Robust approximate symbolic models for a class of continuous-time uncertain nonlinear systems via a control interface ⋆

Pian Yu [a], Dimos V. Dimarogonas [a]

[a] *Division of Decision and Control Systems, EECS, KTH Royal Institute of Technology, 10044 Stockholm, Sweden.*

Abstract

Discrete abstractions have become a standard approach to assist control synthesis under complex specifications. Most techniques for the construction of a discrete abstraction for a continuous-time system require time-space discretization of the concrete system, which constitutes property satisfaction for the continuous-time system non-trivial. In this work, we aim at relaxing this requirement by introducing a control interface. Firstly, we connect the continuous-time uncertain concrete system with its discrete deterministic state-space abstraction with a control interface. Then, a novel stability notion called η-approximately controlled globally practically stable, and a new simulation relation called robust approximate simulation relation are proposed. It is shown that the uncertain concrete system, under the condition that there exists an admissible control interface such that the augmented system (composed of the concrete system and its abstraction) can be made η-approximately controlled globally practically stable, robustly approximately simulates its discrete abstraction. The effectiveness of the proposed results is illustrated by two simulation examples.

Key words: Discrete abstraction, uncertain systems, robust approximate simulation relation, control interface.

1 Introduction

In recent years, discrete abstractions have become one of the standard approaches for control synthesis in the context of complex dynamical systems and specifications [32]. It allows one to leverage computational tools developed for discrete-event systems [7,19,27] and games on automata [5, 21] to assist control synthesis for specifications difficult to enforce with conventional control design methods, such as linear temporal logic [6] specifications. Moreover, if the behaviors of the original system (referred to as the concrete system) and the abstract system (obtained by, e.g., discretizing the state-space) can be formally related by an inclusion or equivalence relation, the synthesized controller is known to be correct by design [13].

For a long time, (bi)simulation relations were a central notion to deal with complexity reduction [24, 25]. It was later pointed out in [2] that this kind of equivalence relation is often too strong. To this end, a new notion called approximate (bi)simulation, which only asks for the closeness of observed behaviors, was introduced in [10]. Based on the notion of incrementally (input-to-state) stable [4], approximately bisimilar symbolic models were built and extended to various systems [12, 26, 37]. However, incrementally (input-to-state) stable is a strong property for dynamical control systems, which makes its applicability restrictive. In [35], the authors relax this requirement by only assuming Lipschitz continuous and incremental forward completeness, and an approximate alternating simulation relation is established by over-approximating the behavior of the concrete system. However, as recently pointed out in [28], this approach may result in a refinement complexity issue. To this end, a new simulation relation, called feedback refinement relation is proposed in [28]. In addition, for monotone systems, the notion of directed alternating simulation relation is proposed for the construction of symbolic models [17].

Although continuous-time systems are extensively studied and various abstraction techniques are proposed in

⋆ This work was supported in part by the Swedish Research Council (VR), in part by the Swedish Foundation for Strategic Research (SSF), in part by the ERC CoG LEAFHOUND, and in part by the Knut and Alice Wallenberg Foundation (KAW).
Corresponding author. Tel.: +46 7 64199298. E-mail address: piany@kth.se (Pian Yu).

the existing literature, most techniques for the construction of symbolic models require time-space discretization of the continuous-time system, which constitute property satisfaction non-trivial since closeness of the observed behaviors between the concrete system and its abstraction is not guaranteed within neighboring discrete time instants. In addition, there is no systematic approach to choose the time-space discretization parameter. Recently, different approaches have been proposed in the literature to deal with this [20,23,30]. In [23], a disturbance simulation relation is introduced for incrementally input-to-state stable nonlinear systems. In [20,30], symbolic control approaches are proposed for a class of sample-data nonlinear systems, where property satisfaction of the continuous-time systems is guaranteed by equipping the finite abstractions with certain robustness margins [20] or assume-guarantee contracts [30]. While almost all the results are providing behavioral relationships between a time discretized version of the original system and its symbolic model, in this paper, we provide for the first time a behavioral relationship between the original continuous-time system and its symbolic model.

This paper investigates the construction of symbolic models for continuous-time uncertain nonlinear systems, and it improves upon most of the existing results by not requiring time-space discretization of the concrete system. The main contributions are as follows. i) We propose a novel stability notion, called η-approximately controlled globally practically stable. This is a property defined on the augmented system (composed of the concrete system and the abstract system) via an admissible control interface. We show that the abstract system can be constructed without time-space discretization. This is crucial for safety-critical applications, in which it is necessary that the trajectories of the concrete system and the abstract system are close enough at all time instants. ii) We define a notion of robust approximate simulation relation. It is shown that for an uncertain concrete system, the abstract system can be constructed such that the concrete system robustly approximately simulates the abstraction. iii) For the class of incrementally quadratic nonlinear systems, the systematic construction of the admissible control interfaces and robust approximate symbolic models under bounded input set is provided.

The introduction of the control interface is inspired by the hierarchical control framework [9,11,31,33], in which an interface is built between a high dimensional concrete system and a simplified low dimensional abstraction of it. Both the concrete system and the abstract system are continuous in [9, 11, 31, 33]. In contrast, in this paper, we propose to build a control interface between the continuous-time concrete system and its discrete state-space abstraction. Moreover, in this paper we consider bounded input set (the input set considered in [9, 11, 31, 33] is unbounded), which brings additional difficulty to constructing the interface. Therefore, the results in this paper are essentially novel and improved with respect to the existing work.

A preliminary version of this work was accepted by the 58th IEEE Conference on Decision and Control (CDC 2019) [34]. Here, we expand this preliminary version in three main directions. First, the framework is generalized to include time-varying uncertain nonlinear systems. A new stability notion, called η-approximately controlled globally practically stable, is proposed. Second, a new simulation relation, called robust approximate simulation relation is proposed to deal with uncertainty. Third, an elaborate motion planning example is added in the simulation section.

The remainder of this paper is organized as follows. In Section 2, notation and preliminaries on system properties are provided. The new stability notion and the construction of symbolic morels are presented in Section 3. In Section 4, an application to incrementally quadratic nonlinear systems is provided. Two illustrative examples are given in Section 5 and Section 6 concludes the paper.

2 Preliminaries

2.1 Notation

Let $\mathbb{R} := (-\infty, \infty)$, $\mathbb{R}_{\geq 0} := [0, \infty)$, $\mathbb{R}_{>0} := (0, \infty)$, $\mathbb{Z}_{>0} := \{1, 2, \ldots\}$ and $\mathbb{Z}_{\geq 0} := \{0, 1, 2, \ldots\}$. Denote $\mathbb{R}^n$ as the n-dimensional real vector space, $\mathbb{R}^{n\times m}$ as the $n \times m$ real matrix space. I_n is the identity matrix of order n and 1_n is the column vector of order n with all entries equal to one. $0_{n\times m}$ is the $n \times m$ matrix with all elements equal to 0. When there is no ambiguity, we use 0 to represent a matrix with proper dimensions and all its elements equal to 0. $[a, b]$ and $[a, b[$ denote closed and right half-open intervals with end points a and b. For $x_1 \in \mathbb{R}^{n_1}, \ldots, x_m \in \mathbb{R}^{n_m}$, the notation $(x_1, x_2, \ldots, x_m) \in \mathbb{R}^{n_1+n_2+\cdots+n_m}$ stands for $[x_1^T, x_2^T, \ldots, x_m^T]^T$. Let $|\lambda|$ be the absolute value of a real number λ, and $\|x\|$ and $\|A\|$ be the Euclidean norm of vector x and matrix A, respectively. Given a function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}^n$, the supremum of f is denoted by $\|f\|_\infty$, which is given by $\|f\|_\infty := \sup\{\|f(t)\|, t \geq 0\}$ and $\|f\|_{[0,\tau)} := \sup\{\|f(t)\|, t \in [0, \tau)\}$. A function f is called bounded if $\|f\|_\infty < \infty$. Given a set S, the interior of S is denoted by int(S), the boundary of S is denoted by $F_r(S)$ and the power set of S is denoted by 2^S. Given two sets S_1, S_2, the notation $S_1 \setminus S_2 := \{x | x \in S_1 \wedge x \notin S_2\}$ stands for the set difference, where $\wedge$ represents the logic operator AND.

A continuous function $\gamma : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is said to belong to class $\mathcal{K}$ if it is strictly increasing and $\gamma(0) = 0$; γ is said to belong to class $\mathcal{K}_\infty$ if $\gamma \in \mathcal{K}$ and $\gamma(r) \to \infty$ as $r \to \infty$. A continuous function $\beta : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is said to belong to class $\mathcal{KL}$ if for each fixed s, the map

$\beta(r,s)$ belongs to class $\mathcal{K}_\infty$ with respect to r and, for each fixed r, the map $\beta(r,s)$ is decreasing with respect to s and $\beta(r,s) \to 0$ as $s \to \infty$. For a set $\mathcal{A} \subseteq \mathbb{R}^n$ and any $x \in \mathbb{R}^n$, we denote by, $\mathrm{d(x,\mathcal{A})}$, the point-to-set distance, defined as $\mathrm{d(x,\mathcal{A})} = \inf_{\mathrm{y}\in\mathcal{A}}\{\|\mathrm{x}-\mathrm{y}\|\}$.

2.2 System properties

Consider a continuous-time uncertain nonlinear system of the form

$$\Sigma : \begin{cases} \dot{x}_1(t) = f(t, x_1(t), u(t), w(t)) \\ y_1(t) = h(x_1(t)), \end{cases} \tag{1}$$

where $x_1(t) \in \mathbb{R}^n, y_1(t) \in \mathbb{R}^l, u(t) \in U \subseteq \mathbb{R}^m$, $w(t) \in W \subseteq \mathbb{R}^{n_w}$ are the state, output, control input, and external disturbance at time t, respectively. The input and disturbance are constrained to sets U and W, respectively. We assume that $f : [0,\infty)\times\mathbb{R}^n\times U\times\mathbb{R}^{n_w} \to \mathbb{R}^n$ is piecewise continuous in t, continuous in x_1, u and w, and the vector field f is such that for any input in U, any disturbance in W, and any initial condition $x_1(0) \in \mathbb{R}^n$, this differential equation has a unique solution. Throughout the paper, we will refer to Σ as the concrete system, that is the system that we actually want to control.

Let $\mathcal{U}$ be the set of all functions that take their values in U and are defined on $\mathbb{R}_{\geq 0}$. Similarly, one can define $\mathcal{W}$ as the set of all functions that take their values in W and are defined on $\mathbb{R}_{\geq 0}$. Given an input signal $u \in \mathcal{U}$, we use the notation $\mathrm{dom}(u)$ to represent the domain of u.

A curve $\xi : [0,\tau[\to \mathbb{R}^n$ is said to be a trajectory of Σ if there exists an input signal $u \in \mathcal{U}$ and a disturbance signal $w \in \mathcal{W}$ satisfying $\dot{\xi}(t) = f(t, \xi(t), u(t), w(t))$ for almost all $t \in [0,\tau[$. A curve $\zeta : [0,\tau[\to \mathbb{R}^l$ is said to be an output trajectory of Σ if $\zeta(t) = h(\xi(t))$ for almost all $t \in [0,\tau[$, where ξ is a trajectory of Σ. We use $\xi(\xi_0, u, w, t)$ to denote the trajectory point reached at time t under the input signal $u \in \mathcal{U}$ and the disturbance signal $w \in \mathcal{W}$ from initial state ξ_0.

The deterministic system is defined as

$$\Sigma_d : \begin{cases} \dot{x}_1(t) = f_d(t, x_1(t), u(t)) \\ y_1(t) = h(x_1(t)), \end{cases} \tag{2}$$

where the function $f_d : [0,\infty)\times\mathbb{R}^n\times U \to \mathbb{R}^n$ represents the deterministic dynamics of the concrete system (1), i.e., $f_d(t, x(t), u(t)) = f(t, x(t), u(t), w(t))$ if $w(t) = 0$. We use $\xi_d(\xi_0, u, t)$ to denote the trajectory point of (2) reached at time t under the input signal $u \in \mathcal{U}$ from initial state ξ_0.

Definition 2.1 *[3] A (deterministic) system is called forward complete (FC) if for every initial condition $x_0 \in \mathbb{R}^n$ and every input signal $u \in \mathcal{U}$, the corresponding solution is defined for all $t \geq 0$.*

By a minor modification of the statement of Definition 2.1, one can define FC for uncertain systems.

Definition 2.2 *The uncertain system (1) is called FC if for every initial condition $x_1(0) \in \mathbb{R}^n$, every input signal $u \in \mathcal{U}$, and every disturbance signal $w \in \mathcal{W}$, the corresponding solution is defined for all $t \geq 0$.*

The following definition of ε-closeness characterizes the closeness between two (output) trajectories.

Definition 2.3 ([15], Definition 4.13) *Given $\varepsilon > 0$, two output trajectories $\zeta_1 : [0,\infty) \to \mathbb{R}^l$ and $\zeta_2 : [0,\infty) \to \mathbb{R}^l$ are ε-close if*

$$\|\zeta_1(t) - \zeta_2(t)\| \leq \varepsilon, \forall t \in [0,\infty).$$

Lemma 2.1 ([16]) *Let $V : [0,\infty)\times\mathbb{R}^n \to \mathbb{R}$ be a continuously differentiable function such that*

$$\begin{aligned} \underline{\alpha}(\|x\|) \leq V(t,x) \leq \bar{\alpha}(\|x\|) \\ \frac{\partial V}{\partial t} + \frac{\partial V}{\partial x} g(t,x,u) \leq -\gamma V(t,x), \quad \forall \|x\| \geq \mu > 0, \end{aligned} \tag{3}$$

$\forall (t,x,u) \in [0,\infty)\times\mathbb{R}^n\times\mathbb{R}^m$, where $\underline{\alpha}$ and $\bar{\alpha}$ are class $\mathcal{K}_\infty$ functions, and $\mu > 0$ and $\gamma > 0$ are constants. Then, the solution $x(t)$ to the differential equation $\dot{x}(t) = g(t, x(t), u(t))$ satisfies

$$\|x(t)\| \leq \beta(\|x(0)\|, t) + \underline{\alpha}^{-1}(\bar{\alpha}(\mu)),$$

where

$$\beta(r,t) = \underline{\alpha}^{-1}(e^{-\gamma t}\bar{\alpha}(r))$$

is a class $\mathcal{KL}$ function.

Proof: First, let us assume $\|x(0)\| > \mu$. There are two possibilities. 1. $\|x(t)\| > \mu, \forall t \geq 0$. Then, one has that (3) holds $\forall t \geq 0$. One can thus derive that $\forall t \geq 0$, $V(t,x) \leq e^{-\gamma t}V(0,x(0)) \leq e^{-\gamma t}\bar{\alpha}(\|x(0)\|)$ and

$$\|x(t)\| \leq \underline{\alpha}^{-1}(V(t,x(t))) \leq \underline{\alpha}^{-1}(e^{-\gamma t}\bar{\alpha}(\|x(0)\|)). \tag{4}$$

2. There exists a time instant $\tau > 0$ such that $\|x(\tau)\| = \mu$. Let $t_1 = \min_{\tau>0}\{\|x(\tau)\| = \mu\}$. Then one has that $\|x(t)\| \geq \mu, \forall t \in [0, t_1]$, and thus (4) holds $\forall t \in [0, t_1]$. For $t \in (t_1,\infty)$, one has either that $\|x(t)\| < \mu, \forall t \in (t_1,\infty)$ or that there exists a time instant $\tau \in (t_1,\infty)$ such that $\|x(\tau)\| = \mu$. Let $t_2 = \min_{\tau>t_1}\{\|x(\tau)\| = \mu\}$. Then one has that $\|x(t)\| \leq \mu, \forall t \in (t_1, t_2]$. For $t \in (t_2,\infty)$, there are also two possibilities. If $\|x(t)\| > \mu, \forall t \in (t_2,\infty)$, then one has that (3) holds $\forall t \in (t_2,\infty)$, and thus

$$\|x(t)\| \leq \underline{\alpha}^{-1}(e^{-\gamma(t-t_2)}\bar{\alpha}(\|x(t_2)\|)) \leq \underline{\alpha}^{-1}(\bar{\alpha}(\mu)). \tag{5}$$

Otherwise, there exists a time instant $\tau > t_2$ such that $\|x(\tau)\| = \mu$. Let $t_3 = \min_{\tau>t_2}\{\|x(\tau)\| = \mu\}$. Then one has that (5) holds $\forall t \in (t_2, t_3]$. Repeating the above analysis, one can conclude that

$$\|x(t)\| \leq \underline{\alpha}^{-1}(e^{-\gamma t}\bar{\alpha}(\|x(0)\|)) + \underline{\alpha}^{-1}(\bar{\alpha}(\mu)), \forall t \geq 0.$$

For other case, i.e., $\|x(0)\| \leq \mu$, the proof can be conducted in a similar manner. Therefore, the conclusion follows. □

3 Main results

3.1 η-approximately controlled globally practically stable

In this paper, the abstraction technique developed in [12] is applied, in which the state-space $\mathbb{R}^n$ is approximated by the lattice

$$[\mathbb{R}^n]_\eta = \left\{q \in \mathbb{R}^n | q_i = k_i \frac{2\eta}{\sqrt{n}}, k_i \in \mathbb{Z}, i = 1, \ldots, n\right\}, \tag{6}$$

where $\eta \in \mathbb{R}_{\geq 0}$ is a state-space discretization parameter. Define the associated quantizer $Q_\eta : \mathbb{R}^n \to [\mathbb{R}^n]_\eta$ as $Q_\eta(x) = q$ if and only if $|x_i - q_i| \leq \eta/\sqrt{n}, \forall i = 1, \ldots n$. Then, one has $\|x - Q_\eta(x)\| \leq \eta, \forall x \in \mathbb{R}^n$.

The abstract system is obtained by applying the state abstraction (6) to the deterministic system (2), and is given by

$$\Sigma' : \begin{cases} x_2(t) = Q_\eta(\hat{x}_2(t)), \\ \dot{\hat{x}}_2(t) = f_d(t, \hat{x}_2(t), v(t)), \\ y_2(t) = h(x_2(t)), \end{cases} \tag{7}$$

where $x_2(t) \in [\mathbb{R}^n]_\eta, y_2(t) \in \mathbb{R}^l$ and $v(t) \in U'$ represent respectively the state, output, and control input of the abstract system. The systems Σ and Σ' have the same output space (i.e., $\mathbb{R}^l$), but different state and input spaces. We note that the input set U' of the abstract system Σ' is a design parameter that will be specified later.

Remark 3.1 *The abstract system Σ' is obtained in two steps. First, the concrete (uncertain) system Σ is abstracted by its deterministic counterpart Σ_d, i.e., $\dot{\hat{x}}_2(t) = f_d(t, \hat{x}_2(t), v(t))$. Then, we apply the state abstraction (6) to the deterministic system Σ_d, i.e., $x_2(t) = Q_\eta(\hat{x}_2(t))$. Note that the state variable $x_2(t)$ is neither continuous nor differentiable due to the state-space discretization.*

Remark 3.2 *The abstraction construction in this work is different from [20, 35]. In [20, 35], the abstraction construction involves both state- and time-space discretization. In this work, only state-space discretization is considered. In addition, the abstract models in [20, 35] are over-approximations of the concrete system in the sense that, under a given control signal, the transitions in the abstract models capture all possible behaviors of the concrete system. However, in this work, no over-approximation is needed when constructing the abstract system.*

Let $\mathcal{U}'$ be the set of all functions that take their values in U' and are defined on $\mathbb{R}_{\geq 0}$. A (hybrid) curve $\xi' : [0, \tau[\to [\mathbb{R}^n]_\eta$ is said to be a trajectory of Σ' if there exists $v \in \mathcal{U}'$ satisfying $\xi'(t) = Q_\eta(\xi(t)), \forall t \in [0, \tau[$, where $\dot{\xi}(t) = f_d(t, \xi(t), v(t))$ and $\xi(0) = \xi'(0)$. A curve $\zeta' : [0, \tau[\to \mathbb{R}^l$ is said to be an output trajectory of Σ' if $\zeta'(t) = h(\xi'(t))$, for almost all $t \in [0, \tau[$, where ξ' is a trajectory of Σ'. With a little abuse of notation, we use $\xi'(\xi'_0, v, t)$ to denote the trajectory point of Σ' reached at time t under the input signal $v \in \mathcal{U}'$ from an initial state $\xi'_0 \in [\mathbb{R}^n]_\eta$.

The control input $u(t)$ of the concrete system (1) will be synthesized hierarchically via the abstract system (7) with a control interface $u_v : \mathbb{R}^m \times \mathbb{R}^n \times [\mathbb{R}^n]_\eta \to \mathbb{R}^m$, which is given by

$$u(t) = u_v(v(t), x_1(t), x_2(t)). \tag{8}$$

Define

$$\hat{X}_0 := \{(x_1, x_2) | x_1 \in \mathbb{R}^n, x_2 \in [\mathbb{R}^n]_\eta, \|x_1 - x_2\| \leq \eta\}. \tag{9}$$

To guarantee that the synthesized controller $u(t)$ is applicable to the concrete system (1), it is necessary that $u(t) = u_v(v(t), x_1(t), x_2(t)) \in U, \forall t \in \mathrm{dom}(u)$. Therefore, we propose the following definition.

Definition 3.1 *The control interface $u_v : \mathbb{R}^m \times \mathbb{R}^n \times [\mathbb{R}^n]_\eta \to \mathbb{R}^m$ is called* admissible *if there exists an input set $U' \neq \emptyset$ such that*

$$u(t) = u_v(v(t), \xi(\xi_0, u_v, w, t), \xi'(\xi'_0, v, t)) \in U$$

$\forall t \in dom(u), \forall(\xi_0, \xi'_0) \in \hat{X}_0, \forall v \in \mathcal{U}', \forall w \in \mathcal{W}$. In this case, the input set U' is called admissible *to u_v.*

Next, we introduce the following stability notion, which will be used for the construction of symbolic models.

Definition 3.2 *Given the concrete system Σ in (1) and the abstract system Σ' in (7). The system pair (Σ, Σ') is called* η-approximately controlled globally practically stable (η-CGPS) *if it is FC and there exist an admissible control interface u_v, a $\mathcal{KL}$ function β, and $\mathcal{K}_\infty$ functions γ_1, γ_2 such that $\forall t \in \mathbb{R}_{\geq 0}$, $\forall(x_0, x'_0) \in \hat{X}_0, \forall v \in \mathcal{U}', \forall w \in \mathcal{W}$, the following condition is satisfied:*

$$\|\xi(x_0, u_v, w, t) - \xi'(x'_0, v, t)\| \leq \beta(\|x_0 - x'_0\|, t) + \gamma_1(\eta) + \gamma_2(\|w\|_\infty).$$

Moreover, u_v is called an interface *for (Σ, Σ'), associated to the η-*CGPS *property.*

Remark 3.3 *According to Definitions 3.1-3.2, a general idea on determining the admissible control interface and the associated input set U' can be provided as follows: firstly, ignore the input constraint for the concrete system (1) by assuming that $U = \mathbb{R}^m$ (in this way, any control interface that maps to $\mathbb{R}^m$ is admissible), and find one or several control interfaces u_v such that (Σ, Σ') is η-*CGPS*. Secondly, taking the real input set U into account, refine the control interfaces obtained in the previous step in a way that the admissible ones and the associated input sets are kept.*

Remark 3.4 *We note that the notion of η-CGPS defined in Definition 3.2 is essentially different from the notion of incrementally input-to-state stable (δ-ISS) given in [4], Definition 4.1 or incrementally forward completeness (δ-FC) given in [35], Definition 2.4. Both δ-ISS and δ-FC are properties defined on the concrete system Σ while η-CGPS is a property defined on the system pair (Σ, Σ'). Moreover, for the concrete system that is not δ-ISS, the η-CGPS property can still hold for the corresponding system pair. Another difference between δ-FC in [35] and η-CGPS is that the β function belongs to class $\mathcal{K}_\infty$ in the Definition of δ-FC while class $\mathcal{KL}$ in Definition 3.2.*

In the following, the Lyapunov function characterization of the stability notion η-CGPS is proposed, which is motivated by [11].

Definition 3.3 *Given the concrete system Σ in (1), the abstract system Σ' in (7), a continuously differentiable function $V : [0, \infty) \times \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_{\geq 0}$, and a control interface u_v. Function V is called a η-*CGPS Lyapunov function *for (Σ, Σ') and u_v is the associated control interface if there exist $\mathcal{K}_\infty$ functions $\underline{\alpha}, \bar{\alpha}, \sigma_1, \sigma_2$, and a constant $\mu > 0$ such that:*

i) $\forall t \in \mathbb{R}_{\geq 0}, \forall x, x' \in \mathbb{R}^n$,

$$\underline{\alpha}(\|x - x'\|) \leq V(t, x, x') \leq \bar{\alpha}(\|x - x'\|); \tag{10}$$

ii) $\forall t \in \mathbb{R}_{\geq 0}, \forall x, x' \in \mathbb{R}^n, \forall v \in U'$, *and* $\forall w \in W$,

$$\frac{\partial V}{\partial x}\{f(t, x, u_v(v, x, Q_\eta(x')), w)\} + \frac{\partial V}{\partial x'} f_d(t, x', v) + \frac{\partial V}{\partial t} \leq -\mu V(t, x, x') + \sigma_1(\eta) + \sigma_2(\|w\|). \tag{11}$$

Then, we can derive the following theorem.

Theorem 3.1 *Given the concrete system Σ in (1) and the abstract system Σ' in (7). If i) Σ is FC, ii) there exists a η-*CGPS Lyapunov function *for (Σ, Σ') and with u_v being the associated control interface, and iii) u_v is* admissible*, then, (Σ, Σ') is η-*CGPS *and u_v is the* interface *for (Σ, Σ'), associated to the η-*CGPS *property.*

Proof: Let V be the η-CGPS Lyapunov function for (Σ, Σ') and u_v the associated control interface. Then, one has (11) holds and thus

$$\begin{aligned}&\frac{\partial V}{\partial x_1}\{f(t, x_1, u_v(v, x_1, Q_\eta(\hat{x}_2)), w)\} + \frac{\partial V}{\partial \hat{x}_2} f_d(t, \hat{x}_2, v) + \frac{\partial V}{\partial t}\\ &\quad\leq -\mu V(t, x_1, \hat{x}_2) + \sigma_1(\eta) + \sigma_2(\|w\|).\end{aligned}$$

Define $\nu := \sup_{t\geq 0}\{\sigma_1(\eta) + \sigma_2(\|w(t)\|)\} = \sigma_1(\eta) + \sigma_2(\|w\|_\infty)$. Then, one has that

$$\begin{aligned}&\frac{\partial V}{\partial x_1}\{f(t, x_1, u_v(v, x_1, Q_\eta(\hat{x}_2)), w)\} + \frac{\partial V}{\partial \hat{x}_2} f_d(t, \hat{x}_2, v) + \frac{\partial V}{\partial t}\\ &\quad\leq -\frac{\mu}{2} V(t, x_1, \hat{x}_2) - \frac{\mu}{2} V(t, x_1, \hat{x}_2) + \sigma_1(\eta) + \sigma_2(\|w\|)\\ &\quad\leq -\frac{\mu}{2} V(t, x_1, \hat{x}_2)\end{aligned}$$

for all $\|x_1 - \hat{x}_2\| \geq \underline{\alpha}^{-1}(2\nu/\mu)$. According to Lemma 2.1, one can further have

$$\begin{aligned}\|x_1(t) - \hat{x}_2(t)\| &\leq \underline{\alpha}^{-1}(e^{-\frac{\mu}{2}t}\bar{\alpha}(\|x_1(0) - \hat{x}_2(0)\|))\\ &\quad + \underline{\alpha}^{-1}(\bar{\alpha}(\underline{\alpha}^{-1}(2\nu/\mu))).\end{aligned} \tag{12}$$

Moreover, one has from (7) that $\|x_2(t) - \hat{x}_2(t)\| = \|Q_\eta(\hat{x}_2(t)) - \hat{x}_2(t)\| \leq \eta, \forall t$. Thus,

$$\begin{aligned}&\|x_1(t) - x_2(t)\|\\ \leq&\|x_1(t) - \hat{x}_2(t)\| + \|\hat{x}_2(t) - x_2(t)\|\\ \leq&\underline{\alpha}^{-1}(e^{-\frac{\mu}{2}t}\bar{\alpha}(\|x_1(0) - x_2(0)\|)) + \underline{\alpha}^{-1}(\bar{\alpha}(\underline{\alpha}^{-1}(2\nu/\mu))) + \eta\\ \leq&\underline{\alpha}^{-1}(e^{-\frac{\mu}{2}t}\bar{\alpha}(\|x_1(0) - x_2(0)\|)) + \underline{\alpha}^{-1}(\bar{\alpha}(\underline{\alpha}^{-1}(4\sigma_1(\eta))))\\ &+ \eta + \underline{\alpha}^{-1}(\bar{\alpha}(\underline{\alpha}^{-1}(4\sigma_2(\|w\|_\infty))/\mu))).\end{aligned}$$

Combining the fact that u_v is admissible, one can conclude that (Σ, Σ') is η-CGPS and u_v is the interface for (Σ, Σ'), associated to the η-CGPS property. □

3.2 Construction of symbolic models

In this subsection, the construction of symbolic models for the concrete system (1) is considered. Firstly, the notion of robust approximate (bi)simulation relation is proposed.

Definition 3.4 *Given the concrete system Σ in (1) and the abstract system Σ' in (7). Let $\varepsilon > 0$ be a given precision and $\tilde{\varepsilon} \geq 0$. We say that Σ* robustly approximately simulates Σ' with parameters $(\varepsilon, \tilde{\varepsilon})$, denoted by $\Sigma' \preceq_{\mathcal{S}}^{(\varepsilon,\tilde{\varepsilon})} \Sigma$, *if:*

i) $\forall x'_0 \in [\mathbb{R}^n]_\eta, \exists x_0 \in \mathbb{R}^n$ *such that* $(x_0, x'_0) \in \hat{X}_0$, *ii)* $\forall (x_0, x_0') \in \hat{X}_0$, $\forall v \in \mathcal{U}', \exists u \in \mathcal{U}$ *such that* $\forall t \geq 0$,

$$\|h(\xi(x_0, u, w, t)) - h(\xi'(x_0', v, t))\| \leq \varepsilon, \forall w : \|w\|_\infty < \tilde{\varepsilon},$$

where $\hat{X}_0$ *is defined in (9).*

The systems Σ *and* Σ' *are then said to be* robust approximately bisimilar with parameters $(\varepsilon, \tilde{\varepsilon})$, denoted by $\Sigma \cong_{\mathcal{S}}^{(\varepsilon,\tilde{\varepsilon})} \Sigma'$, *if* $\Sigma \preceq_{\mathcal{S}}^{(\varepsilon,\tilde{\varepsilon})} \Sigma'$ *and* $\Sigma' \preceq_{\mathcal{S}}^{(\varepsilon,\tilde{\varepsilon})} \Sigma$.

Remark 3.5 *Item ii) of Definition 3.4 guarantees that for every output trajectory* ζ' *in the abstract system* Σ'*, there exists an output trajectory* ζ *in the concrete system* Σ *such that* ζ' *and* ζ *are* ε*-close (despite the worst disturbance signals). Therefore, for a given specification, e.g., a safety and reachability specification* S*, if one can find an output trajectory in* Σ' *such that* S' *(*S' *is obtained by enlarging all the unsafe sets by* ε *and shrinking all the target sets by* ε*) is satisfied, then one can always find an output trajectory in* Σ *such that* S *is satisfied under all possible disturbances.*

Before proceeding, we need the following additional assumption.

Assumption 3.1 *The output function* $h : \mathbb{R}^n \to \mathbb{R}^l$ *is globally Lipschitz continuous with Lipschitz constant* ρ *on the set* X_ε*. That is,*

$$\|h(x_1) - h(x_2)\| \leq \rho\|x_1 - x_2\|, \forall (x_1, x_2) \in X_\varepsilon,$$

where $X_\varepsilon := \{(x_1, x_2) : \|x_1 - x_2\| \leq \underline{\alpha}^{-1}(\bar{\alpha}(\varepsilon)) + \underline{\alpha}^{-1}\big((\sigma_1(\varepsilon) + \max_{w\in\mathcal{W}}\{\sigma_2(\|w\|_\infty)\})/\mu\big) + \varepsilon\}$, $\underline{\alpha}, \bar{\alpha}, \sigma_1, \sigma_2, \mu$ *are defined in Definition 3.3,* $\mathcal{W}$ *is the set of disturbance signals, and* ε *is the desired precision.*

Assumption 3.1 is not conservative since it only requires Lipschitz continuity within a neighborhood of x_1, the radius of which is determined by the desired precision ε. Note that the Lipschitz constant ρ is independent of ε. Then, we can get the following result.

Theorem 3.2 *Given the concrete system* Σ *in (1) and the abstract system* Σ' *in (7). Let* $\varepsilon > 0$ *be the desired precision. Suppose Assumption 3.1 holds. Assume that there exists a* η-CGPS Lyapunov function V *for* (Σ, Σ') *and let* u_v *be the associated control interface that is* admissible. *If furthermore, one has that* $\|w\|_\infty < \tilde{\varepsilon} := \sigma_2^{-1}(\mu\underline{\alpha}(\bar{\alpha}^{-1}(\underline{\alpha}(\varepsilon/\rho)))/4), \forall w \in \mathcal{W}$*; then,* $\Sigma' \preceq_{\mathcal{S}}^{(\varepsilon,\tilde{\varepsilon})} \Sigma$ *if*

$$\begin{aligned}\underline{\alpha}^{-1}(\bar{\alpha}(\eta)) + \eta + \underline{\alpha}^{-1}\left(\bar{\alpha}\left(\underline{\alpha}^{-1}\left(\frac{4\sigma_1(\eta)}{\mu}\right)\right)\right)& \\ < \frac{\varepsilon}{\rho} - \underline{\alpha}^{-1}\left(\bar{\alpha}\left(\underline{\alpha}^{-1}\left(\frac{4\sigma_2(\|w\|_\infty)}{\mu}\right)\right)\right)&.\end{aligned} \quad (13)$$

Proof: By definition of $[\mathbb{R}^n]_\eta$, for all $x_0 \in \mathbb{R}^n$, there exists $x_0' \in [\mathbb{R}^n]_\eta$ such that $\|x_0 - x_0'\| \leq \eta$. Then, one has from Assumption 3.1 that

$$\|h(x_0) - h(x_0')\| \leq \rho\|x_0 - x_0'\| \leq \varepsilon.$$

Hence, $(x_0, x_0') \in \hat{X}_0$. Item *i)* of Definition 3.4 holds.

Given $(x_0, x_0') \in \hat{X}_0$ and an input signal $v \in \mathcal{U}'$. Since the control interface u_v is admissible, then one has $u(t) = u_v(t, v(t), \xi(x_0, u_v, w, t), \xi'(x_0', v, t)) \in U, \forall t \in \mathrm{dom}(v)$. Thus, $u \in \mathcal{U}$. Let $q(t) = \xi(x_0', v, t))$. Then, one has $x_2(t) = \xi'(x_0', v, t) = Q_\eta(q(t)), \forall t \in \mathrm{dom}(v)$. Let also $x_1(t) = \xi(x_0, u_v, w, t))$, where u_v is the admissible control interface. To prove item *ii)* of Definition 3.4, it is sufficient to prove that $\|h(x_1(t)) - h(x_2(t)\| \leq \varepsilon, \forall t \in \mathrm{dom}(v)$.

Since V is a η-CGPS Lyapunov function for (Σ, Σ'), then (11) holds. One has from Theorem 3.1 that

$$\begin{aligned}\|x_1(t) - q(t)\| \leq\ & \underline{\alpha}^{-1}(e^{-\frac{\mu}{2}t}\bar{\alpha}(\|x_1(0) - q(0)\|)) \\ & + \underline{\alpha}^{-1}(\bar{\alpha}(\underline{\alpha}^{-1}(4\sigma_1(\eta)/\mu))) \\ & + \underline{\alpha}^{-1}(\bar{\alpha}(\underline{\alpha}^{-1}(4\sigma_2(\|w\|_\infty))/\mu))).\end{aligned}$$

In addition, $\|x_1(0) - q(0)\| = \|\xi(0) - \xi'(0)\| = \|x_0 - x_0'\| \leq \eta$. Using (13), one can further get

$$\begin{aligned}\|x_1(t) - x_2(t)\| &\leq \|x_1(t) - q(t)\| + \|q(t) - x_2(t)\| \\ &= \|x_1(t) - q(t)\| + \|q(t) - Q_\eta(q(t))\| \\ &\leq \varepsilon/\rho,\end{aligned}$$

and thus $\|h(x_1(t)) - h(x_2(t))\| \leq \rho\|x_1(t) - x_2(t)\| \leq \varepsilon$. Item *ii)* of Definition 3.4 holds and thus $\Sigma' \preceq_{\mathcal{S}}^{(\varepsilon,\tilde{\varepsilon})} \Sigma$. □

Remark 3.6 *In Theorem 3.2, one can further deduce that* $\Sigma' \cong_{\mathcal{S}}^{(\varepsilon,\tilde{\varepsilon})} \Sigma$ *if the input set of* Σ *is unbounded (i.e.,* $U = \mathbb{R}^n$*) or if the control interface can be designed as* $u(t) = u_v(v(t), x_1(t), x_2(t)) = v(t), \forall t \geq 0$ *(e.g., for incrementally stable systems).*

Remark 3.7 *The construction of symbolic models and the implementation of the admissible control interface rely on the computation of the state-space abstraction and the abstract controller. For different systems, computational tools have been developed for this purpose, e.g., PESSOA [22], SCOTS [29], and LTLCon [18].*

Remark 3.8 *One key step for the construction of symbolic models is to find an admissible control interface. From Definition 3.1, one can see that for a control interface* u_v *to be admissible, the key factor is to find an input map* U' *admissible to* u_v*. When the input set for the concrete system is unbounded, i.e.,* $U = \mathbb{R}^m$*, any control interface that maps to* $\mathbb{R}^m$ *is admissible. However, in practical applications, input saturations are common constraints. We note that when the input set for the concrete system is bounded, it is not always possible to find* *an admissible control interface. The good news is that, for a certain class of incrementally quadratic nonlinear systems, we show in the next section that it is possible to construct an admissible control interface u_v, such that Σ robustly approximately simulates Σ'.*

4 Incrementally quadratic nonlinear systems

In this section, we consider a class of perturbed incrementally quadratic nonlinear systems [8], for which the systematic construction of the admissible control interface and robust approximate symbolic models is possible. This kind of nonlinear systems are very useful and include many commonly encountered nonlinearities, such as the global Lipschitz nonlinearity, as special cases. In addition, many practical applications, such as vehicle models, manipulators, and electrical power convertors, are incrementally quadratic nonlinear systems.

Consider the nonlinear time-varying system described by

$$\Sigma_1 : \begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + Ep(t, C_q x + D_q p) + w(t) \\ y(t) = Cx(t), \end{cases} \tag{14}$$

where $x(t) \in \mathbb{R}^n, y(t) \in \mathbb{R}^l$, $u(t) \in U \subseteq \mathbb{R}^m$, and $w(t) \in W \subset \mathbb{R}^n$ are the state, output, control input, and external disturbance, respectively, $p : \mathbb{R}_{\geq 0} \times \mathbb{R}^{l_p} \to \mathbb{R}^{l_e}$ represents the known continuous nonlinearity of the system, and A, B, C, E, C_q, D_q are constants matrices of appropriate dimensions.

Definition 4.1 *[1] Given a function $p : \mathbb{R}_{\geq 0} \times \mathbb{R}^{l_p} \to \mathbb{R}^{l_e}$, a symmetric matrix $M \in \mathbb{R}^{(l_p+l_e)\times(l_p+l_e)}$ is called an incremental multiplier matrix for p if it satisfies the following incremental quadratic constraint for any $q_1, q_2 \in \mathbb{R}^{l_p}$:*

$$\begin{bmatrix} q_2 - q_1 \\ p(t, q_2) - p(t, q_1) \end{bmatrix}^T M \begin{bmatrix} q_2 - q_1 \\ p(t, q_2) - p(t, q_1) \end{bmatrix} \geq 0. \tag{15}$$

Remark 4.1 *The incremental quadratic constraint (15) includes a broad class of nonlinearities as special cases. For instance, the globally Lipschitz condition, the sector bounded nonlinearity, and the positive real nonlinearity $p^T Sq \geq 0$ for some symmetric, invertible matrix S. Some other nonlinearities that can be expressed using the incremental quadratic constraint were discussed in [1, 8], such as the case when the Jacobian of p with respect to q is confined in a polytope or a cone.*

Assumption 4.1 *There exist matrices $P = P^T \succ 0, L$ and a scalar $\alpha > 0$ such that the following matrix inequality*

$$\begin{bmatrix} P(A+BL) + (A+BL)^T P + 2\alpha P & PE \\ E^T P & 0 \end{bmatrix} + \begin{bmatrix} C_q & D_q \\ 0 & I \end{bmatrix}^T M \begin{bmatrix} C_q & D_q \\ 0 & I \end{bmatrix} \leq 0 \tag{16}$$

is satisfied, where $M = M^T$ is an incremental multiplier matrix for function p.

Remark 4.2 *The matrix inequality (16) is not a LMI. Hence, one can not solve for P, L reliably via, e.g., the interior point method algorithms. However, we note that parameterization methods, such as block diagonal parameterization [1] can be utilized to transform (16) into Ricatti equations and/or LMIs under certain conditions. Moreover, we note that several necessary and/or sufficient conditions have been provided in [1, 8] to guarantee the existence of solutions to (16).*

The abstract system (obtained by applying the state-space discretization (6)) is given by

$$\Sigma_1' : \begin{cases} \xi(t) = Q_\eta(\hat{\xi}(t)) \\ \dot{\hat{\xi}}(t) = A\hat{\xi}(t) + Bv(t) + Ep(t, C_q\hat{\xi} + D_q p), \\ \zeta(t) = C\xi(t), \end{cases} \tag{17}$$

where $v(t) \in U'$.

According to Remark 3.3, we first ignore the input constraint for the concrete system (14) by assuming that $U = \mathbb{R}^m$. The control interface $u_v : \mathbb{R}^m \times \mathbb{R}^n \times [\mathbb{R}^n]_\eta \to \mathbb{R}^m$ is then designed as

$$u_v(v(t), x(t), \xi(t)) = v(t) + L(x(t) - \xi(t)), \tag{18}$$

where L is the solution of (16). One can verify that u_v is admissible by letting $U' = \mathbb{R}^m$. Then, we get the following result.

Theorem 4.1 *Consider the concrete system (14) with the input set $U = \mathbb{R}^m$ and the abstract system (17). Let $\varepsilon > 0$ be the desired precision. The input $u(t)$ of (14) is synthesized by the control interface (18). Suppose that Assumption 4.1 holds and the disturbance set W satisfies $\|w\|_\infty < \tilde{\varepsilon} := \alpha\varepsilon\sqrt{\lambda_{\min}(P)}/(2\|c\|\sqrt{\lambda_{\max}(P)}), \forall w \in \mathcal{W}$; then, $\Sigma_1' \preceq_{\mathcal{S}}^{(\varepsilon,\tilde{\varepsilon})} \Sigma_1$ if the state-space discretization parameter η satisfies*

$$\eta \leq \left(\frac{\varepsilon}{\|C\|} - \frac{2\sqrt{\lambda_{\max}(P)}\|w\|_\infty}{\alpha\sqrt{\lambda_{\min}(P)}} \right) \frac{\alpha\sqrt{\lambda_{\min}(P)}}{\alpha\sqrt{\lambda_{\min}(P)} + \sqrt{\alpha^2\lambda_{\max}(P) + 2\|\hat{L}\|}},$$

where $\hat{L} = L^T B^T PBL$ and P, L, α are the solution to (16).

Proof: Let $e(t) = \xi(t) - \hat{\xi}(t)$, then one has $\|e(t)\| \leq \eta, \forall t$. Define $\delta(t) = x(t) - \hat{\xi}(t)$. Then, from (14) and (17) one has

$$\begin{aligned}\dot{\delta}(t) =& A\delta(t) + BL(\delta(t) + e(t)) \\ &+ E(p(t, C_q x + D_q p) - p(t, C_q \hat{\xi} + D_q p)) + w(t) \\ =& A_c \delta(t) + BLe(t) + E\Phi_p(t, x, \hat{\xi}) + w(t),\end{aligned}$$

where $A_c = A + BL$ and

$$\Phi_p(t, x, \hat{\xi}) = p(t, C_q x + D_q p) - p(t, C_q \hat{\xi} + D_q p).$$

Post and pre multiplying both sides of inequality (16) by $(\delta(t), \Phi_p(t, x, \hat{\xi}))$ and its transpose and using condition (15) we obtain

$$\delta^T(t) P\dot{\delta}(t) \leq -\alpha\delta^T(t)P\delta(t) + \delta^T(t)PBLe(t) + \delta^T(t)Pw(t).$$

Consider the following Lyapunov function candidate

$$V(t, x, \hat{\xi}) = (x - \hat{\xi})^T P (x - \hat{\xi}).$$

Then, one has $\lambda_{\min}(P)\|x - \hat{\xi}\|^2 \leq V(t, x, \hat{\xi}) \leq \lambda_{\max}(P)\|x - \hat{\xi}\|^2$. Taking the derivative of V on t, one has

$$\begin{aligned}\dot{V}(t, x, \hat{\xi}) =& 2\delta^T(t)P\dot{\delta}(t) \\ \leq& -2\alpha\delta^T(t)P\delta(t) + 2\delta^T(t)PBLe(t) \\ &+ 2\delta^T(t)Pw(t) \\ \leq& -\alpha V(t, x, \hat{\xi}) + \frac{2}{\alpha}\|\hat{L}\|\eta^2 + \frac{2}{\alpha}\|P\|\|w(t)\|^2.\end{aligned} \tag{19}$$

Therefore, $V(t, x, \hat{\xi})$ is a valid η-CGPS Lyapunov function for (Σ_1, Σ_1'), where $\underline{\alpha}(x) = \lambda_{\min}(P)x^2, \bar{\alpha}(x) = \lambda_{\max}(P)x^2$, $\sigma_1(\eta) = 2\|\hat{L}\|\eta^2/\alpha$ and $\sigma_2(\|w\|_\infty) = 2\|P\|\|w\|_\infty^2/\alpha$. In addition, one can verify that Assumption 3.1 holds with $\rho = \|C\|$. Then, the conclusion follows from Theorem 3.2. □

Next, we will show how to find an input set U' admissible to u_v when the real input set U is considered.

From Theorem 4.1, we have (19) holds. Then, using the comparison principle, we can further get

$$\begin{aligned}&V(t, x(t), \hat{\xi}(t)) \\ \leq& e^{-\alpha t}V(t, x(0), \hat{\xi}(0)) + \frac{2\|\hat{L}\|\eta^2 + 2\|P\|\|w\|^2}{\alpha^2}(1 - e^{-\alpha t}) \\ \leq& \lambda_{\max}(P)\eta^2 + \frac{2\|\hat{L}\|\eta^2 + 2\|P\|\|w\|^2}{\alpha^2}.\end{aligned}$$

Then, one can further have

$$\|x(t) - \hat{\xi}(t)\| \leq \sqrt{\frac{V(t, x(t), \hat{\xi}(t))}{\lambda_{\min}(P)}} \leq K_1\eta + K_2\bar{w},$$

where $K_1 = \sqrt{\lambda_{\max}(P)/\lambda_{\min}(P) + 2\|\hat{L}\|/(\alpha^2\lambda_{\min}(P))}$, $K_2 = \sqrt{2\lambda_{\max}(P)/(\alpha^2\lambda_{\min}(P))}$, $\bar{w} = \max_{w\in\mathcal{W}}\{\|w\|_\infty\}$, and $\|x(t) - \xi(t)\| \leq \|x(t) - \hat{\xi}(t)\| + \|\hat{\xi}(t) - \xi(t)\| \leq (K_1 + 1)\eta + K_2\bar{w}$. Define $e_u(t) = u(t) - v(t)$. Then, one has

$$\begin{aligned}\|e_u(t)\| =& \|L(x(t) - \xi(t))\| \\ \leq& \|L\|((K_1 + 1)\eta + K_2\bar{w}).\end{aligned} \tag{20}$$

From (20), one can see that the norm of the relative error between $u(t)$ and $v(t)$, i.e., $\|e_u(t)\|$ is upper bounded, and the radius of the upper bound is determined by η and $\bar{w}$ (due to the special form of control interface that was designed in (18)). Let

$$\tilde{U} = \left\{z \in U | \mathrm{d}(z, F_r(U)) < \|L\|((K_1 + 1)\eta + K_2\bar{w})\right\},$$

be the set of points in U, whose distance to the boundary of U is less than $\|L\|((K_1 + 1)\eta + K_2\bar{w})$. Then, by choosing $U' = U \setminus \tilde{U}$, one can guarantee that $u(t) \in U, \forall v(t) \in U', \forall t \geq 0$. Moreover, we note that when Σ_1 is deterministic, i.e., $w(t) \equiv 0$, one can always find $U' \neq \emptyset$ for all $U, \mathrm{intU} \neq \emptyset$ since $U' \to U$ as $\eta \to 0$.

5 Simulation

In this section, two simulation examples are provided to validate the effectiveness of the theoretical results.

5.1 Example 1

Consider a mobile robot moving in $\mathbb{R}^2$, the dynamics of which is given by:

$$\Sigma_2 : \begin{cases}\dot{x}_1(t) = Ax_1(t) + Bu(t) + w(t) \\ y_1(t) = x_1(t),\end{cases} \tag{21}$$

where

$$A = \begin{bmatrix}0.2 & 0.3 \\ 0.5 & -0.5\end{bmatrix}, B = \begin{bmatrix}1 & 0 \\ 0 & 1\end{bmatrix}.$$

The input set $U = [-5, 5] \times [-5, 5]$ and the disturbance set $W = [-0.05, 0.05] \times [-0.05, 0.05]$. The problem is to drive the robot in the bounded workspace $\mathbb{W}$ shown in Fig. 1, where the three grey solid polygons O_1, O_2, O_3 represent obstacles and the three green solid polygons S_1, S_2, S_3 represent target regions. The goal of the motion planning problem consists in visiting all the three target regions S_1, S_2, S_3 infinitely many times while avoiding collision with the obstacles. This specification can be represented by a linear temporal logic (LTL) [6] formula $\phi = \mathsf{G}\mathbb{W} \wedge \mathsf{G}(\neg(O_1 \vee O_2 \vee O_3)) \wedge \mathsf{G}(\mathsf{F}S_1 \wedge \mathsf{F}S_2 \wedge \mathsf{F}S_3)$, where $\neg, \wedge, \vee$ are negation, logic 'AND', logic 'OR' operators, respectively, and G, F are temporal operators 'ALWAYS' and 'EVENTUALLY', respectively. The details about the syntax and semantics of LTL can be found in [6], Chapter 5.

