Compositional Abstraction-based Synthesis for Cascade Discrete-Time Control Systems
Adnane Saoud, Pushpak Jagtap, Majid Zamani, Antoine Girard

To cite this version:

HAL Id: hal-01761180
https://hal.archives-ouvertes.fr/hal-01761180
Submitted on 7 Apr 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Compositional Abstraction-based Synthesis for Cascade Discrete-Time Control Systems

Adnane Saoud**, Pushpak Jagtap***, Majid Zamani***, Antoine Girard*

* Laboratoire des Signaux et Systèmes (L2S) - CNRS, 91192 Gif sur Yvette, France. (e-mail: {adnane.saoud, antoine.girard}@l2s.centralesupelec.fr)
** Laboratoire Spécification et Vérification - CNRS, ENS Paris-Saclay, 91235 Cachan Cedex, France.
*** Technical University of Munich, Munich, 80333 Germany (e-mail: {pushpak.jagtap, zamani}@tum.de).

Abstract: Abstraction-based synthesis techniques are limited to systems with moderate size. Thus to contribute towards scalability of these techniques, in this paper we propose a compositional abstraction-based synthesis for cascade interconnected discrete-time control systems. Given a cascade interconnection of several components, we provide results on the compositional construction of finite abstractions based on the notion of approximate cascade composition. Then, we provide a compositional controller synthesis for cascade interconnection. Finally, we demonstrate the applicability and effectiveness of the results using a numerical example and compare it with different abstraction and controller synthesis schemes.

Keywords: Symbolic control, Compositional abstraction, Compositional controller synthesis, Cascade composition, Discrete-time control system.

1. INTRODUCTION

Control and verification of dynamical systems using discrete abstractions and formal methods have been an ongoing research area in recent years (see Tabuada (2009) and the references therein). In such approaches, a discrete abstraction (i.e. a dynamical system with finite number of states) is constructed from the original system. When the concrete and abstract systems are related by some behavioral relation such as simulation, alternating simulation or their approximate versions, the discrete controller synthesized for the abstraction can be refined into a hybrid controller for the original system. The use of discrete abstractions principally enables the use of techniques developed in the areas of supervisory control of discrete event systems (Cassandras and Lafortune (2009)) and algorithmic game theory (Bloem et al. (2012)).

The construction of the discrete abstraction (a.k.a. symbolic model) is often based on a discretization of the state space. As a result, symbolic control techniques suffer severely from the curse of dimensionality (the computational complexity for synthesizing abstractions and controllers grows exponentially with the state space dimension).

To tackle this problem, several compositional approaches were recently proposed. The authors in (Tazaki and Imura (2009)) proposed a compositional approach for finite state abstractions of a network of control systems based on the notion of interconnection-compatible approximate bisimulation. The results in (Pola et al. (2016)) provide compositional constructions of approximately bisimilar finite abstractions for networks of discrete-time control systems under some incremental stability property. In (Mallik et al. (2016)), the notion of (approximate) disturbance simulation was used for compositional synthesis of continuous-time systems, where the states of the neighboring components were modeled as disturbance signals. The authors in (Dallal and Tabuada (2015), Kim et al. (2017), and Meyer et al. (2015)) use contract based design and assume-guarantee reasoning to provide compositional construction of controllers.

In spirit, our work is motivated by the recent work in (Hussien et al. (2017)) where a compositional abstraction was proposed for the class of partially feedback linearizable systems. However, this work is limited to the type of abstractions proposed in (Zamani et al. (2012)). In our work, we propose a compositional abstraction framework for cascade interconnected discrete-time control systems. Our framework allows the use of different types of abstractions for individual components in the cascade composition.
such as abstractions based on state-space quantization (Tabuada (2009)), partition (Meyer et al. (2015)), covering (Reißig (2011)), or without any state space discretization (Girard (2014)). Moreover, we provide results on the compositional controller synthesis as well.

In this paper, we provide a compositional abstraction-based controller synthesis framework for a cascade composition of $N$ discrete-time control systems. The main contributions of the work are divided into three parts. First, we introduce the notion of approximate cascade composition, which enables cascade composition of corresponding abstractions (possibly of different types). The use of different types of abstractions allows for more flexibility in the design of the overall symbolic model because each component may be suitable for a particular type of abstraction. Second, with the help of the aforementioned notion, we provide results on the compositional construction of abstractions for cascade interconnected systems. Third, we propose a compositional controller synthesis procedure for cascade composition of $N$ discrete time control systems. Finally, we demonstrate the applicability and effectiveness of the results using a numerical example and compare it with different abstraction and controller synthesis schemes.

The paper is organized as follows. In Section 2, we introduce the class of systems considered in this paper. In Section 3, we introduce the notion of approximate cascade composition and we show how one can use this notion to construct abstractions compositionally. In Section 4, we show how one can synthesize controllers compositionally for cascade interconnected systems. An example is given in Section 5 to show the merits of the theoretical results.

### 2. CONTROL SYSTEMS AND PRELIMINARIES

**Notation:** The symbols $\mathbb{N}$ and $\mathbb{R}^+_0$ denote the set of nonnegative integer and nonnegative real numbers, respectively. For any $x_1, x_2, x_3 \in X$, the map $d_X : X \times X \rightarrow \mathbb{R}^+_0$ is a pseudometric if the following conditions hold: (i) $x_1 = x_2$ implies $d(x_1, x_2) = 0$; (ii) $d(x_1, x_2) = d(x_2, x_1)$; (iii) $d(x_1, x_3) \leq d(x_1, x_2) + d(x_2, x_3)$. The closed ball centered at $x \in X$ with radius $R$ is defined by $B_R(x) = \{y \in X \mid d(x, y) \leq R\}$. Similarly, for $X \subseteq X$, $B_R(X) = \bigcup_{x \in X} B_R(x)$. We identify a relation $\mathcal{R} \subseteq A \times B$ with the map $\mathcal{R} : A \rightarrow 2^B$ defined by $b \in \mathcal{R}(a)$ if and only if $(a, b) \in \mathcal{R}$. Given a relation $\mathcal{R} \subseteq A \times B$, $\mathcal{R}^{-1}$ denotes the inverse relation defined by $\mathcal{R}^{-1} = \{(b, a) \in B \times A \mid (a, b) \in \mathcal{R}\}$.

#### 2.1 Discrete-time control systems

We consider the class of discrete-time control systems as the following:

**Definition 2.1.** The discrete-time control system $\Sigma$ is defined by a tuple $\Sigma = (X, U, f)$, where $X$ is a set of states, $U$ is a set of inputs, the map $f : X \times U \rightarrow X$ is called the transition function.

Consider the discrete-time control system $\Sigma$ of the form

$$x(k + 1) = f(x(k), u(k)),$$

where $x(k) \in X$ and $u(k) \in U$ for all $k \in \mathbb{N}$

#### 2.2 Transition systems and behavioral relations

We recall the notion of transition system introduced in (Tabuada (2009)) which later serves as a unified modeling framework for the discrete-time control systems, their discrete abstractions, and cascade compositions.

**Definition 2.2.** A transition system is a tuple $S = (X, X_0, U, \Delta, Y, H)$ where $X$ is a set of states (possibly infinite), $X_0 \subseteq X$ is a set of initial states, $U$ is a set of inputs (possibly infinite), $\Delta \subseteq X \times U \times X$ is a transition relation, $Y$ is a set of outputs, and $H : X \rightarrow Y$ is an output map.

We denote $x' \in \Delta(x, u)$ as an alternative representation for a transition $(x, u, x') \in \Delta$, where state $x'$ is called a $u$-successor (or simply successor) of state $x$, for some input $u \in U$. Given $x \in X$, the set of enabled (admissible) inputs for $x$ is denoted by $U^a(x)$ and defined as $U^a(x) = \{u \in U \mid (x, u, x') \notin \Delta\}$. A trajectory of the transition system is a finite or infinite sequence of transitions $\sigma = (x_0, u^1, x_1, u^2, x_2, \ldots)$, where $x_{i+1} \in \Delta(x_i, u_i)$, for $i \in \mathbb{N}$. The output behavior associated to the trajectory $\sigma$ is the sequence of outputs $\sigma_y = y_0, y_1, y_2, \ldots$ where $y_i = H(x_i)$ for all $i \in \mathbb{N}$. The set of all output behaviors of the transition system $S$ is denoted by symbol $Y$. The transition system is said to be:

- **pseudometric**, if the input set $U$ and the output set $Y$ are equipped with pseudometrics $d_U : U \times U \rightarrow \mathbb{R}^+_0$ and $d_Y : Y \times Y \rightarrow \mathbb{R}^+_0$, respectively.
- **finite (or symbolic)**, if $X$ and $U$ are finite.
- **deterministic**, if there exists at most a $u$-successor of $x$, for any $x \in X$ and $u \in U$.

In the sequel, we consider the approximate relationship for transition systems based on the notion of approximate (alternating) simulation relation to relate abstractions to concrete systems. We start by introducing the notion of approximate simulation relation (Julius et al. (2009)).

**Definition 2.3.** Let $S_1 = (X_1, X_{10}, U_1, \Delta_1, Y_1, H_1)$ and $S_2 = (X_2, X_{20}, U_2, \Delta_2, Y_2, H_2)$ be two transition systems such that $Y_1$ and $Y_2$ are subsets of the same pseudometric space $Y$ equipped with a pseudometric $d_Y$ and satisfying $B_{Y_1}(y_1) \subseteq Y_2$ for some $y_1 \in \mathbb{R}^+_0$ and $U_1, U_2$ are subsets of the same pseudometric space $U$ equipped with a pseudometric $d_U$. Let $\mu \geq 0$. A relation $\mathcal{R} \subseteq X_1 \times X_2$ is said to be an $(\epsilon, \mu)$-approximate simulation relation from $S_1$ to $S_2$, if it satisfies the following conditions:

(i) $\forall x_{20} \in X_{20}, \exists x_{10} \in X_{10}$ such that $(x_{10}, x_{20}) \in \mathcal{R}$;
(ii) $\forall (x_1, x_2) \in \mathcal{R}, d_Y(H(x_1, H_2(x_2)) \leq \epsilon$;
(iii) $\forall (x_1, x_2) \in \mathcal{R}$, $\forall u_1 \in U_1^{a}(x_1), \forall x'_{12} \in \Delta_1(x_1, u_1), \exists u_2 \in U_2^{a}(x_2)$ with $d_U(u_1, u_2) \leq \mu$ and $x'_{22} \in \Delta_2(x_2, u_2)$ satisfying $(x'_{12}, x'_{22}) \in \mathcal{R}$.

We denote the existence of an $(\epsilon, \mu)$-approximate simulation relation from $S_1$ to $S_2$ by $\mathcal{R} \approx_{(\epsilon, \mu)} S_2$.

We can see that when $\mu = 0$, we recover the classical notion of approximate simulation relation introduced in (Girard and Pappas (2007)) and when $\mu = \infty$, we get the definition of approximate simulation relation given in (Tabuada (2009)).

When using non-deterministic abstractions for the original discrete-time control systems, we need to consider relationships that explicitly capture the adversarial nature of
nondeterminism. The notion of approximate alternating simulation relation introduced in (Tabuada (2009)) is suitable for this case.

**Definition 2.4.** Let $S_1 = (X_1, X_{10}, U_1, \Delta_1, Y_1, H_1)$ and $S_2 = (X_2, X_{20}, U_2, \Delta_2, Y_2, H_2)$ be two transition systems such that $Y_1$ and $Y_2$ are subsets of the same pseudometric space $U$ equipped with a pseudometric $d_U$ and satisfying $B_s(Y_1) = Y_2$ for some $\varepsilon \in \mathbb{R}^+_0$ and $U_1, U_2$ are subsets of the same pseudometric space $U$ equipped with a pseudometric $d_U$. Let $\mu \geq 0$. A relation $R \subseteq X_1 \times X_2$ is said to be an $(\varepsilon, \mu)$-approximate alternating simulation relation from $S_2$ to $S_1$, if the following conditions are satisfied:

(i) $\forall x_{20} \in X_{20}, \exists x_{10} \in X_1$ such that $(x_{10}, x_{20}) \in R$;
(ii) $\forall (x_1, x_2) \in R$, $d_U(H_1(x_1), H_2(x_2)) \leq \varepsilon$;
(iii) $\forall (x_1, x_2) \in R$, $\exists u_2 \in U_2$, $\exists u_1 \in U_1$ such that $d_U(u_2, u_1) \leq \mu$ such that $\forall x'_2 \in \Delta_2(x_2, u_2)$ satisfying $(x'_2, x'_2) \in R$.

We denote the existence of an $(\varepsilon, \mu)$-approximate alternating simulation relation from $S_2$ to $S_1$ by $S_2 \preceq_{\varepsilon, \mu} S_1$.

We can see that when $\mu = \varepsilon = 0$ the approximate alternating simulation relation coincides with the feedback refinement relation given in (Reissig et al. (2017)).

**Remark 2.5.** We can see that the definitions of approximate (alternating) simulation relations used in the paper are slightly different from the classical ones. Unlike classical definitions, in our definitions the choice of the inputs is constrained by some distance property. However, these input constraints are not restrictive and the notions of (alternating) simulation relations used are verified by different abstraction techniques presented in the literature.

We define a pseudometric transition system associated with discrete-time control system $\Sigma = (X, U, f)$ by a tuple $S(\Sigma) = (X, X_0, U, \Delta, Y, H)$ where

- $X_0 \subseteq X, U = U$;
- $x' \in \Delta(x, u)$ is a transition from state $x \in X$ and input $u \in U$ if and only if $x' = f(x, u)$;
- $Y = X$, and $H : X \rightarrow Y$ is given by $H(x) = x$.

3. APPROXIMATE CASCADE COMPOSITION AND COMPOSITIONAL ABSTRACTION

In this section, we define the notion of approximate cascade composition of two transition systems which is latter used for construction of compositional abstractions and compositional controller synthesis.

