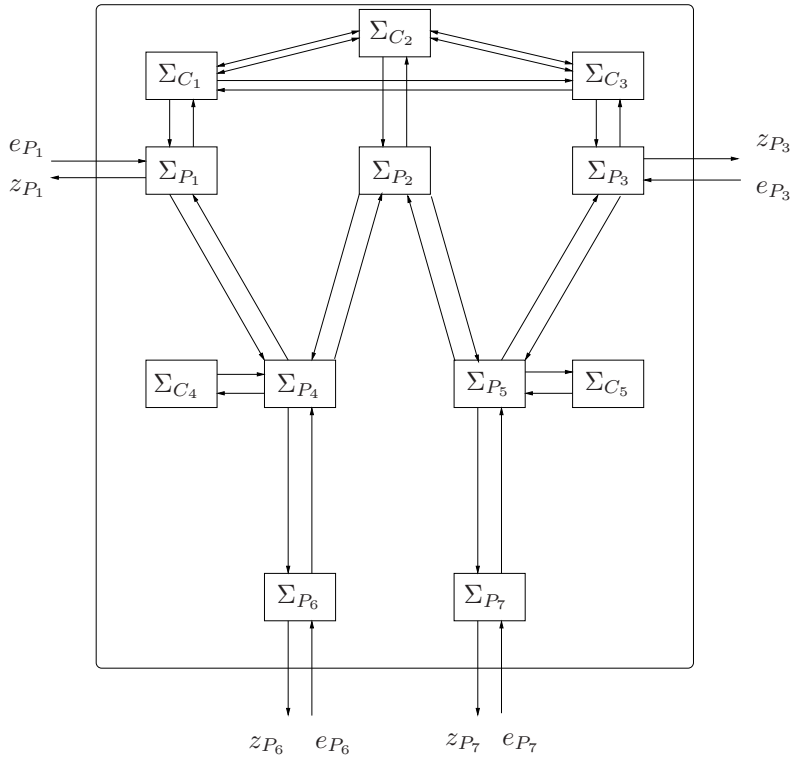

Figure 1.1.: Model of a multi-product batch process.

subsystems Σ_{P_i} and Σ_{C_i}, Example 1.1 thus illustrates how complex the model of a relatively simple industrial process can become.

Modeling these systems requires modular procedures, i.e., individual components as well as their interconnections have to be described formally and then combined to obtain a model of the whole process. Modular modeling techniques have been studied for various application, e. g. for manufacturing systems [51] and chemical processes [46, 16]. The focus of this thesis lies on compositional analysis and control techniques. Historically, the problem of how desired properties of complex systems can be verified systematically despite the "curse of dimensionality" has been addressed in the area of formal verification, a branch of computer science. In model checking [14] the design of a program represented as a transition system is verified by formulating

properties in terms of a temporal logic. There exist automated procedures to evaluate logical formulas even for large systems. To reduce the complexity arising from interconnections of subsystems the modular structure can be used to decompose the global verification task into several subproblems involving components of the overall system. Based on guaranteed properties of subsystems the corresponding properties of the overall system can be inferred, thus reducing the computational effort significantly when compared to checking the interconnected system as a whole. In particular, compositional and assume-guarantee reasoning [31, 32, 58] follows this principle. To apply compositional analysis techniques, implementations (the modeled system behavior) and specifications (the desired system behavior or property) have to be represented in the same descriptive framework. If the implemented system behavior is included in (or even equivalent to) the specified one the design is guaranteed to be correct.
Formal methods like model checking and compositional reasoning are defined for labeled transition systems. This motivated researchers from computer science and systems theory to adopt some of these techniques by interpreting dynamical control systems as generalized transition systems. The results of this thesis are based on further advances achieved in recent years, in particular with respect to (bi)simulation theory for continuous-time dynamical systems using their differential equation description. Bisimulation relations were introduced as a notion of equivalence between labeled transition systems by Milner [48] and Park [57]. Intuitively, two systems are bisimilar if they cannot be distinguished by interconnecting them to a common environment. This concept of external equivalence makes bisimulations especially useful for compositional analysis. Subsystems of a network of interacting processes can be replaced by components of lower complexity which are equivalent with respect to bisimulation. In this sense, bisimulation equivalence also prescribes a reduction procedure. By contrast, the one-sided version of bisimulations – simulation relations – defines abstractions of systems. That is, an abstraction captures all the external behavior of the original system and possibly even more than that. Put reciprocally, the simulated system refines details that are absent in the abstraction. Compositional and assume-guarantee reasoning schemes often use abstraction-refinement procedures based on simulation relations [79, 25]. In particular, if a component system satisfies, i. e. is similar to, its specification it can be replaced by the latter in the overall network. In recent years, bisimulation theory has been adopted to continuous-time control systems, see [56, 55, 69]. Usually, the original concept is mimicked by defining bisimulation relations of continuous-time systems with respect to their state trajectories and external variables. However, it has been shown in [74] that the existence of a bisimulation relation can be equivalently formulated as a geometric control problem, namely the modified disturbance decoupling problem [81]. This facilitates a linear-algebraic characterization of bisimulation relations for continuous-time systems based on

the differential equations describing the system model. The advantage of this structural notion of bisimulation lies in efficient and elegant algorithms for computations of maximal bisimulation relations. In this thesis, we make use of structural (bi)simulation relations to develop compositional and assume-guarantee reasoning techniques.