Let the desired precision be $\varepsilon = 1$. The control interface is designed as

$$u_v(v(t), x(t), \xi(t)) = v(t) - \frac{1}{2} B^T P(x(t) - \xi(t)), \quad (22)$$

where P is the solution to the ARE $A^T P + PA - PBB^T P + I_2 = 0$. According to Theorem 4.1, the desired precision ε can be achieved by choosing the state-space discretization parameter $\eta = 0.15$. Then, by further choosing $U' = [-3.5, 3.5] \times [-3.5, 3.5]$, one can guarantee that the control interface (22) is admissible. The abstract system (obtained by applying the state-space abstraction (6)) is denoted by Σ_2' and the output of Σ_2' is denoted by y_2.

Using the LTL control synthesis toolbox LTLCon [18], we first synthesize a trajectory and the associated control policy for the abstract system Σ_2', which is shown by the red solid line in Fig. 1. One can see that any trajectory remaining within the distance 1 from this trajectory satisfies the problem specification. We note that in this example, the state-space abstraction is obtained in two steps: 1. The state-space is discretized based on the atomic propositions defined in the LTL formula ϕ. This step is the same as [18], and can be done using LTLCon. 2. We further discretize each state obtained in step 1 according to the state-space abstraction technique (6). We have added this step to LTLCon since it is not included there in [18].

The output trajectory y_1 of Σ_2 is obtained by applying the synthesized input for the abstract system Σ_2' via the control interface (22). Furthermore, in order to validate robustness, we run 100 realizations of the disturbance trajectories. The resulting trajectories for these 100 realizations are shown (by the solid blue line) in Fig. 1. One can see that all the trajectories satisfy the goal of the motion planning problem. The evolution of the output error $\|y_1 - y_2\|$ for the 100 realizations is depicted in Fig. 2, and one can see that the desired precision is preserved at all times. In addition, the evolution of the input components v_1, v_2 for the abstract system Σ_2' and the input components u_1, u_2 for the concrete system Σ_2 are plotted in Fig. 3, respectively. One can see that $u \in U$ (i.e., the input constraint is satisfied) at all times.

The desired precision is $\varepsilon = 1$ in this example while the simulation result in Fig. 2 shows that the output error

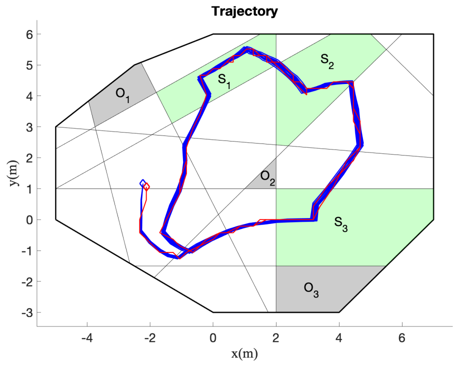

Fig. 1. Output trajectories of the concrete system Σ_2 (blue lines) for 100 realizations of disturbance signals and output trajectory of the abstract system Σ_2' (red line).

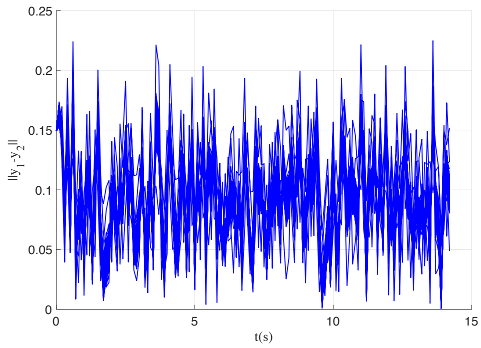

Fig. 2. The evolution of $\|y_1 - y_2\|$ for 100 realizations of disturbance signals.

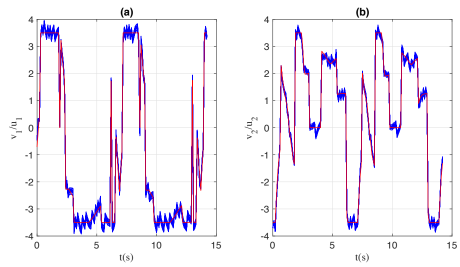

Fig. 3. The evolution of the inputs u (blue lines) for 100 realizations of disturbance signals and v (red line).

$\|y_1 - y_2\|$ is at most 0.25. This means that the theoretical bound of η obtained using Theorem 4.1 can be conservative (due to the use of Lyapunov-like function).

5.2 Example 2

In this example, we consider the (undisturbed) pendulum system studied in [26], which is described by

$$\Sigma_3 : \dot{x}(t) = f(x(t)) + Ax(t) + Bu(t), \quad (23)$$

where

$$A = \begin{bmatrix} 0 & 1 \\ 0 & -\frac{k}{m} \end{bmatrix}, B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, f(x) = \begin{bmatrix} 0 \\ -\frac{g}{l}\sin x_1 \end{bmatrix}.$$

The constant $g = 9.8$ is the gravity acceleration, $l = 5$ is the length of the rod, $m = 0.5$ is the mass, and $k = 3$ is the coefficient of friction. Here, we omit $y(t) = x(t)$ for simplicity. The pendulum works in the state-space $X = [-1, 1] \times [-1, 1]$ and the input set $U = [-1.5, 1.5]$. One can verify that (23) is δ-ISS.

Denote by P_1 and P_2 two different periodic motions, where P_1 requires the state of Σ_3 to cycle between $(-0.4, 0)$ and $(0, 0)$ while P_2 requires the state to cycle between $(-0.4, 0)$ and $(0.4, 0)$. Similarly to [26], the objective here is to find a control strategy that enforces system Σ_3 to satisfy a specification P, where P requires the execution of the sequence of periodic motions P_1, P_1, P_2, P_1, P_1. In the following, we will compare our construction of the abstract system with the one proposed in [26].

For the desired precision $\varepsilon = 0.25$, an abstract system, denoted by $T_{\tau,\eta,\mu}(\Sigma_3)$, is proposed in [26], where $\tau = 2, \eta = 0.4$, and $\mu = 1.5 \times 10^{-4}$ are respectively the time-, state-, and control-space discretization parameters. Denote by x_1, x_2 and q_1, q_2 the two state components of Σ_3 and $T_{\tau,\eta,\mu}(\Sigma_3)$, respectively. In [26], a control strategy that enforces P is synthesized and the state trajectory (x_1, x_2) is plotted. Here, we further plot the trajectories of the state errors $x_1 - q_1$ and $x_2 - q_2$ in Fig. 4, where the black dashed lines represent the desired precision and the red stars mark the values at the discrete instants $t = i\tau, i = 1, \ldots, 12$.

Next, we construct the abstract system using the state-space abstraction (6), which gives

$$\Sigma_3' : \begin{cases} \xi(t) = Q_\eta(\hat{\xi}(t)), \\ \dot{\hat{\xi}}(t) = f(\hat{\xi}(t)) + A\hat{\xi}(t) + Bv(t), \end{cases} \tag{24}$$

where $\xi(t) = (\xi_1(t), \xi_2(t)) \in [X]_\eta$ and $v(t) \in U'$ are the state and control input of (24), respectively. Since (23) is δ-ISS, the control interface can be chosen as $u_v(t) \equiv v(t)$ and the input set as $U' = U$. According to Theorem 4.1, the same precision $\varepsilon = 0.25$ can be achieved by choosing the state-space discretization parameter $\eta = 0.2$. The simulation result is shown in Fig. 5, where the trajectories of the state errors $x_1 - \xi_1$ and $x_2 - \xi_2$ are depicted.

Let us compare Figs. 4 and 5. The abstract system proposed in [26] only ensures that the desired precision $\varepsilon = 0.25$ is preserved at discrete instants (as shown at the red stars in Fig. 4) while the abstract system proposed in this work ensures that the desired precision $\varepsilon = 0.25$ is preserved continuously (see Fig. 5). This difference results from the fact that our method does not involve time-space discretization.

