Nonlinear Analysis: Hybrid Systems 30 (2018) 58–71

Contents lists available at ScienceDirect

Nonlinear Analysis: Hybrid Systems

journal homepage: www.elsevier.com/locate/nahs

Deadlock-free output feedback controller design based on approximately abstracted observers ☆

Masashi Mizoguchi, Toshimitsu Ushio *

Graduate School of Engineering Science, Osaka University, 1-3 Machikaneyama, Toyonaka, Osaka, 560-8531, Japan

ARTICLE INFO

Article history:
Received 16 May 2017
Accepted 15 April 2018
Available online 5 May 2018

Keywords:
Symbolic control
Abstraction
Observer
Alternating simulation relation
Approximate contractive relation

ABSTRACT

In this paper, we design a deadlock-free symbolic output feedback controller. A physical plant is modeled by an infinite transition system, whose verification and synthesis problems are generally undecidable in finite time steps. Then, we consider an abstracted model of the physical plant. Assume that a controller for the abstracted plant model is given if the state of the physical plant is fully measured. For the application to the case of partial observation, we design an observer induced by the abstracted plant model and obtain an output feedback controller. The proposed observer computes sets of candidates of the current state with injected inputs and observed outputs. The control input is determined in such a way that every candidate state listed by the observer satisfies the control specification that had been achieved by the controller in the case of full observation, which implies that the proposed approach suppresses the effects of the partial observation. A deadlock-free controller is computed iteratively by eliminating transitions to deadlock states.

1. Introduction

Over the past few decades, the control of hybrid systems has been studied [1]. An approach to the design of embedded controllers is symbolic control that is paid much attention to in these days. In symbolic control, it is an important issue to find an algorithmic procedure for the design of a finite symbolic controller. A physical plant is an infinite-state system for which verification and synthesis problems are undecidable in general. For the analysis within finite time steps, state abstraction based on (bi)simulation was introduced [2]. A notion of (bi)simulation was originally used to evaluate the equivalence of behaviors of two concurrent systems [3], that is, if there exists a (bi)simulation relation between the physical plant and its abstracted model, it is concluded that the abstracted model describes all behaviors of the physical plant. But, this condition is often too restrictive for abstraction [4]. Then, approximate abstraction based on approximated (bi)simulation was introduced. The performance of the abstraction is evaluated with a Lyapunov-like function called a (bi)simulation function that determines if two given systems exhibit similar behaviors within a specified precision [5–9]. For the evaluation of behaviors of two systems, a notion of alternating simulation also plays an important role as well as (bi)simulation since it was proposed in [10]. It is well-known that the symbolic synthesis is dealt with alternating simulation as long as the plant is finite [2]. In order to design an abstracted symbolic controller, approximate alternating simulation was proposed [5].

Recently, symbolic control was extended to a networked control system. Communication networks often have delays, which may affect the stability of the plant. Then, the design of robust symbolic controllers has been studied. Some studies

☆ This work was supported by JSPS KAKENHI No. JP15K14007.

* Corresponding author.
E-mail addresses: mizoguchi@hopf.sys.es.osaka-u.ac.jp (M. Mizoguchi), ushio@sys.es.osaka-u.ac.jp (T. Ushio).

https://doi.org/10.1016/j.nahs.2018.04.001
1751-570X/

model network delays as perturbations [11–15], and others apply state prediction to deal with delays [16–18]. In the past few years, it was shown that the input–output dynamical stability, which is a kind of the input–output stability, is preserved under an approximate contractive alternating simulation relation [19–22]. These results lead us to design a robust controller for a physical plant with its approximately abstracted model.

Since a state of a plant is not fully measured in general, synthesis problems under partial observation have been studied with various approaches such as game strategies and specification-based estimators [23–25]. Approximately abstraction under partial observation can be seen in [26–32]. For discrete event systems, it is common to design an observer that lists possible candidates of the current plant state [33,34], and this observer-based approach was applied to design an abstracted controller [35].