Consider a cascade composition of two transition systems having output of the first system as an input to the second one. However, this might not be the case for the cascade composition of their corresponding abstractions. To mitigate the mismatch between the output of the abstraction of the first system and the input to the abstraction of the second system, we introduce the notion of approximate cascade composition as the following.

**Definition 3.1.** Let $S_1 = (X_1, X_{10}, U_1, \Delta_1, Y_1, H_1)$ and $S_2 = (X_2, X_{20}, U_2, \Delta_2, Y_2, H_2)$ be two pseudometric transition systems such that $Y_1$ and $Y_2$ are subsets of the same pseudometric space equipped with a pseudometric $d_U$, and $\mu \geq 0$. Systems $S_1$ and $S_2$ are said to be $\mu$-approximate cascade composable if and only if $Y_1 \subseteq R_{\mu}^+(U_2)$, where $R_{\mu} \subseteq Y_1 \times Y_2$ satisfies $u_2 \in R_{\mu}(y_1)$ if and only if $d_U(u_2, y_2) \leq \mu$. The $\mu$-approximate cascade composition is defined by a tuple $S_1||S_2 = (X, X_0, U, \Delta_2, Y, H)$, where

- $X = X_1 \times X_2$;
- $X_0 = X_{10} \times X_{20}$;
- $U = U_1 \cup U_2$;
- $(x_1, x'_2) \in \Delta_2(x_1, x_2, u_2)$ if and only if $x'_1 \in \Delta_1(x_1, u_1)$ and there exists $u_2 \in U_2$ with $H_1(x_1) \in R_{\mu}^{-1}(u_2)$ and $x'_2 \in \Delta_2(x_2, u_2)$;
- $Y = Y_2$;
- $H(x_1, x'_2) = H_2(x'_2)$.

**Remark 3.2.** We can see that the introduced notion of approximate cascade composition is quite general. In particular, when $R_{\mu}$ is an identity relation ($\mu = 0$), we find the cascade composition in its usual sense and we denote $S_1||S_2$ simply by $S_1|S_2$.

In the remaining part of this section, we provide relations between composition of $N$-subsystems by using relations between individual components. First we provide results for composition of two systems in the following theorems.

**Theorem 3.3.** Consider cascade composable pseudometric transition systems $S_1, S_2$ and $(\mu_2 + \varepsilon_1)$-approximate cascade composable pseudometric systems $S_1, S_2$. If $S_1 \preceq_{\varepsilon_1, \mu_1} S_1$ with a relation $R_1$ and $S_2 \preceq_{\varepsilon_2, \mu_2} S_2$ with a relation $R_2$, then relation $R \subseteq X_1 \times X_2 \times X_1 \times X_2$ defined by:

$$R = \{(x_1, x_2, x_1, x_2) \in X_1 \times X_2 \times X_1 \times X_2 | (x_1, x_1) \in R_1 \text{ and } (x_2, x_2) \in R_2\}$$

is an $(\varepsilon_2, \mu_1)$-approximate simulation relation from $S_1||S_2$ to $S_1||S_2$, i.e. $S_1||S_2 \preceq_{\varepsilon_2, \mu_1} S_1||S_2$.

**Proof.** The first condition of definition 2.3 is directly satisfied.

Let $(x_1, x_2, x_1, x_2) \in R$. We have $d_U(H(x_1, x_2), \hat{H}(x_1, x_2)) = d_U(H(x_1), H(x_2)) \leq \varepsilon_2$ where the equality comes from the definition of the output maps for cascade and approximate cascade compositions and the inequality comes from the second condition of Definition 2.3. Consider $(x_1, x_2, x_1, x_2) \in R$ and any $u_1 \in U^{\alpha}(x_1, x_2)$. Consider the transition $(x'_1, x'_2) \in \Delta_2(x_1, x_1, u_1)$ (i.e., $x'_1 \in \Delta_1(x_1, u_1)$ and $x'_2 \in \Delta_2(x_2, H_1(x_1)))$. From definition of the relation $R$ we have $(x_1, x_1) \in R_1$, $u_1 \in U^{\alpha}(x_1, x_2)$ and $x'_1 \in \Delta_1(x_1, u_1)$. Then, from the third condition of Definition 2.3, there exists $\hat{u}_1 \in U_1^{\alpha}(\hat{x}_1)$ with $d_U(u_1, \hat{u}_1) \leq \mu_1$ and there exists $\hat{x}_1 \in \Delta_1(\hat{x}_1, \hat{u}_1)$ such that $x'_1 = \Delta_1(\hat{x}_1, \hat{u}_1)$. Similarly, $(x_2, x_2) \in R_2$, and from Definition 3.1 we have $u_2 = H_2(x_1) \in U_2^{\alpha}(x_1, x_2)$. Consider $x'_2 \in \Delta_2(x_2, H_1(x_1))$, then, using the third condition of Definition 2.3 for the relation $R_2$, there exists $\hat{u}_2 \in U_2^{\alpha}(\hat{x}_2)$ with $d_U(u_2, \hat{u}_2) \leq \mu_2$ and there exists $\hat{x}_2 \in \Delta_2(\hat{x}_2, \hat{u}_2)$ satisfying $(x'_2, x'_2) \in R_2$.

