PAPER

Deadlock-Free Symbolic Smith Controllers Based on Prediction for Nondeterministic Systems**

Masashi MIZOGUCHI[†*a)], ***Member and*** **Toshimitsu USHIO**[†], ***Fellow***

SUMMARY The Smith method has been used to control physical plants with dead time components, where plant states after the dead time is elapsed are predicted and a control input is determined based on the predicted states. We extend the method to the symbolic control and design a symbolic Smith controller to deal with a nondeterministic embedded system. Due to the nondeterministic transitions, the proposed controller computes all reachable plant states after the dead time is elapsed and determines a control input that is suitable for all of them in terms of a given control specification. The essence of the Smith method is that the effects of the dead time are suppressed by the prediction, however, which is not always guaranteed for nondeterministic systems because there may exist no control input that is suitable for all predicted states. Thus, in this paper, we discuss the existence of a deadlock-free symbolic Smith controller. If it exists, it is guaranteed that the effects of the dead time can be suppressed and that the controller can always issue the control input for any reachable state of the plant. If it does not exist, it is proved that the deviation from the control specification is essentially inevitable.

key words: *Smith predictor, symbolic control, dead time, approximated alternating simulation, deadlock*

1. Introduction

Dead times exist in many control systems such as chemical plants, data networks, and remote control of space robotics [1]. These dead times often degrade control performances and influence the stability of the plant.

O. Smith introduced a predictor to improve the performance of the controller when the plant has a dead time component [2]. Shown in Fig. 1 is a structure of the closed-loop system, where $G[z] \cdot z^{-L}$ is a plant with a rational transfer function $G[z]$ and a dead time L, $G_c[z]$ is a controller such as a PID controller designed for $G[z]$, and $P[z]$ is a model of $G[z]$. If $P[z] = G[z]$, the transfer function from r to y is given by

$$\frac{G[z]G_c[z]}{1 + G[z]G_c[z]} z^{-L}. \tag{1}$$

Apparently, (1) implies that the dead time component is out of the feedback loop and the output $y[k]$ is controlled based on the delayed reference $r[k - L]$. Intuitively, the system $P[z]$ predicts the state of the plant after L times, and the minor loop consisting of $G_c[z]$ and $P[z]$ determines a control input that is suitable for the predicted state. The Smith controller and its modifications and extensions have been studied [3], [4]. The Smith controller is also extended to nonlinear systems [5] and digital controllers [6]. The key point of Smith controllers is that controllers are successfully extended to control plants with dead times by predicting plant states after the dead times are elapsed.

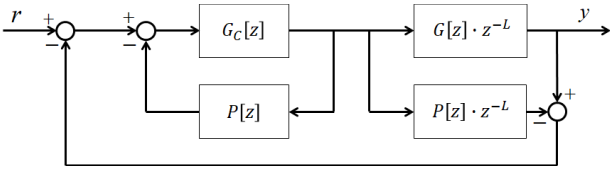

Fig. 1 The block diagram of the (classical) Smith controller.

On the other hand, symbolic approaches have gathered attentions for the control of embedded systems in order to deal with complicated control specifications and nondeterministic transitions [7]–[9]. Recently, an approximate contractive alternating (bi)simulation relation (acASR) is introduced, which enforces robustness against abstraction errors, sporadic disturbances such as packet dropouts, and input errors [10]–[12]. The authors extended the acASR-based symbolic synthesis to partial observation and delayed systems [13]–[17]. These approaches are extended to networked control systems [18], [19]

Especially, in [16], the authors proposed a framework of a symbolic Smith controller, which proves that the Smith method is applicable not only in the classical control but also in symbolic control. A symbolic controller designed for a plant with no dead time is successfully extended to control a plant with a dead time by adding a predictor on plant states after the dead time is elapsed. Note that this is same as (classic) Smith controllers in terms that $G_c[z]$ stabilizing $G[z]$ is still useful for $G[z] \cdot z^{-L}$ by adding a predictor as shown in Fig. 1. In contrast to the other approaches [20]–[23], it is proved that the control performance does not degrade by the dead time and that the controlled plant still satisfies a control specification. However, it should be guaranteed that there always exists a control input that is suitable for all predicted states if the plant has nondeterministic transitions, which has not been considered.

Thus, in this paper, we discuss the design of a deadlock-free symbolic Smith controller for a plant with nondetermin-

Manuscript received January 10, 2021.
Manuscript revised April 5, 2021.
Manuscript publicized May 14, 2021.

[†]The authors are with the Graduate School of Engineering Science, Osaka University, Toyonaka-shi, 560-8531 Japan.
[*]Presently, with the Research and Development Group, Hitachi Ltd, Hitachi-shi, 319-1292 Japan.

**This work was supported by JST ERATO Grant Number JPMJER1603, Japan.

a) E-mail: mizoguchi@hopf.sys.es.osaka-u.ac.jp

DOI: 10.1587/transfun.2021EAP1002

istic transitions and show the condition for the existence of the controller. If the deadlock-free controller exists, it is guaranteed that the effects of the dead time can be suppressed and that control inputs are always issued for any reachable states of the plant. If it does not exist, it is shown that the effects of the dead time cannot be suppressed and that the degrade of the control performance is essentially inevitable.

2. Symbolic Control

In this section, we review several notions of symbolic control and show an existence condition of a symbolic controller for a plant with no dead time.

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 $x \in \mathbb{R}$, $\lfloor x \rfloor \in \mathbb{Z}$ is defined by $\lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \leq x\}$. For any $a \in \mathbb{R}$ and any $b \in \mathbb{R}$ such that $a < b$, $[a, b[\subseteq \mathbb{R}$ and $[a, b] \subseteq \mathbb{R}$ are defined by $[a, b[:= \{x \in \mathbb{R} \mid a \leq x < b\}$ and $[a, b] := \{x \in \mathbb{R} \mid a \leq x \leq b\}$, respectively. For a given set A, denoted by 2^A is the power set of A: $2^A := \{A' \text{ is a set.} \mid A' \subseteq A\}$. For given sets B and C, denoted by B^C is a set of all mappings from C to B.

2.2 Symbolic Systems and Approximate Relations

The following definitions refer to fundamental notions for the symbolic control [11].

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 $x \in X$, let $U(x) = \{u \in U \mid r(x, u) \neq \emptyset\}$. We extend the transition map $r : X \times U^* \to 2^X$ in the following ways:

1. $r(x, \varepsilon) = \{x\}$; and
2. $r(x, t\sigma) = \{x'' \in X \mid \exists x' \in r(x, t) : x'' \in r(x', \sigma)\}$,

where ε is the empty string, and U^* is a set of all finite input strings over U. A deadlock state $x \in X$ is a state such that $U(x) = \emptyset$, and we say that S is deadlock-free iff the following condition is satisfied:

$$\forall x \in X : \ U(x) \neq \emptyset.$$

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, denoted by $R_X \subseteq X_1 \times X_2$ is a projection of R to the state sets X_1, X_2 as follows:

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

In addition, for a parameterized relation[†] $R(\epsilon) \subseteq X_1 \times X_2 \times U_1 \times U_2$ over the state sets X_1, X_2 and the input sets U_1, U_2, denoted by $R_X(\epsilon) \subseteq X_1 \times X_2$ is a projection of $R(\epsilon)$ to the state sets X_1, X_2 as follows:

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

Then, the following definition describes an approximate contractive alternating simulation relation between two systems. 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 $\epsilon \in [\kappa, \infty[$:

1. $\forall x_{10} \in X_{10}, \exists x_{20} \in X_{20} : (x_{10}, x_{20}) \in R_X(\kappa)$;
2. $\forall x_1 \in X_1, \forall u_1 \in U_1(x_1), \forall x_2 \in X_2, \exists u_2 \in U_2(x_2)$:

$$(x_1, x_2) \in R_X(\epsilon) \Rightarrow [(x_1, x_2, u_1, u_2) \in R(\epsilon)] \wedge \left[\forall x_2' \in r_2(x_2, u_2), \exists x_1' \in r_1(x_1, u_1) : (x_1', x_2') \in R_X(\kappa + \beta\epsilon + \lambda \mathsf{d}(u_1, u_2))\right].$$

If $R(\epsilon)$ is $(0, 0, 0)$-acASR, we simply call R an alternating simulation relation (ASR).

Let $S = (X, X_0, U, r)$ and $S_C = (X_C, X_{C0}, U_C, r_C)$ be two systems, and consider a relation $R_C(\epsilon) \subseteq X_C \times X \times U_C \times U$. We call the pair $(S_C, R_C(\epsilon))$ a controller for S if there exist parameters $\kappa, \lambda \in \mathbb{R}_{\geq 0}$, $\beta \in [0, 1[$, and a map $\mathsf{d_C} : U_C \times U \to \mathbb{R}_{\geq 0}$ such that $R_C(\epsilon)$ is a (κ, β, λ)-acASR from S_C to S with $\mathsf{d_C}$. Intuitively, S_C is a system that describes all feasible behaviors for S. In this sense, we call S_C the control specification for S. By the pair $(S_C, R_C(\epsilon))$, behaviors of the plant S and those of the specification S_C are synchronized with respect to $R_C(\epsilon)$, which implies that the specification is enforced on the plant.

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, and let $R \subseteq X_1 \times X_2 \times U_1 \times U_2$ be a relation. We define the composition of S_1 and S_2 with respect to R, denoted by $S := S_1 \times_R S_2 = (X, X_0, U, r)$ where

- $X = X_1 \times X_2$;
- $X_0 = (X_{10} \times X_{20}) \cap R_X$;
- $U = U_1 \times U_2$; and
- $r : X \times U \to 2^X$ is defined as follows: $(x_1', x_2') \in r((x_1, x_2), (u_1, u_2))$ iff

$$\left[x_1' \in r_1(x_1, u_1)\right] \wedge \left[x_2' \in r_2(x_2, u_2)\right] \wedge [(x_1, x_2, u_1, u_2) \in R] \wedge \left[(x_1', x_2') \in R_X\right].$$

[†]We consider a parameterized relation for finite abstraction of (possibly) infinite transition systems. Intuitively, the parameter ϵ describes bounded errors between the actual and the finite abstracted plant states. An example of such parameterized relation is shown in Sect. 4.

If $R(\epsilon)$ is a (κ,β,λ)-acASR from S_1 to S_2 with d, we replace the above definitions of X_0 and r with the following conditions:

- $X_0 = (X_{10} \times X_{20}) \cap R_X(\kappa)$; and
- $r : X \times U \to 2^X$ is defined as follows: $(x_1', x_2') \in r((x_1, x_2), (u_1, u_2))$ iff

$$\begin{aligned}&\left[x_1' \in r_1(x_1, u_1)\right] \wedge \left[x_2' \in r_2(x_2, u_2)\right] \wedge \\ &\left[(x_1, x_2, u_1, u_2) \in R(e(x_1, x_2))\right] \wedge \\ &\left[(x_1', x_2') \in R_X(\kappa + \beta e(x_1, x_2) + \lambda \mathsf{d}(u_1, u_2))\right],\end{aligned}$$

where $e(x_1, x_2) := \inf\{\epsilon \in [\kappa, \infty[\mid (x_1, x_2) \in R_X(\epsilon)\}$.