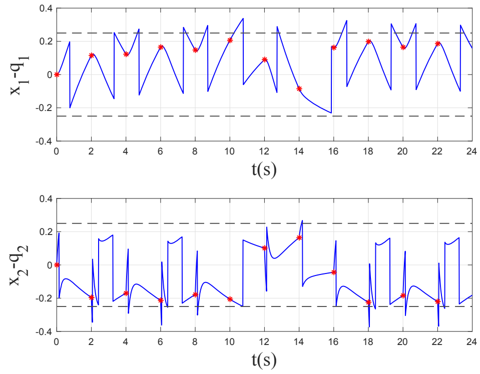

Fig. 4. The trajectories of the state errors $x_1 - q_1$ (up) and $x_2 - q_2$ (down) with the abstract system $T_{\tau,\eta,\mu}(\Sigma_3)$ proposed in [26], where the black dashed lines represent the desired precision $\varepsilon = 0.25$ and the red stars mark the values at the discrete instants $t = i\tau, i = 1, \ldots, 12$.

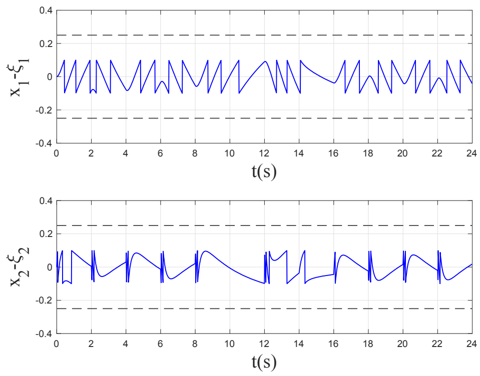

Fig. 5. The trajectories of the state errors $x_1 - \xi_1$ (up) and $x_2 - \xi_2$ (down) with our proposed abstract system (24).

6 Conclusion

This paper involved the construction of discrete state-space symbolic models for continuous-time uncertain nonlinear systems. Firstly, a stability notion called η-CGPS and its Lyapunov function characterizations were proposed. After that, a notion of robust approximate simulation relation was further introduced. It was shown that every continuous-time uncertain concrete system, under the condition that there exists an admissible control interface such that the augmented system can be made η-CGPS, robustly approximately simulates its discrete state-space abstraction. In the future, more efficient abstraction techniques, such as multi-scale abstraction [14], will be taken into account and experimental validation will be pursued.

References

[1] Açıkmeşe, B., & Corless, M. (2011). Observers for systems with nonlinearities satisfying incremental quadratic constraints. *Automatica*, 47(7), 1339-1348.

[2] Alur, R., Henzinger, T. A., Lafferriere, G., & Pappas, G. J. (2000). Discrete abstractions of hybrid systems. *Proceedings of the IEEE*, 88(7), 971-984.

[3] Angeli, D., & Sontag, E. D. (1999). Forward completeness, unboundedness observability, and their Lyapunov characterizations. *Systems & Control Letters*, 38(4-5), 209-217.

[4] Angeli, D. (2002). A Lyapunov approach to incremental stability properties. *IEEE Transactions on Automatic Control*, 47(3), 410-421.

[5] Arnold, A., Vincent, A., & Walukiewicz, I. (2003). Games for synthesis of controllers with partial observation. *Theoretical Computer Science*, 28(1), 734.

[6] Baier, C., & Katoen, J. P. (2008). Principles of model checking. MIT press.

[7] Cassandras, C., & Lafortune, S. (1999). Introduction to Discrete Event Systems. Boston, MA: Kluwer.

[8] D'Alto, L., & Corless, M. (2013). Incremental quadratic stability. Numerical Algebra, *Control & Optimization*, 3(1), 175-201.

[9] Fu, J., Shah, S., & Tanner, H. G. (2013, June). Hierarchical control via approximate simulation and feedback linearization. *In 2013 American Control Conference (pp. 1816-1821)*. IEEE.

[10] Girard, A., & Pappas, G. J. (2007). Approximation metrics for discrete and continuous systems. *IEEE Transactions on Automatic Control*, 52(5), 782-798.

[11] Girard, A., & Pappas, G. J. (2009). Hierarchical control system design using approximate simulation. *Automatica*, 45(2), 566-571.

[12] Girard, A., Pola, G., & Tabuada, P. (2009). Approximately bisimilar symbolic models for incrementally stable switched systems. *IEEE Transactions on Automatic Control*, 55(1), 116-126.

[13] Girard, A. (2012). Controller synthesis for safety and reachability via approximate bisimulation. *Automatica*, 48(5), 947-953.

[14] Girard, A., Gössler, G., & Mouelhi, S. (2015). Safety controller synthesis for incrementally stable switched systems using multiscale symbolic models. *IEEE Transactions on Automatic Control*, 61(6), 1537-1549.

[15] Goedel, R., Sanfelice, R. G., & Teel, A. R. (2012). Hybrid dynamical systems: modeling stability, and robustness. *Princeton University Press.*

[16] Khalil, H. K. (2002). Nonlinear Systems. *Prentice Hall*, 3rd edn.

[17] Kim, E. S., Arcak, M., & Seshia, S. A. (2017). Symbolic control design for monotone systems with directed specifications. *Automatica*, 83, 10-19.

[18] Kloetzer, M., & Belta, C. (2008). A fully automated framework for control of linear systems from temporal logic specifications. *IEEE Transactions on Automatic Control*, 53(1), 287-297.

[19] Kumar, R., & Garg, V. (1995). Modeling Control of Logical Discrete Event Systems. Boston, MA: Kluwer.

[20] Liu, J., & Ozay, N. (2016). Finite abstractions with robustness margins for temporal logic-based control synthesis. *Nonlinear Analysis: Hybrid Systems*, 22, 1-15.

[21] Madhusudan, P., Nam, W., & Alur, R. (2003). Symbolic computational techniques for solving games. *Electronic Notes in Theoretical Computer Science*, 89(4), 578-592.

[22] Mazo, M., Davitian, A., & Tabuada, P. (2010, July). Pessoa: A tool for embedded controller synthesis. *In International Conference on Computer Aided Verification* (pp. 566-569). Springer, Berlin, Heidelberg.

[23] Mallik, K., Schmuck, A. K., Soudjani, S., & Majumdar, R. (2018). Compositional synthesis of finite-state abstractions. *IEEE Transactions on Automatic Control*, 64(6), 2629-2636.

[24] Milner, R. (1989). Communication and concurrency. *Prentice Hall*.

[25] Park, D. (1981). Concurrency and automata on infinite sequences. *In Theoretical computer science (pp. 167-183)*. Springer, Berlin, Heidelberg.

[26] Pola, G., Girard, A., & Tabuada, P. (2008). Approximately bisimilar symbolic models for nonlinear control systems. *Automatica*, 44(10), 2508-2516.

[27] Ramadge, P. J., & Wonham, W. M. (1987). Modular feedback logic for discrete event systems. *SIAM Journal on Control and Optimization*, 25(5), 1202-1218.

[28] Reissig, G., Weber, A., & Rungger, M. (2016). Feedback refinement relations for the synthesis of symbolic controllers. *IEEE Transactions on Automatic Control*, 62(4), 1781-1796.

[29] Rungger, M., & Zamani, M. (2016). SCOTS: A tool for the synthesis of symbolic controllers. *In Proceedings of the 19th international conference on hybrid systems: Computation and control (pp. 99-104)*.

[30] Saoud, A., Girard, A., & Fribourg, L. (2020). Contract-based design of symbolic controllers for safety in distributed multiperiodic sampled-data systems. *IEEE Transactions on Automatic Control*, 66(3), 1055-1070.

[31] Smith, S. W., Arcak, M., & Zamani, M. (2020). Approximate abstractions of control systems with an application to aggregation. *Automatica*, 119, 109065.

[32] Tabuada, P. (2009). Verification and control of hybrid systems: a symbolic approach. *Springer Science & Business Media*.

[33] Yang, K., & Ji, H. (2017). Hierarchical analysis of large-scale control systems via vector simulation function. *Systems & Control Letters*, 102, 74-80.

[34] Yu, P., & Dimarogonas, D. V. (2019). Approximately symbolic models for a class of continuous-time nonlinear systems. *In 2019 IEEE 58th Conference on Decision and Control (CDC) (pp. 4349-4354)*.

[35] Zamani, M., Pola, G., Mazo, M., & Tabuada, P. (2011). Symbolic models for nonlinear control systems without stability assumptions. *IEEE Transactions on Automatic Control*, 57(7), 1804-1809.

[36] Zamani, M., van de Wouw, N., & Majumdar, R. (2013). Backstepping controller synthesis and characterizations of incremental stability. *Systems & Control Letters*, 62(10), 949-962.

[37] Zamani, M., Esfahani, P. M., Majumdar, R., Abate, A., & Lygeros, J. (2014). Symbolic control of stochastic systems via approximately bisimilar finite abstractions. *IEEE Transactions on Automatic Control*, 59(12), 3135-3150.