Moreover, the condition $d_U(u_2, \hat{u}_2) \leq \mu_2$ implies that $d_U(u_2, \hat{u}_2, H_1(x_1)) \leq d_U(u_2, H_1(x_1)) \leq \mu_2 + \varepsilon_1$, hence, $H_1(\hat{x}_2) \in R_{\mu_2 + \varepsilon_1}(\hat{u}_2)$. Thus condition (iii) in Definition 2.3 holds and one obtains $S_1||S_2 \preceq_{\varepsilon_2, \mu_1} S_1||S_2$. \qed
Fig. 1. Illustration of compositional abstraction of $N$ cascade compositional transition systems using notion of $μ$-approximate cas- cade composition and $(ε, μ)$-approximate (alternating) simulation relations as formalized in Theorems 3.3 and 3.4.

**Theorem 3.4.** Consider cascade composable pseudometric transition systems $S_1, S_2$ and $(μ_2 + ε_1)$-approximate cas- cade composable pseudometric systems $S_1, S_2$. If $S_1 \preceq_{\epsilon_1, μ_1} S_1$ with some relation $R_1$ and $S_2 \preceq_{\epsilon_2, μ_2} S_2$ with some relation $R_2$ then the relation $R \subseteq X_1 \times X_2 \times \times X_2$ defined by:

$$
R = \{(x_1, x_2, 2, x'_2) \in X_1 \times X_2 \times \times X_2 \mid (x_1, x'_1) \in R_1 \text{ and } (x_2, x_2') \in R_2\}
$$

is an $(\epsilon_2, \mu_1)$-approximate alternating simulation relation from $S_1||_{μ_2+ε_2} S_1$ to $S_2||_{μ_2+ε_2} S_2$, i.e. $S_1||_{μ_2+ε_2} S_2 \preceq_{\epsilon_2, μ_1} S_1||_{μ_2+ε_2} S_2$.

**Proof.** $R_1$ is an approximate alternating simulation relation and $R_2$ is an approximate simulation relation. Hence, the first condition of Definition 2.4 follows immediately.

Let $(x_1, x_2, x_1', x_2') \in \mathcal{R}$ and for any $u_1 \in U^c(x_1', x_2)$. From (3) we have $(x_1, x_1') \in \mathcal{R}_1$ and for any $u_1 \in U^c(x_1', x_2)$ by using condition (iii) of Definition 2.4, we can pick $u_1 \in U^c(x_1')$ with $d_{\mathcal{U}_1}(u_1, u_1') \leq \mu_1$ such that for all $x_2' \in D_{x_1}(x_1) \times \times x_2$ there exists $x_1'$ satisfying $(x_1', x_1') \in R_1$. Now, consider $(x_1, x_2') \in \mathcal{D}_2(x_2, x_2)$. From (3), we have $(x_2, x_2') \in \mathcal{R}_2$ and from Definition 3.1 we have $u_2 = H_2(x_2) \in U^c(x_2)$.

Consider $x_2' \in \mathcal{D}_2(x_2, u_2)$, then using the third condition of Definition 2.3 for the relation $\mathcal{R}_2$ there exists $u_2 \in U^c(x_2)$ with $d_{\mathcal{U}_2}(u_2, u_2') \leq \mu_2$ and there exists $x_2' \in \mathcal{D}_2(x_2, u_2)$ satisfying $(x_2', x_2') \in \mathcal{R}_2$. Moreover, the condition $d_{\mathcal{U}_2}(u_2, u_2') \leq \mu_2$ implies that $d_{\mathcal{U}_2}(u_2, H_1(x_1)) \leq d_{\mathcal{U}_d}(u_2, u_2') + d_{\mathcal{U}_d}(u_2, H_1(x_1)) \leq \mu_2 + \epsilon_1$, hence $H_1(x_1) \in \mathcal{R}_n^{-1} \times x_1'. \mathcal{R}_n$ Thus condition (iii) in Definition 2.4 holds and one gets $S_1||_{μ_2+ε_2} S_2 \preceq_{\epsilon_2, μ_1} S_1||_{μ_2+ε_2} S_2$. □

In next corollaries, we provide generalization of the results in Theorems 3.3 and 3.4 for cascade composition of $N$ transition systems. The results are direct consequences of Theorems 3.3 and 3.4 and thus stated without proofs. An illustration of these results is given in Figure 1.