2.3 Symbolic Controller Design without Dead Times

We review an abstracted controller proposed by Rungger and Tabuada in [11] summarized as follows:

- Consider a finite abstracted model of a plant;
- Design a controller for the abstracted model; and
- Obtain a controller for the plant.

The following assumption formally imposes the existence of the abstracted plant model and the controller.

Assumption 1 Let $S = (X, X_0, U, r)$ be a physical plant to be controlled. Assume the existence of a system $\hat{S} = (\hat{X}, \hat{X}_0, \hat{U}, \hat{r})$ such that there exists a (κ,β,λ)-acASR $R(\epsilon) \subseteq \hat{X} \times X \times \hat{U} \times U$ from $\hat{S}$ to S with d for some $\kappa, \lambda \in \mathbb{R}_{\geq 0}$, $\beta \in [0, 1[$, and a map $\mathsf{d} : \hat{U} \times U \to \mathbb{R}_{\geq 0}$. We also assume that a controller for $\hat{S}$ is already given by the pair $(\hat{S}_C, \hat{R}_C)$ where $\hat{S}_C = (\hat{X}_C, \hat{X}_{C0}, \hat{U}_C, \hat{r}_C)$ and the relation $\hat{R}_C \subseteq \hat{X}_C \times \hat{X} \times \hat{U}_C \times \hat{U}$ is an ASR from $\hat{S}_C$ to $\hat{S}$.

Then, we have the following theorem that shows the configuration of the controller for the plant [11].

Theorem 1 Under Assumption 1, consider the composed system $S_C := \hat{S}_C \times_{\hat{R}_C} \hat{S} = (X_C, X_{C0}, U_C, r_C)$ and the following relation $R_C(\epsilon) \subseteq X_C \times X \times U_C \times U$:

$$\begin{aligned}R_C(\epsilon) = \{((\hat{x}_C, \hat{x}), x, (\hat{u}_C, \hat{u}), u) \in X_C \times X \times U_C \times U \mid \\ [(\hat{x}, x, \hat{u}, u) \in R(\epsilon)] \wedge [(\hat{x}_C, \hat{x}, \hat{u}_C, \hat{u}) \in \hat{R}_C]\}.\end{aligned} \tag{2}$$

Then, the pair $(S_C, R_C(\epsilon))$ is a controller for S.

Theorem 1 implies that we have a controller for S by composing $\hat{S}_C$ and $\hat{S}$. However, if there exists an input dead time, the approach is not applicable. This is because they are derived from relations that will probably be violated due to the mismatch of states of delayed plants and those of controllers. Then, in this paper, we extend this framework to control delayed plants. We propose prediction in contexts of symbolic control that is inspired from the Smith controller in the classical control theory.

3. Design of a Deadlock-Free Symbolic Smith Controller

In this section, we design a deadlock-free symbolic Smith controller. The procedures are summarized as follows. First, we introduce a symbolic model of a delayed plant (Definition 3). Second, we design a symbolic Smith predictor (Definition 4) and a system to feedback prediction errors (Definition 5) equivalent to $P[z]$ and $P[z] \cdot z^{-L}$, respectively, in Fig. 1. Third, we compose them and prove an acASR implying that a control input can successfully be determined in terms of a control specification (Theorem 2). Finally, we introduce an operator to obtain a deadlock-free subtransition system of the symbolic Smith controller.

3.1 Model of the Plant with the Input Dead Time

The plant with the dead time is modeled by the following transition system[†].

Definition 3 We define a system with a dead time L

$$S_D = (X_D, X_{D0}, U_D, r_D) \tag{3}$$

induced by $S = (X, X_0, U, r)$, where

- $X_D = X \times U^L$;
- $X_{D0} = \{(x_0, u_0^1, u_0^2, \ldots, u_0^L) \in X_0 \times U^L \mid r(x_0, u_0^1 u_0^2 \ldots u_0^L) \neq \emptyset\}$;
- $U_D = U \times U$; and
- $r_D : X_D \times U_D \to 2^{X_D}$ is defined as follows:

$$\begin{aligned}&r_D((x, u^1, u^2, \ldots, u^L), (u_D^1, u_D^2)) \\ &= \begin{cases}\{(x', u^2, \ldots, u^L, u_D^2) \mid x' \in r(x, u_D^1)\} & \\ \qquad\qquad \text{if } u_1^D = u^1, & \\ \emptyset \qquad\qquad \text{otherwise.} & \end{cases}\end{aligned}$$

The input of S_D is a pair of inputs: $u_D^1 = u^1$ is an updated input of the plant, while u_D^2 is a control input stored in the queue and will be injected into the plant after L time steps are elapsed.

Each state $(x, u^1, u^2, \ldots, u^L) \in X_D$ means as follows:

- The state x is the current state of the plant; and
- U^L denotes the First-In-First-Out (FIFO) queue, that is, the states u^1, u^2, …, u^L are waiting control inputs due to the dead time component.

Intuitively, S_D is the composition of the plant S and the queue with L memories describing the dead time. This is equivalent to the delayed plant $G[z] \cdot z^{-L}$ in the classical control theory, which is the composition of the rational transfer function $G[z]$ (corresponding to S in the symbolic control) and a dead time component z^{-L} (corresponding to L-length FIFO

[†]To simplify the discussion, we assume that S is a discrete-time transition system.

memories). In order to determine the initial condition, we consider the case where the first L initial input sequence, denoted by $u_0^1 u_0^2 \dots u_0^L$ satisfying $r(x_0, u_0^1 u_0^2 \dots u_0^L) \neq \emptyset$, is stored in the queue and the actuator updates to u_0^1 because the plant starts at the initial time. This is different from the classical control where initial states are not explicitly considered or implicitly set to 0 in most cases.

3.2 Symbolic Smith Predictor

We introduce a symbolic Smith predictor induced by $\hat{S} = (\hat{X}, \hat{X}_0, \hat{U}, \hat{r})$ that updates prediction by computing all reachable states from the latest measured state with the L-length latest input sequence. Since the plant is generally nondeterministic, the predictor does not predict the state uniquely. Instead, the predictor lists all candidates. Thus, the set of states of the predictor, denoted by $\hat{\mathbf{X}}$, is the power set of $\hat{X}$. For each state $\hat{\mathbf{x}} \in \hat{\mathbf{X}} = 2^{\hat{X}} \setminus \{\emptyset\}$, a mapping $\hat{\mathbf{u}} : \hat{\mathbf{x}} \to \hat{U}$ that assigns each candidate state $\hat{x} \in \hat{\mathbf{x}}$ to an input $\hat{\mathbf{u}}(\hat{x}) \in \hat{U}(\hat{x})$ will be called an input map. Let $\hat{\mathbf{U}} = \bigcup_{\hat{\mathbf{x}} \in \hat{\mathbf{X}}} \hat{U}^{\hat{\mathbf{x}}}$ be a set of all input mappings with respect to $\hat{\mathbf{X}}$. Denoted by $\mathrm{dom}(\hat{\mathbf{u}}) \subseteq \hat{X}$ is the domain of the input map $\hat{\mathbf{u}}$. Then, we define a transition map $\hat{r}^e : \hat{\mathbf{X}} \times \hat{\mathbf{U}}^* \to \hat{\mathbf{X}}$ induced by $\hat{r} : \hat{X} \times \hat{U} \to 2^{\hat{X}}$ as follows:

1. For each $\hat{\mathbf{x}} \in \hat{\mathbf{X}}$ and each $\hat{\mathbf{u}} \in \hat{\mathbf{U}}$,

$$\hat{r}^e(\hat{\mathbf{x}}, \hat{\mathbf{u}}) = \begin{cases} \bigcup_{\hat{x} \in \hat{\mathbf{x}}} \hat{r}(\hat{x}, \hat{\mathbf{u}}(\hat{x})) & \text{if } \hat{\mathbf{x}} = \mathrm{dom}(\hat{\mathbf{u}}), \\ \emptyset & \text{otherwise.} \end{cases}$$

2. For each $\hat{\mathbf{x}} \in \hat{\mathbf{X}}$, each input map sequence $\hat{\mathbf{t}} \in \hat{\mathbf{U}}^*$, and each input map $\hat{\mathbf{u}} \in \hat{\mathbf{U}}$,

$$\hat{r}^e(\hat{\mathbf{x}}, \varepsilon) = \hat{\mathbf{x}}; \text{ and}$$

$$\hat{r}^e(\hat{\mathbf{x}}, \hat{\mathbf{t}}\hat{\mathbf{u}}) = \begin{cases} \bigcup_{\hat{x}' \in \hat{r}^e(\hat{\mathbf{x}}, \hat{\mathbf{t}})} \hat{r}(\hat{x}', \hat{\mathbf{u}}(\hat{x}')) \\ \qquad \text{if } \hat{r}^e(\hat{\mathbf{x}}, \hat{\mathbf{t}}) = \mathrm{dom}(\hat{\mathbf{u}}), \\ \emptyset \qquad \text{otherwise.} \end{cases}$$

For simplicity, we write $\hat{r}^e(\hat{x}, \hat{\mathbf{u}})$ for $\hat{r}^e(\{\hat{x}\}, \hat{\mathbf{u}})$.

For any $\hat{\mathbf{u}} \in \hat{\mathbf{U}}$, we introduce the following set of physical inputs:

$$\mathcal{U}(\hat{\mathbf{u}}) = \{u \in U \mid \forall \epsilon \in [\kappa, \infty[, \forall \hat{x} \in \mathrm{dom}(\hat{\mathbf{u}}), \forall x \in X : [(\hat{x}, x) \in R_X(\epsilon) \Rightarrow u \in U(x)] \wedge [(\hat{x}, x, \hat{\mathbf{u}}(\hat{x}), u) \in R(\epsilon)]\}.$$

Intuitively, $\mathcal{U}(\hat{\mathbf{u}})$ is a set of common physical inputs that are valid at all states in $\mathrm{dom}(\hat{\mathbf{u}})$. Recall that, in the prediction-based approach, the controller determines a control input that is valid for all estimated states to achieve the control specification.

For the estimation at the initial time, we impose the following assumption that there exists a common physical input during the first L time steps.

Assumption 2 There exist an initial state $\hat{x}_0 \in \hat{X}_0$ and an initial input map sequence $\hat{\mathbf{u}}_\mathbf{0}^1 \hat{\mathbf{u}}_\mathbf{0}^2 \dots \hat{\mathbf{u}}_\mathbf{0}^L$ ($\hat{\mathbf{u}}_\mathbf{0}^i \in \hat{\mathbf{U}}, i \in \{1, 2, \dots, L\}$) such that

$$\forall i \in \{1, 2, \dots, L\} : [\mathrm{dom}(\hat{\mathbf{u}}_\mathbf{0}^i) = \hat{r}^e(\hat{x}_0, \hat{\mathbf{u}}_\mathbf{0}^1 \hat{\mathbf{u}}_\mathbf{0}^2 \dots \hat{\mathbf{u}}_\mathbf{0}^{i-1})] \wedge [\mathcal{U}(\hat{\mathbf{u}}_\mathbf{0}^i) \neq \emptyset]. \tag{4}$$

Note that, if $\hat{S}$ is a finite transition system, Assumption 2 can be tested in finite steps. Then, the symbolic Smith predictor is formally defined as follows.