1.1.2. Compositional techniques in systems and control theory

Example 1.1 illustrates the need for compositional analysis techniques in the area of systems theory and control. Complexity has to be dealt with as a result of large state space dimensions. Like in the two-product batch process of Figure 1.1, interconnections between plant and controller systems or between subsystems of the overall plant are characteristics of control systems. This motivates the use of compositional techniques for control related purposes, e.g. to verify system theoretic properties of large-scale systems or to design decentralized control schemes capable of satisfying a global specification. A classical example for compositional reasoning in systems theory is the passivity theorem which states that the interconnection of two passive systems is again passive [63]. In this work, we will further develop the notion of passivity as a compositional property. To do so, passivity as a fundamental property of a control system has to be expressed in the same formalism, i.e. as a control system itself. We will show that this is possible for passivity and, to some extent, also for stability in the sense of Lyapunov. The idea is to specify properties by means of target dynamics that should be achieved by the original system. This can also be used for controller design, e.g. in the so-called immersion and invariance principle [4] where the target system is defined on an attractive and invariant manifold. Unlike in computer science, however, formulating specifications in the same language as the system model is not always part of the design process. In the context of this research, specifications are always interpreted as target systems, either explicitly defined to check passivity or stability or more abstractly to capture properties related to control performance. How to construct such specifications systematically would be an interesting topic for future research. This also holds for the problem of how to decompose global specifications into local subspecifications corresponding to subsystems of the plant. A starting point could be the decomposition strategies presented in [52, 53]. Given a transition system, these results include a procedure how to construct an isomorphic transition system given as the product of subsystems.
The next focus lies on controller design strategies for complex interconnected systems. Decentralized control [41, 17, 64] is the attempt to control the subsystems of a global plant individually by local controllers in such a way that the overall controlled system satisfies its specification. This concept has an im-

portant advantage: Restrictions due to limited communication and controller action between component systems can be incorporated naturally in the design of decentralized schemes. In the batch process depicted in Figure 1.1, the tank Σ_{P_1} is only connected to the first reactor Σ_{P_4} and similarly, Σ_{P_3} can only influence the second reactor Σ_{P_5} while tank Σ_{P_2} is connected to both reactors. The local controllers Σ_{C_1} and Σ_{C_3} only need to react to changes of the fill height of the respective reactors Σ_{P_4} and Σ_{P_5}. Likewise, distributed sensor and actuator locations like in structural monitoring [44], process control [61] and distributed robotic networks [9] also restrict communication between subsystems. Hence, the design procedures and consequently the hardware requirements for the network of all decentralized controllers should be much simpler than the corresponding global controller achieving the same performance. However, the difficulty of decentralized control is coordination, i.e. guaranteeing that the interconnection of locally controlled subsystems of the plant satisfies the desired global control target. In this respect, decentralized control can be seen as a complementary notion of compositional analysis. In this work, we therefore approach decentralized control problems using compositional analysis techniques. Different scenarios are possible, namely starting bottom-up from the level of local controllers such that a global specification is achieved as well as top-down from the level of a global specification that can be decomposed into subspecifications corresponding to subsystems of the plant.

The main aim of control theory has always been to develop procedures to construct controllers (global or decentralized) such that the closed-loop system satisfies the predefined specifications. By contrast, less is known about controller design methods for discrete transition systems, the supervisory control theory for discrete-event systems [62] being a notable exception. Recently, controller synthesis methods for classes of hybrid systems have been proposed [47, 59, 68] that follow the "correct by design"(or "correct by construction") paradigm. That is, instead of separating the implementation from the verification step in the synthesis process, correct by design methods automatically generate implementations from previously verified abstractions. Hence, correctness is always guaranteed provided the refinement procedure is formally correct. Moreover, the problem that final implementations are hard to check due to their complexity is circumvented.

This is especially beneficial when the controller implemented in software interacts with a continuous environment. Systems that combine elements of discrete and continuous dynamics are, depending on the context, referred to as hybrid systems (which we will use throughout) or embedded systems or cyber-physical systems. Many real-life systems exhibit hybrid behavior, e.g. the valves and pumps controlling the the multi-product batch process of Example 1.1. The interplay of continuous and discrete dynamics requires to merge analysis and design methods for transition systems on the one hand (the computer science approach) and for continuous-time dynamical systems

on the other hand (the systems and control approach). Within computer science, most commonly the mathematical formalism of labeled transition systems used to describe discrete-event systems is generalized to incorporate continuous variables. The resulting hybrid automata (e. g. [1, 45, 21]) then describe the continuous dynamics in terms of the trajectories. An alternative idea is to abstract hybrid by discrete dynamics, although often at the cost of very large discrete state space dimensions [2, 50, 23]. The focus lies on verification problems such as safety requirements, which have been implemented in several software packages (e.g. [22, 29]). By contrast, hybrid system models in the area of system and control often use differential-algebraic equations for the continuous part, see [77] for an overview. Starting from [43, 8] various subclasses were studied such as switching linear systems [60] or stochastic hybrid automata [13]. Analysis problems concern amongst others existence and uniqueness of solutions [27] and controller design methods. These include model-predictive and LMI-based control concepts, see e. g. [34] and [5]. In the last part of this thesis we investigate compositional analysis methods for switching linear systems combining the mathematical formalism of systems theory to benefit from structural notions of bisimulation relations and the compositional analysis techniques developed in formal verification to analyze system theoretic properties and develop decentralized control schemes.