**Corollary 3.5.** Let $S_1, \ldots, S_N, \hat{S}_1, \ldots, \hat{S}_N$ be a collections of $2N$ pseudometric transition systems satisfying the following assumptions:

(i) for $i \in \{1, \ldots, N\}$, $S_i \preceq_{\epsilon_i, μ_i} \hat{S}_i$;
(ii) for $i \in \{2, \ldots, N\}$, $S_i$ and $S_i$ are cascade composable and $S_{i-1}$ and $S_i$ are $(μ_1 + ε_{i-1})$-approximate cascade composable.

Then we have $S_1||_{μ_2+ε_2} S_1 ||_{μ_2+ε_2} \ldots ||_{μ_2+ε_2} S_N \preceq_{\epsilon_N, μ_N} \hat{S}_1 ||_{μ_2+ε_2} \hat{S}_2 ||_{μ_2+ε_2} \ldots ||_{μ_2+ε_2} \hat{S}_N$.

**Corollary 3.6.** Let $S_1, \ldots, S_N, \hat{S}_1, \ldots, \hat{S}_N$ be a collections of $2N$ pseudometric transition systems satisfying the following assumptions:

(i) $S_1 \preceq_{\epsilon_1, μ_1} S_1$;
(ii) for $i \in \{2, \ldots, N\}$, $S_i \preceq_{\epsilon_i, μ_i} \hat{S}_i$;
(iii) for $i \in \{2, \ldots, N\}$, $S_i$ and $S_i$ are cascade composable and $S_{i-1}$ and $S_i$ are $(μ_1 + ε_{i-1})$-approximate cascade composable.

Then we have $S_1||_{μ_2+ε_2} S_1 ||_{μ_2+ε_2} \ldots ||_{μ_2+ε_2} S_N \preceq_{\epsilon_N, μ_N} S_1 ||_{μ_2+ε_2} \ldots ||_{μ_2+ε_2} S_N$.

**4. COMPOSITIONAL CONTROLLER SYNTHESIS**

In this section, we provide compositional synthesis approach for synthesizing controllers enforcing some specification $Y_{spec} \subseteq \mathcal{Y}$ on the output of $S_1||_{μ_2} S_2$.

Consider system $S = (X, X_0, U, \Delta, Y, H)$ and a memoryless controller $C$ : $X \rightarrow 2^X$ such that for all $x \in X$, $C(x) \subseteq U^c(x)$. Let $dom(C)$ be the domain of controller defined by $dom(C) = \{x \in X | \text{ if } C(x) \neq \emptyset \in X\}$. We define a controlled transition system by a tuple $S_C = (X, X_0, U_C, \Delta_C, Y_C, H_C)$, where $X_C = X \cup dom(C)$, $X_0 = X_0 \cap dom(C)$, $U_C = U, Y_C = Y, H_C = H$, and transition $x_C \in \Delta_C(x_C, u_C)$ if and only if $x_C \in \Delta(x_C, u_C)$ and $u_C \in C(x_C)$.

Given a specification $Y_{spec} \subseteq \mathcal{Y}$ on the output set of $S$, we say that $C$ is a controller for $S$ enforcing the specification $Y_{spec}$ if $\mathcal{Y}_C \subseteq Y_{spec}$ where $\mathcal{Y}_C$ is the set of all output behaviors of the controlled transition system $S_C$. The next theorem shows the main result of this section.

**Theorem 4.1.** Let $S_1$ and $S_2$ be two pseudometric transition systems which are $μ$-approximate cascade composable. Let $C_2$ be a controller for $S_2$ enforcing some specification $Y_{spec}$ on its output $Y_2$. Then $S_1$ is $μ$-approximate cascade composable with $S_2C_2$. Moreover, let $C_1$ be a controller for $S_1||_{μ_2} S_2C_2$ enforcing specification $Y_{spec}$ on its output $Y_2$ and $C$ be a controller for $S_1||_{μ_2} S_2C_2$ defined by:

$$
C(x_1, x_2) = \begin{cases} C_1(x_1, x_2), & \text{if } \exists u_2 \in C_2(x_2) \\
\emptyset, & \text{with } H_1(x_1) \in \mathcal{R}_n^{-1}(u_2); \\
\emptyset, & \text{otherwise.}
\end{cases}
$$
Then \( (S_1|\mu S_2)C = (S_1|\mu S_2)_C C_1 \), and controller \( C \) enforces \( \mathcal{V}_{\text{spec}} \) on the output of \( S_1|\mu S_2 \).