Definition 4 Under Assumption 2, we define a system

$$\hat{\mathbf{S}} = (\hat{\mathbf{X}}, \hat{\mathbf{X}}_\mathbf{0}, \hat{\mathbf{U}}, \hat{\mathbf{r}}) \tag{5}$$

induced by $\hat{S} = (\hat{X}, \hat{X}_0, \hat{U}, \hat{r})$ with respect to $\hat{x}_0 \in \hat{X}_0$ and $\hat{\mathbf{u}}_\mathbf{0}^1 \hat{\mathbf{u}}_\mathbf{0}^2 \dots \hat{\mathbf{u}}_\mathbf{0}^L$ ($\hat{\mathbf{u}}_\mathbf{0}^i \in \hat{\mathbf{U}}, i \in \{1, 2, \dots, L\}$) satisfying (4) where

- $\hat{\mathbf{X}}_\mathbf{0} = \{\hat{r}^e(\hat{x}_0, \hat{\mathbf{u}}_\mathbf{0}^1 \hat{\mathbf{u}}_\mathbf{0}^2 \dots \hat{\mathbf{u}}_\mathbf{0}^L)\} \subseteq \hat{\mathbf{X}}$; and
- $\hat{\mathbf{r}} : \hat{\mathbf{X}} \times \hat{\mathbf{U}} \to 2^{\hat{\mathbf{X}}}$ is defined as follows:

$$\hat{\mathbf{r}}(\hat{\mathbf{x}}, \hat{\mathbf{u}}) = \begin{cases} 2^{\hat{r}^e(\hat{\mathbf{x}}, \hat{\mathbf{u}})} \setminus \{\emptyset\} \\ \quad \text{if } \forall \hat{x} \in \hat{\mathbf{x}} : [\hat{r}^e(\hat{x}, \hat{\mathbf{u}}) \neq \emptyset] \wedge [\mathcal{U}(\hat{\mathbf{u}}) \neq \emptyset], \\ \emptyset \text{ otherwise.} \end{cases}$$

The system $\hat{\mathbf{S}}$ is equivalent to $P[z]$ in the classical control theory to predict plant states after the dead time is elapsed. Note that, in symbolic control, we consider plants (possibly) with non-deterministic transitions. It is also noticed that the initial states should be properly considered. Then, since $\hat{\mathbf{S}}$ predicts the state of the plant when a control input arrives, each initial state of $\hat{\mathbf{S}}$ is a set of reachable states from the initial state $\hat{x}_0 \in \hat{X}_0$ of $\hat{S}$ with the initial input map sequence $\hat{\mathbf{u}}_\mathbf{0}^1 \hat{\mathbf{u}}_\mathbf{0}^2 \dots \hat{\mathbf{u}}_\mathbf{0}^L$ satisfying (4). It is important that the state of $\hat{\mathbf{S}}$ is L time steps forward compared with that of $\hat{S}$.

For the symbolic Smith predictor, the latest measured state and the latest input sequence are key information for the prediction. So, we introduce the following transition system that stores them.

Definition 5 We define a system

$$\hat{S}_D = (\hat{X}_D, \hat{X}_{D0}, \hat{U}_D, \hat{r}_D) \tag{6}$$

induced by $\hat{\mathbf{S}} = (\hat{\mathbf{X}}, \hat{\mathbf{X}}_\mathbf{0}, \hat{\mathbf{U}}, \hat{\mathbf{r}})$ constructed with respect to $\hat{x}_0 \in \hat{X}_0$ and $\hat{\mathbf{u}}_\mathbf{0}^1 \hat{\mathbf{u}}_\mathbf{0}^2 \dots \hat{\mathbf{u}}_\mathbf{0}^L$ ($\hat{\mathbf{u}}_\mathbf{0}^i \in \hat{\mathbf{U}}, i \in \{1, 2, \dots, L\}$) satisfying (4) where

- $\hat{X}_D = \hat{X} \times \hat{\mathbf{U}}^L$;
- $\hat{X}_{D0} = \{(\hat{x}_0, \hat{\mathbf{u}}_\mathbf{0}^1, \hat{\mathbf{u}}_\mathbf{0}^2, \dots, \hat{\mathbf{u}}_\mathbf{0}^L)\} \subseteq \hat{X}_0 \times \hat{\mathbf{U}}^L$;
- $\hat{U}_D = \hat{\mathbf{U}} \times \hat{\mathbf{U}}$; and
- $\hat{r}_D : \hat{X}_D \times \hat{U}_D \to 2^{\hat{X}_D}$ is defined as follows:

$$\hat{r}_D((\hat{x}, \hat{\mathbf{u}}^1, \hat{\mathbf{u}}^2, \dots, \hat{\mathbf{u}}^L), (\hat{\mathbf{u}}_\mathbf{D}^1, \hat{\mathbf{u}}_\mathbf{D}^2)) = \begin{cases} \{(\hat{x}', \hat{\mathbf{u}}^2, \hat{\mathbf{u}}^3, \dots, \hat{\mathbf{u}}^L, \hat{\mathbf{u}}_\mathbf{D}^2) \mid \hat{x}' \in \hat{r}^e(\hat{x}, \hat{\mathbf{u}}_\mathbf{D}^1)\} \\ \quad \text{if } [\hat{\mathbf{u}}_\mathbf{D}^1 = \hat{\mathbf{u}}^1] \wedge [\mathcal{U}(\hat{\mathbf{u}}_\mathbf{D}^2) \neq \emptyset] \wedge \\ \quad [\mathrm{dom}(\hat{\mathbf{u}}_\mathbf{D}^2) = \hat{r}^e(\hat{x}, \hat{\mathbf{u}}^1 \hat{\mathbf{u}}^2 \dots \hat{\mathbf{u}}^L)], \\ \emptyset \quad \text{otherwise.} \end{cases}$$

The system $\hat{S}_D$ plays a role of $P[z] \cdot z^{-L}$ in the classical control theory. Each state $\hat{x}_D = (\hat{x}, \hat{\mathbf{u}}^1, \hat{\mathbf{u}}^2, \ldots, \hat{\mathbf{u}}^L) \in \hat{X}_D$ is composed of the abstracted current plant state $\hat{x}_D$ and latest input sequence $\hat{\mathbf{u}}^1, \hat{\mathbf{u}}^2, \ldots, \hat{\mathbf{u}}^L \in \hat{X}_D$. In contrast to the classic control theory, we improve the prediction not by feeding back subtraction $G[z] \cdot z^{-L} - P[z] \cdot z^{-L}$ but by considering approximated contractive alternating simulations. We have the following lemma that shows the synchronization between $\hat{\mathbf{S}}$ and $\hat{S}_D$.

Lemma 1 Under Assumptions 1 and 2, we construct $\hat{\mathbf{S}}$, given by Definition 4, w.r.t. $\hat{x}_0 \in \hat{X}_0$ and $\hat{\mathbf{u}}_\mathbf{0}^1 \hat{\mathbf{u}}_\mathbf{0}^2 \ldots \hat{\mathbf{u}}_\mathbf{0}^L$ ($\hat{\mathbf{u}}_\mathbf{0}^i \in \hat{\mathbf{U}}, i \in \{1, 2, \ldots, L\}$) satisfying (4). We also construct $\hat{S}_D$, given by Definition 5, induced by $\hat{\mathbf{S}}$. Then, the following relation $\hat{\mathbf{R}} \subseteq \hat{\mathbf{X}} \times \hat{X}_D \times \hat{\mathbf{U}} \times \hat{U}_D$ is an ASR from $\hat{\mathbf{S}}$ to $\hat{S}_D$:

$$\begin{aligned}&\hat{\mathbf{R}} = \\ &\{(\hat{\mathbf{x}}, (\hat{x}, \hat{\mathbf{u}}^1, \hat{\mathbf{u}}^2, \ldots, \hat{\mathbf{u}}^L), \hat{\mathbf{u}}, (\hat{\mathbf{u}}_\mathbf{D}^1, \hat{\mathbf{u}}_\mathbf{D}^2)) \in \hat{\mathbf{X}} \times \hat{X}_D \times \hat{\mathbf{U}} \times \hat{U}_D \mid \\ &\quad [\hat{\mathbf{x}} = \hat{r}^e(\hat{x}, \hat{\mathbf{u}}^1 \hat{\mathbf{u}}^2 \ldots \hat{\mathbf{u}}^L)] \wedge [\hat{\mathbf{u}}^1 = \hat{\mathbf{u}}_\mathbf{D}^1] \wedge [\hat{\mathbf{u}} = \hat{\mathbf{u}}_\mathbf{D}^2]\}.\end{aligned} \tag{7}$$

Intuitively, Lemma 1 implies that the prediction is improved by feeding back the latest measured state as shown in Fig. 2.

$\hat{S}_D$ is also synchronized with S_D as shown in Lemma 2 describing that $\hat{x}_D$ in a state $\hat{x}_D = (\hat{x}, \hat{\mathbf{u}}^1, \hat{\mathbf{u}}^2, \ldots, \hat{\mathbf{u}}^L) \in \hat{X}_D$ is always an abstracted current state and that $\hat{\mathbf{u}}^1, \hat{\mathbf{u}}^2, \ldots, \hat{\mathbf{u}}^L \in \hat{X}_D$ is the latest input sequence.

Lemma 2 Under Assumptions 1 and 2, we construct $\hat{S}_D$, given by Definition 5, induced by $\hat{\mathbf{S}}$ w.r.t. $\hat{x}_0 \in \hat{X}_0$ and $\hat{\mathbf{u}}_\mathbf{0}^1 \hat{\mathbf{u}}_\mathbf{0}^2 \ldots \hat{\mathbf{u}}_\mathbf{0}^L$ ($\hat{\mathbf{u}}_\mathbf{0}^i \in \hat{\mathbf{U}}, i \in \{1, 2, \ldots, L\}$) satisfying (4). Consider the plant with the dead time S_D given by Definition 3. We introduce a map $\mathsf{d}_D : \hat{U}_D \times U_D \to \mathbb{R}_{\geq 0}$ defined as follows:

$$\mathsf{d}_D((\hat{\mathbf{u}}_\mathbf{D}^1, \hat{\mathbf{u}}_\mathbf{D}^2), (u_D^1, u_D^2)) = \max_{\hat{x} \in \mathrm{dom}(\hat{\mathbf{u}}_\mathbf{D}^1)} \mathsf{d}(\hat{\mathbf{u}}_\mathbf{D}^1(\hat{x}), u_D^1). \tag{8}$$

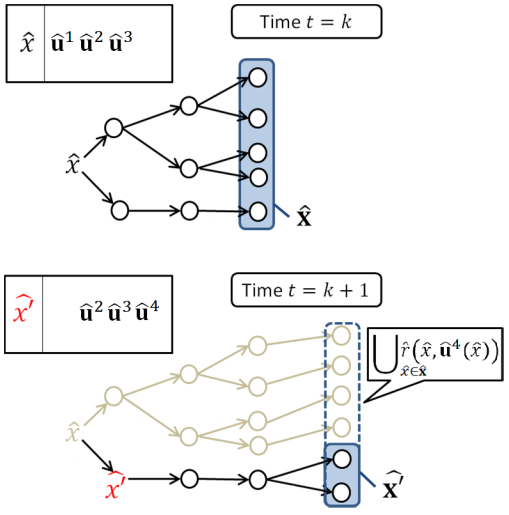

Fig. 2 The prediction is improved by considering reachable states from the latest measured state.

Then, the following relation $R_D(\epsilon) \subseteq \hat{X}_D \times X_D \times \hat{U}_D \times U_D$ is a (κ, β, λ)-acASR from $\hat{S}_D$ to S_D with d_D:

$$\begin{aligned}&R_D(\epsilon) = \\ &\{((\hat{x}, \hat{\mathbf{u}}^1, \ldots, \hat{\mathbf{u}}^L), (x, u^1, \ldots, u^L), (\hat{\mathbf{u}}_\mathbf{D}^1, \hat{\mathbf{u}}_\mathbf{D}^2), \\ &(u_D^1, u_D^2)) \in \hat{X}_D \times X_D \times \hat{U}_D \times U_D \mid [\hat{\mathbf{u}}_\mathbf{D}^1 = \hat{\mathbf{u}}^1] \wedge \\ &[u_D^1 = u^1] \wedge [(\hat{x}, x, \hat{\mathbf{u}}_\mathbf{D}^1(\hat{x}), u_D^1) \in R(\epsilon)] \wedge \\ &[\forall i \in \{1, 2, \ldots, L\} : u^i \in \mathcal{U}(\hat{\mathbf{u}}^i)] \wedge [u_D^2 \in \mathcal{U}(\hat{\mathbf{u}}_\mathbf{D}^2)]\}.\end{aligned} \tag{9}$$

Since each input $u^i \in U$ satisfies $u^i \in \mathcal{U}(\hat{\mathbf{u}}^i)$, the input u^i is valid at each predicted candidate in $\mathrm{dom}(\hat{\mathbf{u}}^i)$. Then, the determined input u_D^2 such that $u_D^2 \in \mathcal{U}(\hat{\mathbf{u}}_\mathbf{D}^2)$ is valid at each predicted state after the dead time is elapsed. This is essential for the prediction-based approach.

3.3 Deadlock-Free Symbolic Smith Controller

In order to determine a control input map that satisfies the specification, we introduce a system, denoted by $\hat{\mathbf{S}}_\mathbf{C}$, that is induced by $\hat{S}_C$. As in the case of $\hat{\mathbf{S}}$, each state of $\hat{\mathbf{S}}_\mathbf{C}$, denoted by $\hat{\mathbf{x}}_\mathbf{C}$, is a subset of $\hat{X}_C$ because $\hat{S}_C$ is generally nondeterministic. Let $\hat{\mathbf{U}}_\mathbf{C} = \bigcup_{\hat{\mathbf{x}}_\mathbf{C} \in \hat{\mathbf{X}}_\mathbf{C}} \hat{U}_C^{\hat{\mathbf{x}}_\mathbf{C}}$ be a set of all input mappings with respect to $\hat{\mathbf{X}}_\mathbf{C}$. Denoted by $\mathrm{dom}(\hat{\mathbf{u}}_\mathbf{C}) \subseteq \hat{X}_C$ is the domain of the input map $\hat{\mathbf{u}}_\mathbf{C}$. Then, we define a transition map $\hat{r}_C^e : \hat{\mathbf{X}}_\mathbf{C} \times \hat{\mathbf{U}}_\mathbf{C}^* \to \hat{\mathbf{X}}_\mathbf{C}$ induced by $\hat{r}_C : \hat{X}_C \times \hat{U}_C \to 2^{\hat{X}_C}$ as follows:

1. For each $\hat{\mathbf{x}}_\mathbf{C} \in \hat{\mathbf{X}}_\mathbf{C}$ and each $\hat{\mathbf{u}}_\mathbf{C} \in \hat{\mathbf{U}}_\mathbf{C}$,
$$\hat{r}_C^e(\hat{\mathbf{x}}_\mathbf{C}, \hat{\mathbf{u}}_\mathbf{C}) = \begin{cases} \bigcup_{\hat{x}_C \in \hat{\mathbf{x}}_\mathbf{C}} \hat{r}_C(\hat{x}_C, \hat{\mathbf{u}}_\mathbf{C}(\hat{x}_C)) \\ \qquad \text{if } \hat{\mathbf{x}}_\mathbf{C} = \mathrm{dom}(\hat{\mathbf{u}}_\mathbf{C}), \\ \emptyset \qquad \text{otherwise.} \end{cases}$$
2. For each $\hat{\mathbf{x}}_\mathbf{C} \in \hat{\mathbf{X}}_\mathbf{C}$, each input map sequence $\hat{\mathbf{t}}_\mathbf{C} \in \hat{\mathbf{U}}_\mathbf{C}^*$, and each input map $\hat{\mathbf{u}}_\mathbf{C} \in \hat{\mathbf{U}}_\mathbf{C}$,
$$\hat{r}_C^e(\hat{\mathbf{x}}_\mathbf{C}, \varepsilon) = \hat{\mathbf{x}}_\mathbf{C}; \text{ and}$$
$$\hat{r}_C^e(\hat{\mathbf{x}}_\mathbf{C}, \hat{\mathbf{t}}_\mathbf{C} \hat{\mathbf{u}}_\mathbf{C}) = \begin{cases} \bigcup_{\hat{x}'_C \in \hat{r}_C^e(\hat{\mathbf{x}}_\mathbf{C}, \hat{\mathbf{t}}_\mathbf{C})} \hat{r}_C(\hat{x}'_C, \hat{\mathbf{u}}_\mathbf{C}(\hat{x}'_C)) \\ \qquad \text{if } \hat{r}_C^e(\hat{\mathbf{x}}_\mathbf{C}, \hat{\mathbf{t}}_\mathbf{C}) = \mathrm{dom}(\hat{\mathbf{u}}_\mathbf{C}), \\ \emptyset \quad \text{otherwise.} \end{cases}$$
For simplicity, we write $\hat{r}_C^e(\hat{x}_C, \hat{\mathbf{u}}_\mathbf{C})$ for $\hat{r}_C^e(\{\hat{x}_C\}, \hat{\mathbf{u}}_\mathbf{C})$.

The system $\hat{\mathbf{S}}_\mathbf{C}$ is equivalent to $G_c[z]$ determining control inputs in the classical control theory. It is noticed that $\hat{S}_C$ is extended to consider nondeterministic transitions. Recall that the state of $\hat{\mathbf{S}}$ is L time steps forward compared with that of $\hat{S}$. In order to assign every predicted state to a control input satisfying the specification, it is necessary that the state of $\hat{\mathbf{S}}_\mathbf{C}$ is also L time steps forward with that of $\hat{S}_C$. Then, we impose the following assumption that refers to the synchronization between $\hat{\mathbf{S}}_\mathbf{C}$ and $\hat{\mathbf{S}}$ at the initial time.

Assumption 3 Consider $\hat{x}_0 \in \hat{X}_0$ and $\hat{\mathbf{u}}_\mathbf{0}^1 \hat{\mathbf{u}}_\mathbf{0}^2 \ldots \hat{\mathbf{u}}_\mathbf{0}^L$ ($\hat{\mathbf{u}}_\mathbf{0}^i \in \hat{\mathbf{U}}, i \in \{1, 2, \ldots, L\}$) satisfying (4). Then, there exist

$\hat{x}_{C0} \in \hat{X}_{C0}$ and $\hat{\mathbf{u}}^1_{\mathbf{C0}}\hat{\mathbf{u}}^2_{\mathbf{C0}}\dots\hat{\mathbf{u}}^L_{\mathbf{C0}}$ ($\hat{\mathbf{u}}^i_{\mathbf{C0}} \in \hat{\mathbf{U}}_{\mathbf{C}}, i \in \{1,2,\dots,L\}$) satisfying the following condition:

$$\begin{aligned}&\forall \hat{x}^L_0 \in \hat{r}^e(\hat{x}_0, \hat{\mathbf{u}}^1_{\mathbf{0}}\hat{\mathbf{u}}^2_{\mathbf{0}}\dots\hat{\mathbf{u}}^{L-1}_{\mathbf{0}}),\\ &\exists \hat{x}^L_{C0} \in \hat{r}^e_C(\hat{x}_{C0}, \hat{\mathbf{u}}^1_{\mathbf{C0}}\hat{\mathbf{u}}^2_{\mathbf{C0}}\dots\hat{\mathbf{u}}^{L-1}_{\mathbf{C0}}) :\\ &(\hat{x}^L_{C0}, \hat{x}^L_0, \hat{\mathbf{u}}^L_{\mathbf{C0}}(\hat{x}^L_{C0}), \hat{\mathbf{u}}^L_{\mathbf{0}}(\hat{x}^L_0)) \in \hat{R}_C.\end{aligned} \tag{10}$$

Note that, if $\hat{S}$ and $\hat{S}_C$ are finite transition systems, Assumption 3 can be tested in finite steps.

Definition 6 Under Assumption 3, we define a system

$$\hat{\mathbf{S}}_{\mathbf{C}} = (\hat{\mathbf{X}}_{\mathbf{C}}, \hat{\mathbf{X}}_{\mathbf{C0}}, \hat{\mathbf{U}}_{\mathbf{C}}, \hat{\mathbf{r}}_{\mathbf{C}}) \tag{11}$$

induced by $\hat{S}_C = (\hat{X}_C, \hat{X}_{C0}, \hat{U}_C, \hat{r}_C)$ with respect to $\hat{x}_{C0} \in \hat{X}_{C0}$ and $\hat{\mathbf{u}}^1_{\mathbf{C0}}\hat{\mathbf{u}}^2_{\mathbf{C0}}\dots\hat{\mathbf{u}}^L_{\mathbf{C0}}$ ($\hat{\mathbf{u}}^i_{\mathbf{C0}} \in \hat{\mathbf{U}}_{\mathbf{C}}, i \in \{1,2,\dots,L\}$) satisfying (10) where

- $\hat{\mathbf{X}}_{\mathbf{C0}} = \{\hat{r}^e_C(\hat{x}_{C0}, \hat{\mathbf{u}}^1_{\mathbf{C0}}\hat{\mathbf{u}}^2_{\mathbf{C0}}\dots\hat{\mathbf{u}}^L_{\mathbf{C0}})\} \subseteq \hat{\mathbf{X}}_{\mathbf{C}}$; and
- $\hat{\mathbf{r}}_{\mathbf{C}} : \hat{\mathbf{X}}_{\mathbf{C}} \times \hat{\mathbf{U}}_{\mathbf{C}} \to 2^{\hat{\mathbf{X}}_{\mathbf{C}}}$ is defined as follows:

$$\begin{aligned}&\hat{\mathbf{r}}_{\mathbf{C}}(\hat{\mathbf{x}}_{\mathbf{C}}, \hat{\mathbf{u}}_{\mathbf{C}})\\ &= \begin{cases} 2^{\hat{r}^e_C(\hat{\mathbf{x}}_{\mathbf{C}}, \hat{\mathbf{u}}_{\mathbf{C}})} \setminus \{\emptyset\} \\ \quad \text{if } \forall \hat{x}_C \in \hat{\mathbf{x}}_{\mathbf{C}} : \hat{r}^e_C(\hat{x}_C, \hat{\mathbf{u}}_{\mathbf{C}}) \neq \emptyset, \\ \emptyset \ \text{ otherwise.} \end{cases}\end{aligned}$$

Intuitively, $\hat{\mathbf{S}}_{\mathbf{C}}$ determines an input map such that, for every predicted state, there always exists a control input that satisfies the specification described in $\hat{S}_C$.

Finally, the following theorem shows the configuration of the symbolic Smith controller that is an extension of Theorem 1 to the case of delayed plants.

Theorem 2 Under Assumptions 1, 2, and 3, we construct $\hat{\mathbf{S}}$, given by Definition 4, w.r.t. $\hat{x}_0 \in \hat{X}_0$ and $\hat{\mathbf{u}}^1_{\mathbf{0}}\hat{\mathbf{u}}^2_{\mathbf{0}}\dots\hat{\mathbf{u}}^L_{\mathbf{0}}$ ($\hat{\mathbf{u}}^i_{\mathbf{0}} \in \hat{\mathbf{U}}, i \in \{1,2,\dots,L\}$) satisfying (4). Let $\hat{S}_D$ be a system given by Definition 5 and induced by $\hat{\mathbf{S}}$. We also construct $\hat{\mathbf{S}}_{\mathbf{C}}$, given by Definition 6, w.r.t. $\hat{x}_{C0} \in \hat{X}_{C0}$ and $\hat{\mathbf{u}}^1_{\mathbf{C0}}\hat{\mathbf{u}}^2_{\mathbf{C0}}\dots\hat{\mathbf{u}}^L_{\mathbf{C0}}$ ($\hat{\mathbf{u}}^i_{\mathbf{C0}} \in \hat{\mathbf{U}}_{\mathbf{C}}, i \in \{1,2,\dots,L\}$) satisfying (10). Consider the following relation $\hat{\mathbf{R}}_{\mathbf{C}} \subseteq \hat{\mathbf{X}}_{\mathbf{C}} \times \hat{\mathbf{X}} \times \hat{\mathbf{U}}_{\mathbf{C}} \times \hat{\mathbf{U}}$:

$$\begin{aligned}\hat{\mathbf{R}}_{\mathbf{C}} = \{&(\hat{\mathbf{x}}_{\mathbf{C}}, \hat{\mathbf{x}}, \hat{\mathbf{u}}_{\mathbf{C}}, \hat{\mathbf{u}}) \in \hat{\mathbf{X}}_{\mathbf{C}} \times \hat{\mathbf{X}} \times \hat{\mathbf{U}}_{\mathbf{C}} \times \hat{\mathbf{U}} \mid\\ &\forall \hat{x} \in \hat{\mathbf{x}}, \exists \hat{x}_C \in \hat{\mathbf{x}}_{\mathbf{C}} : (\hat{x}_C, \hat{x}, \hat{\mathbf{u}}_{\mathbf{C}}(\hat{x}_C), \hat{\mathbf{u}}(\hat{x})) \in \hat{R}_C\},\end{aligned} \tag{12}$$

and let $\mathbf{S}_{\mathbf{C}} := \hat{\mathbf{S}}_{\mathbf{C}} \times_{\hat{\mathbf{R}}_{\mathbf{C}}} \hat{\mathbf{S}} \times_{\hat{\mathbf{R}}} \hat{S}_D = (\mathbf{X}_{\mathbf{C}}, \mathbf{X}_{\mathbf{C0}}, \mathbf{U}_{\mathbf{C}}, \mathbf{r}_{\mathbf{C}})$. We introduce the following relation $\mathbf{R}_{\mathbf{C}}(\epsilon) \subseteq \mathbf{X}_{\mathbf{C}} \times X_D \times \mathbf{U}_{\mathbf{C}} \times U_D$:

$$\begin{aligned}&\mathbf{R}_{\mathbf{C}}(\epsilon) =\\ &\{((\hat{\mathbf{x}}_{\mathbf{C}}, \hat{\mathbf{x}}, \hat{x}_D), x_D, (\hat{\mathbf{u}}_{\mathbf{C}}, \hat{\mathbf{u}}, \hat{u}_D), u_D) \in \mathbf{X}_{\mathbf{C}} \times X_D \times \mathbf{U}_{\mathbf{C}} \times U_D \mid\\ &\ [(\hat{\mathbf{x}}_{\mathbf{C}}, \hat{\mathbf{x}}, \hat{\mathbf{u}}_{\mathbf{C}}, \hat{\mathbf{u}}) \in \hat{\mathbf{R}}_{\mathbf{C}}] \wedge [(\hat{\mathbf{x}}, \hat{x}_D, \hat{\mathbf{u}}, \hat{u}_D) \in \hat{\mathbf{R}}] \wedge\\ &\ [(\hat{x}_D, x_D, \hat{u}_D, u_D) \in R_D(\epsilon)]\}.\end{aligned} \tag{13}$$

Then, the pair $(\mathbf{S}_{\mathbf{C}}, \mathbf{R}_{\mathbf{C}}(\epsilon))$ is a controller for S_D given by Definition 3.

The proof is shown in Appendix.

Theorem 2 implies that a symbolic Smith controller is obtained by composing $\hat{\mathbf{S}}_{\mathbf{C}}$, $\hat{\mathbf{S}}$, and $\hat{S}_D$, which is summarized as follows:

1. When the current plant state x_D is measured, $\hat{S}_D$ updates the state $\hat{x}_D$ by the relation $R_D(\epsilon)$;
2. Based on the updated $\hat{x}_D$, $\hat{\mathbf{S}}$ updates the prediction $\hat{\mathbf{x}}$ by the relation $\hat{\mathbf{R}}$, and $\hat{\mathbf{S}}_{\mathbf{C}}$ updates the state $\hat{\mathbf{x}}_{\mathbf{C}}$ by the relation $\hat{\mathbf{R}}_{\mathbf{C}}$; and
3. $\mathbf{S}_{\mathbf{C}}$ determines a control input such that $(\hat{\mathbf{u}}_{\mathbf{C}}, \hat{\mathbf{u}}, \hat{u}_D) \in \mathbf{U}_{\mathbf{C}}((\hat{\mathbf{x}}_{\mathbf{C}}, \hat{\mathbf{x}}, \hat{x}_D))$.

This approach corresponds to the IMC form of the classical Smith controller shown in Fig. 1.

It is noted that $\mathbf{S}_{\mathbf{C}}$ may have deadlock states because the controller determines a common physical input that is valid at all predicted states. In order to compute a deadlock-free sub-transition system of $\mathbf{S}_{\mathbf{C}}$, we introduce the following operator $F : 2^{\mathbf{X}_{\mathbf{C}}} \to 2^{\mathbf{X}_{\mathbf{C}}}$: For any $W \subseteq \mathbf{X}_{\mathbf{C}}$,

$$\begin{aligned}F(W) = \{&\mathbf{x}_{\mathbf{C}} \in W \mid \exists \mathbf{u}_{\mathbf{C}} \in \mathbf{U}_{\mathbf{C}} : \mathbf{r}_{\mathbf{C}}(\mathbf{x}_{\mathbf{C}}, \mathbf{u}_{\mathbf{C}}) \neq \emptyset\\ &\wedge \mathbf{r}_{\mathbf{C}}(\mathbf{x}_{\mathbf{C}}, \mathbf{u}_{\mathbf{C}}) \subseteq W\}.\end{aligned} \tag{14}$$

By the definition of F, the following condition holds:

$$\begin{aligned}&\forall Z, \forall Z' \subseteq \mathbf{X}_{\mathbf{C}} :\\ &[F(Z) \subseteq Z] \wedge [Z' \subseteq Z \Rightarrow F(Z') \subseteq F(Z)],\end{aligned}$$

which means that F is monotonically decreasing. We consider the following iterations $\mathbf{X}^i_{\mathbf{C}}$ ($i \in \mathbb{N}$):

$$\mathbf{X}^0_{\mathbf{C}} = \mathbf{X}_{\mathbf{C}} \text{ and } \mathbf{X}^{i+1}_{\mathbf{C}} = F(\mathbf{X}^i_{\mathbf{C}}). \tag{15}$$

Then, for each $i \in \mathbb{N}$, we have $\mathbf{X}^i_{\mathbf{C}} \supseteq \mathbf{X}^{i+1}_{\mathbf{C}}$. If there exists $k \in \mathbb{N}$ such that $\mathbf{X}^{k+1}_{\mathbf{C}} = F(\mathbf{X}^k_{\mathbf{C}})$, we have the supremal fixed point $\mathbf{X}^*_{\mathbf{C}}$ of F by $\mathbf{X}^*_{\mathbf{C}} = \mathbf{X}^k_{\mathbf{C}}$. Note that if $\hat{S}_C$ and $\hat{S}$ are finite transition systems, such k always exists. If

$$\mathbf{X}^*_{\mathbf{C}} \cap \mathbf{X}_{\mathbf{C0}} \neq \emptyset \tag{16}$$

holds, we define a transition system

$$\mathbf{S}^*_{\mathbf{C}} = (\mathbf{X}^*_{\mathbf{C}}, \mathbf{X}^*_{\mathbf{C0}}, \mathbf{U}^*_{\mathbf{C}}, \mathbf{r}^*_{\mathbf{C}}), \tag{17}$$

where

- $\mathbf{X}^*_{\mathbf{C0}} = \mathbf{X}^*_{\mathbf{C}} \cap \mathbf{X}_{\mathbf{C0}}$;
- $\mathbf{U}^*_{\mathbf{C}} = \mathbf{U}_{\mathbf{C}}$; and
- $\mathbf{r}^*_{\mathbf{C}}(\mathbf{x}_{\mathbf{C}}, \mathbf{u}_{\mathbf{C}}) = \mathbf{r}_{\mathbf{C}}(\mathbf{x}_{\mathbf{C}}, \mathbf{u}_{\mathbf{C}}) \cap \mathbf{X}^*_{\mathbf{C}}$ for each $\mathbf{x}_{\mathbf{C}} \in \mathbf{X}^*_{\mathbf{C}}$ and $\mathbf{u}_{\mathbf{C}} \in \mathbf{U}^*_{\mathbf{C}}$.

$\mathbf{S}^*_{\mathbf{C}}$ is a deadlock-free sub-transition system of $\mathbf{S}_{\mathbf{C}}$. Let $\mathbf{R}^*_{\mathbf{C}}(\epsilon)$ be the restriction of $\mathbf{R}_{\mathbf{C}}(\epsilon)$ to $\mathbf{X}^*_{\mathbf{C}} \times X_D \times \mathbf{U}^*_{\mathbf{C}} \times U_D$. Then, it is obvious that $\mathbf{R}^*_{\mathbf{C}}(\epsilon)$ is a (κ, β, λ)-acASR from $\mathbf{S}^*_{\mathbf{C}}$ to $\mathbf{S}$ with $\mathsf{d}'_{\mathbf{C}}$, and the pair $(\mathbf{S}^*_{\mathbf{C}}, \mathbf{R}^*_{\mathbf{C}}(\epsilon))$ is a deadlock-free symbolic Smith controller for S_D.

Eliminating deadlock states is important in the proposed framework because we deal with nondeterminstic transition

systems, where prediction is based on listing all candidates of plant states after the deadtime is elapsed. In order to guarantee the satisfaction of the specification, it is necessary that a control input determined by a symbolic Smith controller is valid for all candidates listed by the predictor. Note that, if (16) does not hold, we cannot design a deadlock-free symbolic controller.

We will demonstrate the proposed approach in the next section using an example of on-off control via networks with some packet dropouts that may cause nondetermistic transitions to deadlock states.

4. Illustrative Example

We consider a liquid-level control problem with a tank as shown in Fig. 3. The control input is the close/open of the valve $u(t) \in \{0,1\}$ at each time step. The inflow velocity is given by $v_i(t) := \alpha u(t)$, where $\alpha \in \mathbb{R}_{>0}$ is a constant value. Let $x(t) \in [0, V_{max}]$ be the volume of the liquid in the tank, where $V_{max} \in \mathbb{R}_{>0}$ is the maximum capacity. The liquid surface height is given by $h(t) := \frac{x(t)}{A}$ with the surface area of the tank $A \in \mathbb{R}_{>0}$. The outflow velocity is given by $v_o(t) := \frac{h(t)}{R}$ with resistance $R \in \mathbb{R}_{>0}$. Then, the dynamics of the tank is given by

$$\begin{aligned} &x[k+1] \\ &= e^{-\frac{CT}{AR}} x[k] + \frac{\alpha ABR}{C}\left(1 - e^{-\frac{CT}{AR}}\right) u[k] + d[k], \end{aligned} \tag{18}$$

where B and $C \in \mathbb{R}_{>0}$ are the cross-sectional areas of the upper and lower pipe, respectively, $T \in \mathbb{R}_{>0}$ is a sampling period, and $d[k] \in \mathbb{R}$ is a random noise satisfying $|d[k]| < 0.5$ for all $k \in \mathbb{Z}_{\geq 0}$. First, we cast (18) as the system $S_1 = (X_1, X_{10}, U_1, r_1)$ where $X_1 = [0, V_{max}]$, $X_{10} = \{x_{10} \in X\}$, $U_1 = \{0,1\} \times [-0.5, 0.5]$ and $r_1 : X_1 \times U_1 \to X_1$ is defined as follows:

$$r_1(x_1, (u_1, d)) = \begin{cases} x_1' & \text{if } x_1' \in X_1, \\ V_{max} & \text{if } x_1' \geq V_{max}, \\ 0 & \text{if } x_1' \leq 0, \end{cases} \tag{19}$$

where $x_1' = e^{-\frac{CT}{AR}} x_1 + \frac{\alpha ABR}{C}\left(1 - e^{-\frac{CT}{AR}}\right) u_1 + d$.

Next, we consider a network between the controller and the plant. The control input is sent via an unreliable network with packet dropouts [11], and its dynamics is modeled by an automaton shown in Fig. 4. We use the system $S_2 = (X_2, X_{20}, U_2, r_2)$ where $X_2 = \{0,1\}$, $X_{20} = \{0\}$, $U_2 = \{\perp\}$, and $r_2 : X_2 \times U_2 \to 2^{X_2}$ is given in the obvious way to model the network behavior. If a data dropout occurs, i.e., $x_2 = 1$, the input signal is set to 0 automatically. On the other hand, if the data is successfully received by the actuator, i.e., $x_2 = 0$, the input determined by the controller is injected into the plant (after the dead time is elapsed). Then, the networked plant to be controlled $S = (X, X_0, U, r)$ is given by the composition of S_1 and S_2, i.e., $X := X_1 \times X_2$, $X_0 := X_{10} \times X_{20}$, and $U := U_1 \times U_2$. The transition map $r : X \times U \to 2^X$ is defined by $(x_1', x_2') \in r((x_1, x_2), ((u_1, d)u_2))$ iff

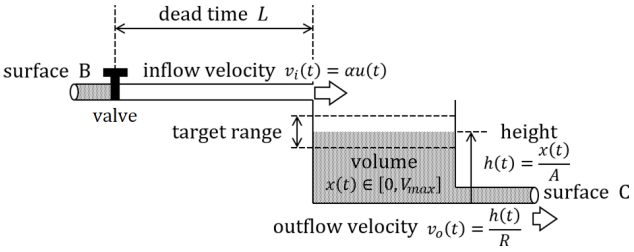

Fig. 3 The liquid-level control problem with a single tank.

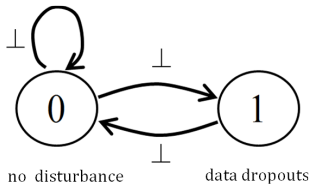

Fig. 4 Automaton model of dynamics of the communication channel.

$$x_1' \in \begin{cases} r_1(x_1, (u_1, d)) \cup r_1(x_1, (0, d)) & \text{if } x_2 = 0, \\ r_1(x_1, (u_1, d)) & \text{if } x_2 = 1; \text{ and} \end{cases} \tag{20}$$

$$x_2' \in r_2(x_2, u_2). \tag{21}$$

We construct an abstracted model $\hat{S}$ for S. First, we introduce the symbolic model of S_1, denoted by $\hat{S}_1 = (\hat{X}_1, \hat{X}_{10}, \hat{U}_1, \hat{r}_1)$ where $\hat{X}_1 = X_1 \cap \mathbb{Z}$, $\hat{X}_{10} = \max\arg\min_{\hat{x}_{10} \in \hat{X}_1} |x_{10} - \hat{x}_{10}|$, $\hat{U}_1 = \{0,1\}$, and $\hat{r}_1 : \hat{X}_1 \times \hat{U}_1 \to \hat{X}_1$ is defined as follows:

$$\hat{r}_1(\hat{x}_1, \hat{u}_1) = \begin{cases} \hat{x}_1' & \text{if } \hat{x}_1' \in \hat{X}, \\ \lfloor V_{max} \rfloor & \text{if } \hat{x}_1' \geq \lfloor V_{max} \rfloor, \\ 0 & \text{if } \hat{x}_1' \leq 0, \end{cases} \tag{22}$$

where

$$\hat{x}_1' = \max\arg\min_{\hat{x}_1' \in \hat{X}_1} \left| e^{-\frac{CT}{AR}} \hat{x}_1 + \frac{\alpha ABR}{C}\left(1 - e^{-\frac{CT}{AR}}\right) \hat{u}_1 - \hat{x}_1' \right|.$$

Let $\hat{S}_2 = (\hat{X}_2, \hat{X}_{20}, \hat{U}_2, \hat{r}_2)$, where $\hat{X}_2 = X_2$, $\hat{X}_{20} = X_{20}$, $\hat{U}_2 = U_2$, and $\hat{r}_2 = r_2$. Then, we have $\hat{S} = (\hat{X}, \hat{X}_0, \hat{U}, \hat{r})$ by the composition of $\hat{S}_1$ and $\hat{S}_2$, i.e., $\hat{X} := \hat{X}_1 \times \hat{X}_2$, $\hat{X}_0 := \hat{X}_{10} \times \hat{X}_{20}$, and $\hat{U} := \hat{U}_1 \times \hat{U}_2$. The transition map $\hat{r} : \hat{X} \times \hat{U} \to 2^{\hat{X}}$ is defined implicitly by $(\hat{x}_1', \hat{x}_2') \in \hat{r}((\hat{x}_1, \hat{x}_2), (\hat{u}_1, \hat{u}_2))$ iff

$$\hat{x}_1' \in \begin{cases} \hat{r}_1(\hat{x}_1, \hat{u}_1) \cup \hat{r}_1(\hat{x}_1, 0) & \text{if } \hat{x}_2 = 0, \\ \hat{r}_1(\hat{x}_1, \hat{u}_1) & \text{if } \hat{x}_2 = 1; \text{ and} \end{cases} \tag{23}$$

$$\hat{x}_2' \in \hat{r}_2(\hat{x}_2, \hat{u}_2). \tag{24}$$

It is easily proved that the following relation $R(\epsilon) \subseteq \hat{X} \times X \times \hat{U} \times U$ is a $(0.5, e^{-\frac{CT}{AR}}, 1)$-acASR from $\hat{S}$ to S with $\mathsf{d}(\hat{u}_1, (u_1, d)) = |d|$:

$$\begin{aligned} R(\epsilon) = \{&((\hat{x}_1, \hat{x}_2), (x_1, x_2), (\hat{u}_1, \hat{u}_2), ((u_1, d), u_2)) \\ &\in \hat{X} \times X \times \hat{U} \times U \mid [|x_1 - \hat{x}_1| \leq \epsilon] \wedge \\ &[x_2 = \hat{x}_2] \wedge [u_1 = \hat{u}_1] \wedge [u_2 = \hat{u}_2]\}. \end{aligned} \tag{25}$$

We want to keep the volume of the tank in the following range:

$$V_l \le \hat{x}_1 \le V_m. \tag{26}$$

Thus, we have the control specification $\hat{S}_C = (\hat{X}_C, \hat{X}_{C0}, \hat{U}_C, \hat{r}_C)$, where $\hat{X}_C = \hat{X}$, $\hat{X}_{C0} = \hat{X}_0$, $\hat{U}_C = \hat{U}$, and $\hat{r}_C : \hat{X}_C \times \hat{U}_C \to \hat{X}_C$ defined as follows:

$$\hat{r}_C((\hat{x}_{C1}, \hat{x}_{C2}), (\hat{u}_{C1}, \hat{u}_{C2})) = \begin{cases} (\hat{x}'_{C1}, \hat{x}'_{C2}) & \text{if } [V_l \le \hat{x}'_{C1}] \wedge [\hat{u}_{C1} = 0], \\ (\hat{x}'_{C1}, \hat{x}'_{C2}) & \text{if } [\hat{x}'_{C1} \le V_m] \wedge [\hat{u}_{C1} = 1], \\ \emptyset & \text{otherwise,} \end{cases} \tag{27}$$

where $(\hat{x}'_{C1}, \hat{x}'_{C2}) \in \hat{r}((\hat{x}_{C1}, \hat{x}_{C2}), (\hat{u}_{C1}, \hat{u}_{C2}))$. $\hat{S}_C$ describes the target volume range (26) and determines a control input. Intuitively, (27) implies that, if the volume is above (resp. under) the target range (26), the valve should be closed (resp. opened). If the volume is in the target range (26), the valve can be opened or closed nondeterministically. Then, it is easily proved that the following relation $\hat{R}_C \subseteq \hat{X}_C \times \hat{X} \times \hat{U}_C \times \hat{U}$ is an ASR from $\hat{S}_C$ to $\hat{S}$:

$$\hat{R}_C = \{(\hat{x}_C, \hat{x}, \hat{u}_C, \hat{u}) \in \hat{X}_C \times \hat{X} \times \hat{U}_C \times \hat{U} \mid \hat{x} = \hat{x}_C \ \wedge \ \hat{u} = \hat{u}_C\}. \tag{28}$$

Now, Assumption 1 is satisfied. Theorem 1 implies that, letting $S_C := \hat{S}_C \times_{R_C(\epsilon)} \hat{S} = (X_C, X_{C0}, U_C, r_C)$ where the relation $R_C(\epsilon) \subseteq X_C \times X \times U_C \times U$ is defined by (2), the pair $(S_C, R_C(\epsilon))$ is a symbolic feedback controller for S if there is no dead time between the controller and the plant.

Consider the case where the place of the valve is far from the tank, and there exists an input dead time $L \in \mathbb{N}$. We set the parameters as follows.

α	V_{max}	X_0	A	B	C	R	T	V_l	V_m	L
10	35	$\{(0,0)\}$	30	10	10	0.1	0.1	10	25	2

Then, by the existence of the dead time, the synchronization of the controller $(S_C, R_C(\epsilon))$ and the delayed plant S_D fails, which means that the control specification is not satisfied. Thus, we design a symbolic Smith controller that satisfies the control specification. We consider the first L time steps input map sequences $\hat{\mathbf{u}}_\mathbf{0}^1 \hat{\mathbf{u}}_\mathbf{0}^2 \dots \hat{\mathbf{u}}_\mathbf{0}^L$ $(\hat{\mathbf{u}}_\mathbf{0}^i \in \hat{\mathbf{U}}, i \in \{1, 2, \dots, L\})$ and $\hat{\mathbf{u}}_{\mathbf{C0}}^1 \hat{\mathbf{u}}_{\mathbf{C0}}^2 \dots \hat{\mathbf{u}}_{\mathbf{C0}}^L$ $(\hat{\mathbf{u}}_{\mathbf{C0}}^i \in \hat{\mathbf{U}}_\mathbf{C}, i \in \{1, 2, \dots, L\})$ as follows:

$$\hat{\mathbf{u}}_\mathbf{0}^1 \, \hat{\mathbf{u}}_\mathbf{0}^2 \ \dots \ \hat{\mathbf{u}}_\mathbf{0}^L = \mathbf{0}\,\mathbf{0} \ \dots \ \mathbf{0}; \text{ and} \tag{29}$$

$$\hat{\mathbf{u}}_{\mathbf{C0}}^1 \, \hat{\mathbf{u}}_{\mathbf{C0}}^2 \ \dots \ \hat{\mathbf{u}}_{\mathbf{C0}}^L = \mathbf{0}\,\mathbf{0} \ \dots \ \mathbf{0}, \tag{30}$$

where $\mathbf{0}$ is a zero map that assigns every state to the input 0. Intuitively, (29) and (30) imply that the valve is closed at the initial time. Since $x_0 = \hat{x}_0 = \hat{x}_{C0} = 0$ holds, it is easily proved that $\hat{\mathbf{u}}_\mathbf{0}^1 \hat{\mathbf{u}}_\mathbf{0}^2 \dots \hat{\mathbf{u}}_\mathbf{0}^L$ with $\hat{x}_0 \in \hat{X}_0$ and $\hat{\mathbf{u}}_{\mathbf{C0}}^1 \hat{\mathbf{u}}_{\mathbf{C0}}^2 \dots \hat{\mathbf{u}}_{\mathbf{C0}}^L$ with $\hat{x}_{C0} \in \hat{X}_{C0}$ satisfy (4) and (10), respectively. Note that, in this case, every predicted state implies that the tank is empty. We construct $\hat{\mathbf{S}}$ w.r.t. $\hat{x}_0$ and $\hat{\mathbf{u}}_\mathbf{0}^i$ $(i \in \{1, 2, \dots, L\})$ given by (29). $\hat{S}_D$ is induced by $\hat{\mathbf{S}}$. We also construct $\hat{\mathbf{S}}_\mathbf{C}$ w.r.t. $\hat{x}_{C0}$ and $\hat{\mathbf{u}}_{\mathbf{C0}}^i$ $(i \in \{1, 2, \dots, L\})$ given by (30). Let $\mathbf{S_C} := \hat{\mathbf{S}}_\mathbf{C} \times_{\hat{\mathbf{R}}_\mathbf{C}} \hat{\mathbf{S}} \times_{\hat{\mathbf{R}}} \hat{S}_D$ where the relations $\hat{\mathbf{R}}_\mathbf{C} \subseteq \hat{\mathbf{X}}_\mathbf{C} \times \hat{\mathbf{X}} \times \hat{\mathbf{U}}_\mathbf{C} \times \hat{\mathbf{U}}$ and $\hat{\mathbf{R}} \subseteq \hat{\mathbf{X}} \times \hat{X}_D \times \hat{\mathbf{U}} \times \hat{U}_D$ are given by (12) and (7), respectively. Finally, by Theorem 2, it is concluded that the pair $(\mathbf{S_C}, \mathbf{R_C}(\epsilon))$ is a symbolic Smith controller for S_D, where the relation $\mathbf{R_C}(\epsilon) \subseteq \mathbf{X_C} \times X_D \times \mathbf{U_C} \times U_D$ is given by (13). In this case, (16) is satisfied, and we have the deadlock-free controller $(\mathbf{S}_\mathbf{C}^*, \mathbf{R}_\mathbf{C}^*(\epsilon))$. We simulated behaviors of the controlled plant with random occurrences of the packet dropouts shown in Fig. 5. Then, the time response of the plant volume x_1 is shown in Fig. 6. The line in the figure shows the plant state x_1 and each dot is its corresponding abstracted plant state $\hat{x}_1$. Since there is no deadlock, the control inputs are successfully chosen in terms of the specification despite of random noises and data dropouts.

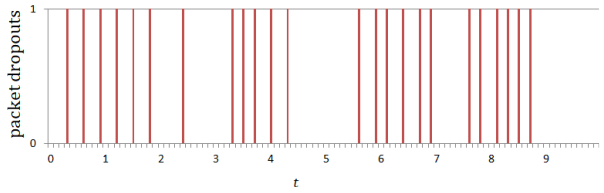

Fig. 5 The occurrences of the packet dropouts.

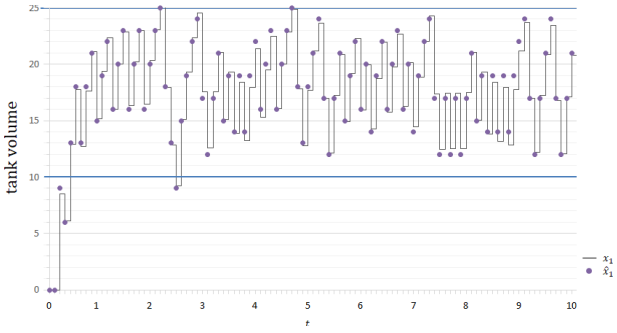

Fig. 6 The time response of the volume of the tank x_1 and $\hat{x}_1$.

It is noticed that x_1 is sometimes out of the target range due to the packet dropouts. We do not ensure that the plant volume always stays in the target range $V_l \le \hat{x}_1 \le V_m$. Instead, we have designed a controller that issues a control input so as to enforce the tank volume to the target range under the nondeterministic transitions. It is shown that a kind of input-to-state stability evaluating the robustness of sporadic disturbances such as packet dropouts is guaranteed by a controller designed based on acASRs [10]–[12]. It is future work to investigate the stability by introducing quantitative input and output maps.

Let us consider another case. The dead time L has been changed to 3.

α	V_{max}	X_0	A	B	C	R	T	V_l	V_m	L
10	35	$\{(0,0)\}$	30	10	10	0.1	0.1	10	25	3

In this case, (16) is not satisfied, then we do not have the deadlock-free controller. Thus, the controller $(\mathbf{S_C}, \mathbf{R_C}(\epsilon))$ reaches a dead lock state where there is no control input such

that every predicted state satisfies the specification. In other words, in this case, the specification is too restrictive for the delayed plant. Intuitively, for the design of a deadlock-free controller, all of the predicted states should be under V_m or over V_l to select a common control input in this example.

5. Conclusion

We design a deadlock-free symbolic Smith controller for a plant with an input dead time on the premise of a given control specification for the abstracted model of the plant. As in the case of the classical Smith controller, the proposed controller determines a control input by prediction. Since the control specification is satisfied at every predicted state by the control input, the controller may have deadlock states. Then, we introduce an operator that eliminates transitions to the deadlock states. If we obtain a deadlock-free controller, it is shown that the effects of the dead time is suppressed and that the specification is satisfied. If the deadlock-free controller does not exist, the specification must be relaxed.

It is future work to investigate the input-to-state stability of the controlled plant quantitatively by introducing cost functions. An extension of the proposed framework is also considerable to the case where a control specification for the plant (not for the abstracted plant model) is given directly.

References

[1] Z. Palmor, "Time-delay compensation — Smith predictor and its modifications," The Control Handbook, vol.1, pp.224–229, 1996.
[2] O. Smith, "Closer control of loops with dead time," Chemical Engineering Progress, vol.53, no.5, pp.217–219, 1957.
[3] G. Alevisakis and D. Seborg, "Control of multivariable systems containing time delays using a multivariable Smith predictor," Chemical Engineering Science, vol.29, no.2, pp.373–380, 1974.
[4] M. Mataušek and A. Micić, "A modified Smith predictor for controlling a process with an integrator and long dead-time," IEEE Trans. Autom. Control, vol.41, no.8, pp.1199–1203, 1996.
[5] C. Kravaris and R. Wright, "Deadtime compensation for nonlinear processes," AIChE J., vol.35, no.9, pp.1535–1542, 1989.
[6] Z. Palmor and Y. Halevi, "Robustness properties of sampled-data systems with dead time compensators," Automatica, vol.26, no.3, pp.637–640, 1990.
[7] P. Tabuada, Verification and Control of Hybrid Systems: A Symbolic Approach, 1st ed., Springer, 2009.
[8] C. Cassandras and S. Lafortune, Introduction to Discrete Event Systems, 2nd ed., Springer, 2009.
[9] R. Goebel, R. Sanfelice, and A. Teel, Hybrid Dynamical Systems: Modeling, Stability, and Robustness, Princeton University Press, 2012.
[10] G. Pola and P. Tabuada, "Symbolic models for nonlinear control systems: Alternating approximate bisimulations," SIAM J. Control and Optim., vol.48, no.2, pp.719–733, 2009.
[11] M. Rungger and P. Tabuada, "A notion of robustness for cyber-physical systems," IEEE Trans. Autom. Control, vol.61, no.8, pp.2108–2123, Aug. 2016.
[12] P. Tabuada, S. Caliskan, M. Rungger, and R. Majumdar, "Towards robustness for cyber-physical systems," IEEE Trans. Autom. Control, vol.59, no.12, pp.3151–3163, Dec. 2014.
[13] M. Mizoguchi and T. Ushio, "Observer-based similarity output feedback control of cyber-physical systems," Proc. 5th IFAC Conference on Analysis and Design of Hybrid Systems, pp.248–253, Oct. 2015.
[14] M. Mizoguchi and T. Ushio, "Output feedback controller design with symbolic observers for cyber-physical systems," Proc. 1st International Workshop on Verification and Validation of Cyber-Physical Systems, pp.37–51, June 2016.
[15] M. Mizoguchi and T. Ushio, "Deadlock-free output feedback controller design based on approximately abstracted observers," Nonlinear Analysis: Hybrid Systems, vol.30, pp.58–71, 2018.
[16] M. Mizoguchi and T. Ushio, "Symbolic control of systems with dead times using symbolic Smith predictors," Proc. 55th IEEE Conference on Decision and Control, pp.5726–5731, Dec. 2016.
[17] M. Mizoguchi and T. Ushio, "Symbolic design of networked control systems with state prediction," IEICE Trans. Inf. & Syst., vol.E100-D, no.6, pp.1158–1165, June 2017.
[18] M. Zamani, M. Mazo, M. Khaled, and A. Abate, "Symbolic abstractions of networked control systems," IEEE Trans, Control Netw. Syst., vol.5, no.4, pp.1622–1634, 2018.
[19] A. Borri, G. Pola, and M.D.D. Benedetto, "Design of symbolic controllers for networked control systems," IEEE Trans. Autom. Control, vol.64, no.3, pp.1034–1046, 2019.
[20] G. Pola, P. Pepe, and M.D.D. Benedetto, "Symbolic models for networks of control systems," IEEE Trans. Autom. Control, vol.61, no.11, pp.3663–3668, Nov. 2016.
[21] A. Borri, G. Pola, and M.D. Di Benedetto, "A symbolic approach to the design of nonlinear networked control systems," Proc. 15th International Conference on Hybrid Systems: Computation and Control, pp.255–264, April 2012.
[22] A. Borri, G. Pola, and M.D. Di Benedetto, "Integrated symbolic design of unstable nonlinear networked control systems," Proc. 51st IEEE Conference on Decision and Control, pp.1374–1379, Dec. 2012.
[23] A. Borri, G. Pola, and M.D. Di Benedetto, "Symbolic control design of nonlinear networked control systems," arXiv preprint arXiv:1404.0237, 2014.

Appendix: Proof of Theorem 2

Proof We introduce a map $\mathsf{d}'_{\mathsf{C}} : \mathbf{U_C} \times U_D \to \mathbb{R}_{\geq 0}$:

$$\mathsf{d}'_{\mathsf{C}}((\hat{\mathbf{u}}_{\mathbf{C}}, \hat{\mathbf{u}}, \hat{u}_D), u_D) = \mathsf{d}_D(\hat{u}_D, u_D)$$

and show that $\mathbf{R_C}(\epsilon)$ satisfies conditions of a (κ, β, λ)-acASR from $\mathbf{S_C}$ to S_D with d'_{C}.

1. Consider any $(\hat{\mathbf{x}}_{\mathbf{C0}}, \hat{\mathbf{x}}_{\mathbf{0}}, \hat{x}_{D0}) \in \mathbf{X_{C0}}$. Then, we have

$$[(\hat{\mathbf{x}}_{\mathbf{C0}}, \hat{\mathbf{x}}_{\mathbf{0}}) \in \hat{\mathbf{R}}_{\mathbf{C}X}] \wedge [(\hat{\mathbf{x}}_{\mathbf{0}}, \hat{x}_{D0}) \in \hat{\mathbf{R}}_X].$$

   Since $R_D(\epsilon)$ is a (κ, β, λ)-acASR from $\hat{S}_D$ to S_D, there exists $x_{D0} \in X_{D0}$ such that $(\hat{x}_{D0}, x_{D0}) \in R_{DX}(\kappa)$ holds. By the definition of $\mathbf{R_C}(\epsilon)$, we have

$$((\hat{\mathbf{x}}_{\mathbf{C0}}, \hat{\mathbf{x}}_{\mathbf{0}}, \hat{x}_{D0}), x_{D0}) \in \mathbf{R}_{\mathbf{C}X}(\kappa).$$

2. First, consider any $((\hat{\mathbf{x}}_{\mathbf{C}}, \hat{\mathbf{x}}, \hat{x}_D), x_D) \in \mathbf{R}_{\mathbf{C}X}(\epsilon)$, and choose any $(\hat{\mathbf{u}}_{\mathbf{C}}, \hat{\mathbf{u}}, \hat{u}_D) \in \mathbf{U_C}((\hat{\mathbf{x}}_{\mathbf{C}}, \hat{\mathbf{x}}, \hat{x}_D))$. Then, we have

$$[(\hat{\mathbf{x}}_{\mathbf{C}}, \hat{\mathbf{x}}, \hat{\mathbf{u}}_{\mathbf{C}}, \hat{\mathbf{u}}) \in \hat{\mathbf{R}}_{\mathbf{C}}] \wedge [(\hat{\mathbf{x}}, \hat{x}_D, \hat{\mathbf{u}}, \hat{u}_D) \in \hat{\mathbf{R}}] \wedge [(\hat{x}_D, x_D) \in R_{DX}(\epsilon)].$$

   Since $R_D(\epsilon)$ is a (κ, β, λ)-acASR from $\hat{S}_D$ to S_D, there exists $u_D \in U_D(x_D)$ such that $(\hat{x}_D, x_D, \hat{u}_D, u_D) \in R_D(\epsilon)$. Thus, by the definition of $\mathbf{R_C}(\epsilon)$, the following condition holds:

$$((\hat{\mathbf{x}}_\mathbf{C}, \hat{\mathbf{x}}, \hat{x}_D), x_D, (\hat{\mathbf{u}}_\mathbf{C}, \hat{\mathbf{u}}, \hat{u}_D), u_D) \in \mathbf{R}_\mathbf{C}(\epsilon).$$

Next, consider any $x'_D \in r_D(x_D, u_D)$. By the (κ, β, λ)-acASR $R_D(\epsilon)$, there exists $\hat{x}'_D \in \hat{r}_D(\hat{x}_D, \hat{u}_D)$ such that $(\hat{x}'_D, x'_D) \in R_{DX}(\kappa + \beta\epsilon + \lambda \mathsf{d}_D(\hat{u}_D, u_D))$. Since $\hat{\mathbf{R}}$ is an ASR from $\hat{\mathbf{S}}$ to $\hat{S}_D$, there exists $\hat{\mathbf{x}}' \in \hat{\mathbf{r}}(\hat{\mathbf{x}}, \hat{\mathbf{u}})$ such that $(\hat{\mathbf{x}}', \hat{x}'_D) \in \hat{\mathbf{R}}_X$. In addition, the definition of $\hat{\mathbf{R}}_\mathbf{C}$ implies the following condition:

$$\forall \hat{x} \in \hat{\mathbf{x}}, \exists \hat{x}_C \in \hat{\mathbf{x}}_\mathbf{C} : (\hat{x}_C, \hat{x}, \hat{\mathbf{u}}_\mathbf{C}(\hat{x}_C), \hat{\mathbf{u}}(\hat{x})) \in \hat{R}_C.$$

Since $\hat{R}_C$ is an ASR from $\hat{S}_C$ to $\hat{S}$, we have

$$\begin{aligned} \forall \hat{x}' \in \hat{r}^e(\hat{\mathbf{x}}, \hat{\mathbf{u}}),\ \exists \hat{x}'_C \in \hat{r}^e_C(\hat{\mathbf{x}}_\mathbf{C}, \hat{\mathbf{u}}_\mathbf{C}) :& \\ (\hat{x}'_C, \hat{x}') \in \hat{R}_{CX}.& \end{aligned} \tag{A·1}$$

On the other hand, the definition of $\hat{\mathbf{r}}$ implies the following condition:

$$\hat{\mathbf{x}}' \subseteq \hat{r}^e(\hat{\mathbf{x}}, \hat{\mathbf{u}}),$$

and by the definition of $\hat{\mathbf{r}}_\mathbf{C}$, we have

$$\hat{\mathbf{r}}_\mathbf{C}(\hat{\mathbf{x}}_\mathbf{C}, \hat{\mathbf{u}}_\mathbf{C}) = 2^{\hat{r}^e_C(\hat{\mathbf{x}}_\mathbf{C}, \hat{\mathbf{u}}_\mathbf{C})} \setminus \{\emptyset\}.$$

Thus, from (A·1), there always exists $\hat{\mathbf{x}}'_\mathbf{C} \in \hat{\mathbf{r}}_\mathbf{C}(\hat{\mathbf{x}}_\mathbf{C}, \hat{\mathbf{u}}_\mathbf{C})$ satisfying

$$\begin{aligned} \forall \hat{x}' \in \hat{\mathbf{x}}',\ \exists \hat{x}'_C \in \hat{\mathbf{x}}'_\mathbf{C} :\ (\hat{x}'_C, \hat{x}') \in \hat{R}_{CX}& \\ \Leftrightarrow (\hat{\mathbf{x}}'_\mathbf{C}, \hat{\mathbf{x}}') \in \hat{\mathbf{R}}_{\mathbf{C}X}.& \end{aligned}$$

Finally, by the definition of the composed system, we have

$$(\hat{\mathbf{x}}'_\mathbf{C}, \hat{\mathbf{x}}', \hat{x}'_D) \in \mathbf{r}_\mathbf{C}((\hat{\mathbf{x}}_\mathbf{C}, \hat{\mathbf{x}}, \hat{x}_D), (\hat{\mathbf{u}}_\mathbf{C}, \hat{\mathbf{u}}, \hat{u}_D)).$$

Thus, by the definitions of $\mathbf{R}_\mathbf{C}(\epsilon)$ and d'_C, the following condition holds:

$$\begin{aligned} &((\hat{\mathbf{x}}'_\mathbf{C}, \hat{\mathbf{x}}', \hat{x}'_D), x'_D) \\ &\quad \in \mathbf{R}_{\mathbf{C}X}(\kappa + \beta\epsilon + \lambda \mathsf{d}'_\mathsf{C}((\hat{\mathbf{u}}_\mathbf{C}, \hat{\mathbf{u}}, \hat{u}_D), u_D)). \end{aligned}$$

Therefore, $\mathbf{R}_\mathbf{C}(\epsilon)$ defined by (13) is a (κ, β, λ)-acASR from $\mathbf{S}_\mathbf{C}$ to S_D with d'_C, and the pair $(\mathbf{S}_\mathbf{C}, \mathbf{R}_\mathbf{C}(\epsilon))$ is a controller for S_D. □

Masashi Mizoguchi received B.S. and M.S. degrees in 2015 and 2017 from Osaka University. His research is symbolic synthesis based on the approximate abstraction.

Toshimitsu Ushio received B.S., M.S. and Ph.D. degrees in 1980, 1982 and 1985, respectively, from Kobe University. He was a Research Assistant at the University of California, Berkeley in 1985. From 1986 to 1990, he was a Research Associate in Kobe University, and became a Lecturer at Kobe College in 1990. He joined Osaka University as an Associate Professor in 1994, and is currently a Professor. His research interests include control of discrete event and hybrid systems and analysis of nonlinear systems. He is a member of SICE, ISCIE, and IEEE.