1.2. Outline of the thesis

The main chapters of this thesis are organized as follows:

- In Chapter 2 we review simulation and bisimulation theory for both labeled transition and linear input-state-output systems. We characterize important properties of (bi)simulations and give a linear algebraic characterization. Furthermore, we give an algorithmic procedure to compute the maximal (bi)simulation relation between two linear systems. The specialization to the non-deterministic case is also dealt with. Brief examples illustrate abstractions of linear systems by simulation and reductions by bisimulation. Most of the content of this chapter is taken from [21] for labeled transition systems and [74] for linear systems.

- Chapter 3 contains a general treatment of compositional reasoning techniques for linear systems based on (bi)simulations. Two different types of interconnections are studied, namely feedback interconnections and parallel compositions. We show that compositional reasoning and both non-circular and circular assume-guarantee reasoning is sound for feedback interconnections of two linear systems. We also investigate whether the converse of these proof rules, i.e. their completeness, holds true. The results are then generalized to series of more than two feedback interconnections. Finally, we discuss compositional analysis techniques for

parallel compositions of linear systems entailing algebraic constraints. In particular, a proof rule based on the decomposition of the given specification is derived. The content of this chapter is an extension of [40] and its preliminary versions [39] and [37].

- In Chapter 4 we generalize some of the previous results to analyze nonlinear input-state-output systems. The main similarity lies in the fact that also for nonlinear systems, the existence of a simulation relation can be cast as a geometric control problem. We give regularity conditions under which nonlinear simulation is a preorder. Both soundness and completeness of compositional reasoning is established. Furthermore, we investigate whether circular assume-guarantee reasoning is sound.

- Chapter 5 discusses the relationship between nonlinear simulation theory and passivity theory. We show that passivity properties of both linear and nonlinear control systems can be equivalently characterized by the existence of a nonlinear simulation relation of the system under consideration and the one-dimensional system associated with the dissipation inequality. We then apply compositional reasoning techniques to prove that the interconnection of two passive systems is again passive. The converse statement can also be shown to hold true for both linear and nonlinear systems. We obtain conditions under which the storage function of a feedback interconnection is uniquely determined as the sum of the storage functions of the components. The results of both Chapter 4 and 5 are based on [36].

- Chapter 6 shows how compositional analysis techniques can be applied to decentralized control problems. We prove that both compositional and assume-guarantee reasoning schemes are sound for feedback interconnections of locally controlled plant systems and their specifications. Thus, we obtain decentralized control schemes that guarantee fulfillment of a global specification provided conditions for the local controllers are satisfied. The problem whether there exists for a given plant and specification a controller such that the controlled plant meets its specification is characterized by achievable simulations. We combine this result, given in terms of the so-called sandwich conditions, with compositional analysis techniques and apply this to our decentralized setting. As a result, we obtain two bottom-up decentralized control schemes that contain necessary conditions for the existence of local controllers such that the overall control network satisfies a global specification. Additionally, we consider a top-down scheme based on circular assume-guarantee reasoning. Starting with a global controller satisfying the overall specification, our result gives conditions for the

existence of local controllers that guarantee the same global control target. The content of this chapter is based on [35].

- Chapter 7 treats compositional analysis for a particular class of hybrid systems, namely switching linear systems. Due to the particular structure of switching linear systems, we develop a structural version of hybrid simulation which is easily checkable and is thus ideally suited for compositional analysis. We show that both compositional and non-circular assume-guarantee reasoning are sound. As to circular assume-guarantee reasoning, we give conditions under which the proof rule holds true. The material presented in this chapter can be found in [38].

- In Chapter 8 we consider a more general class of switching linear systems by adding location invariants and guard conditions. Thus, not only do the discrete dynamics influence the continuous ones through discrete events but the location invariants constraining the continuous evolution at every location (discrete state) can also trigger changes of the discrete state. Our aim is to describe equivalences of such hybrid systems by bisimulation. We therefore incorporate synchronization of guard conditions in the definition of bisimulation relations. As a first step we consider linear systems with inequality constraints representing the continuous part of the hybrid dynamics of switching linear systems. We give necessary and sufficient conditions for the existence of a bisimulation relation between two linear systems with inequality constraints and obtain, using the Farkas lemma, a linear-algebraic characterization. We then define structural hybrid bisimulation relations for switching linear systems with location invariants exploiting the dependencies between discrete and continuous dynamics.

- Chapter 9 highlights the main contributions of the thesis and outlines possible directions of future research.