**Proof.** Since \( S_1 \) is \( \mu \)-approximate cascade composable with \( S_2 \) and the transition systems \( S_2 \) and \( S_2C \) have the same input sets \( U_2C = U_2 \), \( S_1 \) is \( \mu \)-approximate cascade composable with \( S_2C \).

Let \( (S_1|\mu S_2)C = (X_{12C}, X_{12C0}, U_{12C}, \Delta_{12C}, Y_{12C}, H_{12C}) \) and \( (S_1|\mu S_2)_C = (X_{12C}, X_{12C0}, U_{12C}, \Delta_{12C}, Y_{12C}, H_{12C}) \). In order to prove that transition systems \( (S_1|\mu S_2)_C \) and \( (S_1|\mu S_2)C \) are equal we have to prove corresponding elements of two tuples are equal.

We have:

- Let us prove that \( X_{12C} = X_{12C} \).
  We have \( X_{12C} = \text{dom}(C) = \text{dom}(C_1) \cap \{ (x_1, x_2) \mid \exists u_2 \in C_2(x_2), H_1(x_1) \in R_{\mu}^{-1}(u_2) \} \) and \( \text{dom}(C_1) \subseteq U_2(x_1, x_2C_2) \subseteq \{ (x_1, x_2) \mid \exists u_2 \in C_2(x_2), H_1(x_1) \in R_{\mu}^{-1}(u_2) \} \). Hence, \( X_{12C} = \text{dom}(C_1) = X_{12C} \).
- \( X_{12C0} = X_{12C} \).
- \( U_{12C} = U_1 = U_{12C} \).
- \( H_{12C} = H_{12C} \).
- \( Y_{12C} = Y_{12C} \).
- \( (x_1, x_2) \in \Delta_{12C}(x_1, x_2, u_1) \) if and only if \( x'_1 \in \Delta_1(x_1, u_1), x'_2 \in \Delta_2(x_1, u_2), u_1 \in C_1(x_1, x_2), R_{\mu}(u_2) \cap H_1(x_1) \neq \emptyset \) and \( u_2 \in C_2(x_2) \); which is equivalent to \( (x_1', x_2') \in \Delta_{12C}(x_1, x_2, u_1) \).

Hence, transition systems \( (S_1|\mu S_2)_C \) and \( (S_1|\mu S_2)C \) are equal and implies that controller \( C \) enforces \( \mathcal{V}_{\text{spec}} \) on the output of \( S_1|\mu S_2 \).

If we have abstraction \( \hat{S} \) corresponding to \( S \) satisfying \( \hat{S} \preceq_{\mathcal{A}_S} S \) with \( (\varepsilon, \mu) \)-approximate alternating simulation relation \( \mathcal{R} \), one can easily synthesize controller \( \hat{C} \) for \( \hat{S} \) enforcing \( \mathcal{V}_{\text{spec}} \) using various synthesis techniques and this controller can then be refined to a controller \( C \) for the original system (see Tabuada (2009)).

Next we provide similar result as in Theorem 4.1 for compositional controller synthesis for cascade composition of \( N \) transition systems.

**Corollary 4.2.** Let \( S_1, S_2, \ldots, S_N \) be a collection of \( N \) pseudometric transition systems satisfying the following assumptions:

(i) for all \( i \in \{2, \ldots, N\} \), \( S_{i-1} \) and \( S_i \) are \( (\mu_i) \)-approximate cascade composable;
(ii) \( \delta_N \) is a controller for \( S_N \) enforcing some specification \( \mathcal{V}_{\text{spec}} \) on its output \( Y_N \) and for all \( i \in \{1, \ldots, N-1\}, \delta_i \) is a controller for \( S_i|\mu_{i+1}(\cdots(S_N-2|\mu_{N-1}(S_{N-1}|\mu_{N}\mathcal{S}_N)C_{N-1})C_{N-2})\cdots)C_{i+1} \) enforcing specification \( \mathcal{V}_{\text{spec}} \) on the output \( Y_N \).

Then the controller \( C \) defined by: ( \( u_1 \in C(x_1, x_2, \ldots, x_N) \) if and only if \( u_1 \in C_1(x_1, x_2, \ldots, x_N) \) and for all \( i \in \{2, \ldots, N\}, u_i \in C_i(x_1, \ldots, x_N) \) and \( H_{i-1}(x_{i-1}) \subseteq R_{\mu_i}(u_i) \), satisfies 
\[
(S_1|\mu_2 S_2|\mu_3|\cdots|\mu_N S_N)C = (S_1|\mu_2(S_2|\mu_3|\cdots(S_{N-2}|\mu_{N-1}(S_{N-1}|\mu_{N}\mathcal{S}_N)C_{N-1})C_{N-2})\cdots)C_i
\]
and controller \( C \) enforces \( \mathcal{V}_{\text{spec}} \) on the output of \( (S_1|\mu_2 S_2|\mu_3|\cdots|\mu_N S_N)C \).

**Proof.** The proof is similar to the one of Theorem 4.1 and is omitted here. \( \square \)

5. AN EXAMPLE

To show the efficacy of our results, we consider a safety controller synthesis problem of a cascade composition of the following discrete-time control systems:
\[
\begin{align*}
\Sigma_1 &: x_1(k+1) = 0.2x_1(k) + \epsilon(k), \\
\Sigma_2 &: x_2(k+1) = 1.5x_2^2(k) + x_1(k).
\end{align*}
\]

Although the above example is rather small to show the effectiveness of compositionality, it is chosen just for the sake of illustrating the computational advantages of our proposed compositional scheme in comparison with the monolithic one (cf. Table 1). Let \( S_1 \) and \( S_2 \) be the transition systems corresponding to \( \Sigma_1 \) and \( \Sigma_2 \), respectively. To demonstrate the effectiveness of the proposed results, we consider three cases: (i) conventional monolithic abstraction and monolithic controller synthesis (MAMC), (ii) compositional abstraction and monolithic controller synthesis (CAMC), and (iii) compositional abstraction and compositional controller synthesis (CACC). For conventional monolithic abstraction and controller synthesis, we used partition based abstraction satisfying alternating simulation relation as discussed in (Reissig et al. (2017) and Meyer et al. (2015)). The safety controller synthesis is also done directly on the monolithic abstraction.

For constructing compositional abstractions, we construct an \( \varepsilon \)-approximate bisimilar abstraction of \( S_1 \) called \( \hat{S}_1 \) using state-space discretization-free abstraction techniques as discussed in (Girard (2014); Zamani et al. (2017)) and construct abstraction \( \hat{S}_2 \) of \( S_2 \) by partitioning the state set. For constructing \( \hat{S}_1 \) with precisions \( \varepsilon_1 = 0.0016 \) and \( \mu_1 = 0 \), we consider \( U = \{0, 2, 0.4, 0.6, 0.8\} \), length of input sequence \( N = 4 \), and source state \( x_N = 0.5 \). (For description and computation of these parameters see Girard (2014) and Zamani et al. (2017))). For computation of \( \hat{S}_2 \), we consider \( \varepsilon_2(k) \in [0, 1] \) with state quantization parameter \( \eta = 0.01 \) and input of \( S_2 \) which is \( x_2(k) \in [0, 1] \) with input quantization parameter \( \mu = 0.01 \). Hence, the precisions are given by \( \varepsilon_2 = \mu_2 = \sqrt{\mu_2} \). Using these abstractions and results in Theorem 3.4, we have \( \hat{S}_1|\mu_2+\varepsilon_2 \hat{S}_2 \preceq_{\mathcal{A}_S} S_1|\mu_2 \).

Having compositional abstraction, one can easily synthesize safety controller monolithically for \( \hat{S}_1|\mu_2+\varepsilon_2 \hat{S}_2 \) and the safe set \( W = [0, 1] \) using maximal fixed point algorithm (Tabuada (2009)) and then refine the controller for \( S_1|\mu_2 \).

For compositional controller synthesis, we first construct a safety controller \( \hat{C}_2 \) for \( \hat{S}_2 \). Second, we compute safety controller \( \hat{C}_1 \) for \( \hat{S}_1|\mu_2+\varepsilon_2 \hat{S}_2 \), and correspondingly compute \( \hat{C} \) as shown in (4) which is a safety controller for \( \hat{S}_1|\mu_2+\varepsilon_2 \hat{S}_2 \). Having \( \hat{C} \), one can easily refine it to the original interconnected system as discussed in Section 4. Figure 2 shows computed controllers for all three cases. Table 1 gives the computation time for generating the symbolic models and synthesizing the controllers and the size of resulting controllers in terms of number of transitions for all three cases. One can observe that the computation time for CACC is reduced significantly by around 70% as compared to MAMC whereas the size of the controller is reduced only by 3.93%. The numerical implementation
of the example has been done using Matlab on an iMAC with CPU 3.5 GHz Intel Core i7.

6. CONCLUSION

In this paper, we have proposed a compositional synthesis methodology for discrete-time cascade interconnected systems. The introduced notion of approximate cascade composition allows to compose different types of abstractions. Moreover we provided compositional results based on approximate (alternating) simulation relations, and showed how this results can been used for the compositional controller synthesis. A numerical example is given to show the effectiveness of our approach where we used different abstractions for discrete-time cascade interconnected systems. In future work, we extend ideas of the paper to more general interconnections of systems.

REFERENCES