The authors proposed a symbolic output feedback controller in the conference paper [36], where the state space of the physical plant is abstracted to a c-abstracted system and an o-abstracted system. The c-abstracted system is used to obtain a symbolic state feedback controller. In contrast, the o-abstracted system is designed in such a way that all states abstracted to the same o-abstracted state have the same output value. Then, the observer estimates a set of o-abstracted states that may contain the current state of the physical plant, and the controller determines a control input such that a control specification is achieved at every estimated state. This approach can be seen as a generalization of supervisory control [37]. However, several conditions are imposed to consider the worst case between two abstracted systems. Instead, this paper considers another approach that does not use the o-abstracted system. Based on injected inputs and observed outputs, the observer directly estimates c-abstracted candidates of the current state of the physical plant. As well as the previous approach, the controller determines a control input such that the control specification is achieved at every candidate. Then, the effects of the partial observation are suppressed, and the controlled plant still exhibits a desired behavior in spite of the partial observation. It is noticed that the proposed controller has deadlock states where there does not exist any control input that enforces the specification to all estimated candidates. Then, we introduce an operator that eliminates transitions to deadlock states. Finally, a deadlock-free controller is obtained as a supremal fixed point of the operator.

The rest of this paper is organized as follows. In Section 2, we define a system as a transition system, and introduce several fundamental notions related to approximated abstraction. A symbolic observer is designed in Section 3, and we construct a deadlock-free output feedback controller in Section 4. In Section 5, we consider an illustrative example to demonstrate how the proposed controller works.

2. Preliminaries

2.1. Notations

Let $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z}_{\geq 0}$, and $\mathbb{R}_{\geq 0}$ be the sets of integers, real numbers, non-negative integers, and non-negative real numbers, respectively. For any $a \in \mathbb{R}$ and any $b \in \mathbb{R} \cup \{\infty\}$ such that $a \leq b$, $[a, b[\subseteq \mathbb{R}$ is defined as follows:

$$[a, b[:= \{x \in \mathbb{R} \mid a \leq x < b\}.$$

The ∞-norm of $x \in \mathbb{R}^n$ is denoted by $|x|$. For any real number $x \in \mathbb{R}$, $\lfloor x \rfloor$ is the value of the floor function. For given sets A and B, denoted by A^B is a set of all mappings from B to A.

2.2. Systems and approximated alternating relations

We review several fundamental notions for transition systems [20,21].

Definition 1. A system S is a tuple (X, X_0, U, r), where

- X is a set of states;
- $X_0 \subseteq X$ is a set of initial states;
- U is a set of inputs; and
- $r : X \times U \to 2^X$ is a transition map.

For any $x \in X$, $U(x) \subseteq U$ is defined as follows:

$$U(x) = \{u \in U \mid r(x, u) \neq \emptyset\}.$$

Let $S_1 = (X_1, X_{10}, U_1, r_1)$ and $S_2 = (X_2, X_{20}, U_2, r_2)$ be two systems. For a relation $R \subseteq X_1 \times X_2 \times U_1 \times U_2$ over the state sets X_1, X_2 and the input sets U_1, U_2, we denote a projection of R to the state sets X_1, X_2 by $R_X \subseteq X_1 \times X_2$ defined as follows:

$$R_X = \left\{(x_1, x_2) \in X_1 \times X_2 \mid \exists u_1 \in U_1, \exists u_2 \in U_2 : (x_1, x_2, u_1, u_2) \in R \right\}.$$

Definition 2. Let $S_1 = (X_1, X_{10}, U_1, r_1)$ and $S_2 = (X_2, X_{20}, U_2, r_2)$ be two systems, let $\kappa, \lambda \in \mathbb{R}_{\geq 0}$, $\beta \in [0, 1[$ be some parameters, and consider a map $\mathsf{d} : U_1 \times U_2 \to \mathbb{R}_{\geq 0}$. We call a parameterized (by $\epsilon \in [\kappa, \infty[$) relation $R(\epsilon) \subseteq X_1 \times X_2 \times U_1 \times U_2$ a κ-approximate (β, λ)-contractive alternating simulation relation ((κ, β, λ)-acASR) from S_1 to S_2 with d if $R(\epsilon) \subseteq R(\epsilon')$ holds for all $\epsilon \leq \epsilon'$ and the following two conditions hold for all $\epsilon \in [\kappa, \infty[$: