Bounding Errors Due to Switching Delays in Incrementally Stable Switched Systems ⋆

Kengo Kido [*] **Sean Sedwards** [**] **Ichiro Hasuo** [***]

[*] *University of Tokyo & JSPS Research Fellow, Tokyo, Japan*
[**] *University of Waterloo, Waterloo, ON, Canada*
[***] *National Institute of Informatics, Tokyo, Japan*

Abstract: *Time delays* pose an important challenge in networked control systems, which are now ubiquitous. Focusing on switched systems, we introduce a framework that provides an upper bound for errors caused by switching delays. Our framework is based on *approximate bisimulation*, a notion that has been previously utilized mainly for symbolic (discrete) abstraction of state spaces. Notable in our framework is that, in deriving an approximate bisimulation and thus an error bound, we use a simple incremental stability assumption (namely δ-GUAS) that does not itself refer to time delays. That this is the same assumption used for state-space discretization enables a *two-step workflow* for control synthesis for switched systems, in which a single Lyapunov-type stability certificate serves for two different purposes of state discretization and coping with time delays. We demonstrate the proposed framework with a boost DC-DC converter, a common example of switched systems.

Keywords: Switched system, delay, incremental stability, synthesis, approximate bisimulation

1. INTRODUCTION

Time Delays *Networked control* represents an important aspect in various emerging system design paradigms, such as cyber-physical systems and the Internet of Things. Consequently, identifying and addressing challenges inherent in networked control has become a crucial part of the design of reliable real-world systems.

One of the biggest challenge in networked control is *time delay*, which is also called *jitter*. Physical separation of plants from controllers leads to inevitable communication delays. Worse, the rise of *cloud control* is making both physical and logical distances between components even longer and more unpredictable. Precise estimation of communication delays is often hard, let alone reducing them.

These trends in control engineering call for a uniform framework for robustness against potential time delays. In this paper, inspired by the hybrid nature of systems that is intrinsic to networked control, we turn to *approximate bisimulation* for coping with delays.

Approximate Bisimulation An approximate bisimulation is a binary relation between states of two systems, that witnesses the proximity of the systems' behaviors. The notion was first introduced in Girard and Pappas (2007) as a quantitative relaxation of *bisimulation*, a well-established coinductive equivalence notion between discrete transition systems.

⋆ Thanks are due to Georgios Fainekos, Krzysztof Czarnecki, Toshimitsu Ushio and the anonymous reviewers for helpful discussions and comments. The authors are supported by JST ERATO HASUO Metamathematics for Systems Design Project (No. JPMJER1603), and JSPS Grant-in-Aid No. 15K11984. K.K. is supported by Grant-in-Aid for JSPS Fellows No. 15J05580.

Approximate bisimulation has been actively studied ever since: a notable theoretical result is its connection to *incremental stability* in Pola et al. (2008); on the application side, it has been widely used in (discretized) *symbolic abstraction* of continuous systems. See Girard and Pappas (2011) for an overview.

In this paper we focus on switched systems, and use an approximate bisimulation for error bounds between: a system Σ_{τ,δ_0} with bounded time delays; and the corresponding system Σ_τ without delays. The choice of switched systems as our subject is justified by the envisaged applications in networked control. In a switched system, a plant has finitely many operation modes and mode changes are dictated by a switching signal that is sent from a controller.

Approximate Bisimulation for Switching Delays Our contributions in technical terms are as follows. Our system model Σ_{τ,δ_0} is a (potentially nonlinear) switched system where switching signals are nearly periodic with a period τ; the system exhibits potential switching delays within a prescribed bound δ_0. Our interest is in the difference between the behaviors of Σ_{τ,δ_0} and those of the delay-free simplification Σ_τ. We turn the two systems into (discrete-time) transition systems $T(\Sigma_{\tau,\delta_0})$ and $T(\Sigma_\tau)$; between them we establish an approximate bisimulation that witnesses proximity of their behaviors. The approximate bisimulation is derived from an *incremental stability* assumption of the dynamics of the system Σ_{τ,δ_0}, namely *δ-GUAS*. More specifically, we present a construction that turns a Lyapunov-type certificate for δ-GUAS into an approximate bisimulation.

Our workflow resembles those in existing works about the use of approximate bisimulation. That is, 1) starting from an incrementally stable system T, one devises an

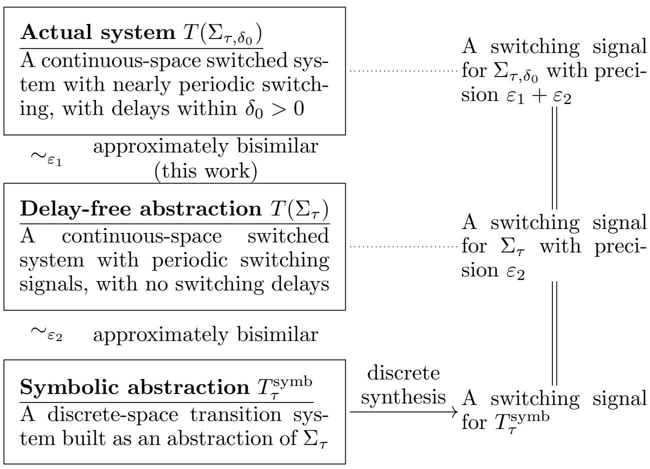

Fig. 1. A two-step control synthesis workflow for switched systems with delays.

abstraction T^{abst} of the system; and 2) one establishes an approximate bisimulation between T and T^{abst} out of a Lyapunov-like certificate of stability. Then the outcome of analysis of T^{abst} (verification, control synthesis, etc.) can be carried over to the original system T, modulo the error bounded by the approximate bisimulation.

One novelty of the current work is that, unlike most of the existing works that aim at a symbolic (discrete) abstraction of a state space, our abstraction $T^{\mathrm{abst}} = \Sigma_\tau$ is a *temporally* idealized system without switching delays.

Lyapunov-like certificates of stability, for the purpose of bounding errors caused by time delays, have already been used in the works by Pola et al. (2010a,b). Compared to these existing works, the current work is distinguished in that we rely only on a standard and relatively simple notion of stability, that does not refer to time delays per se. Indeed, what we rely on is δ-GUAS—the same stability notion used for state-space discretization in many existing works. [1] The abundance of analyses of δ-GUAS in the literature (e.g. Girard (2010); Girard et al. (2010); Pola et al. (2008)) suggests that our use of it is an advantage when it comes to application to various concrete systems. See §7 for further discussions on related work.

Two-Step Control Synthesis for Switched Systems with Delays Even better, our reliance on δ-GUAS enables the following two-step synthesis workflow, where we combine the current results and those in Girard et al. (2010). See Fig. 1. Our results derive the first error bound ε_1 between the original system Σ_{τ,δ_0} and the delay-free abstraction Σ_τ. The latter system Σ_τ is a delay-free periodic switched system, to which we can apply the state-space discretization technique in Girard et al. (2010). We thus construct a discretized symbolic model T_τ^{symb} and establish the second approximate bisimulation $\sim_{\varepsilon_2}$ in Fig. 1. The fact that our construction relies on the same stability assumptions used in Girard et al. (2010) means the following: for establishing both of the approximate bisimulations $\sim_{\varepsilon_1}$ and $\sim_{\varepsilon_2}$, we can reuse the same Lyapunov function, instead of finding two different Lyapunov functions.

[1] We also identify additional technical constraints besides δ-GUAS (such as Assumption 5.1) that are unique to the current setting.

Once we obtain a symbolic model, we can apply to it various discrete techniques, such as supervisory control of discrete event systems (as in Ramadge and Wonham (1987)). This is the horizontal arrow at the bottom of Fig. 1. The resulting controller (i.e. a switching signal, in the current setting) is then guaranteed, by the two approximate bisimulations, to work well with Σ_τ (with precision ε_2) and with Σ_{τ,δ_0} (with precision $\varepsilon_1 + \varepsilon_2$). [2]

This way we ultimately derive a switching signal for the original system Σ_{τ,δ_0} whose precision $\varepsilon_1 + \varepsilon_2$ is guaranteed. The workflow in Fig. 1 takes two steps that separate concerns (namely time delays and discretization of state spaces). While this two-step approach can potentially lead to loss of generality (especially in comparison with Pola et al. (2010a), see §7), it seems to help coping with the problem's complexity. We demonstrate our workflow in §6, where we successfully derive a controller for a boost DC-DC converter example with additional switching delays.

Contributions Overall, our contributions are summarized as follows. We present a construction of an approximate bisimulation between a nearly-periodic switched systems and its (exactly) periodic approximation. This allows us to bound the difference between trajectories due to switching delays. Thanks to our focus on switched systems we can use a common stability assumption (namely δ-GUAS) as the ingredient of the construction; this allows us to combine the current results with the existing results on symbolic abstraction and control synthesis, leading to a two-step control synthesis workflow (Fig. 1) where the same stability analysis derives two approximate bisimulations.

We focus on common δ-GAS Lyapunov function certificates of δ-GUAS in this paper. The case where multiple δ-GAS Lyapunov functions are given is deferred to the extended version (Kido et al. (2017)). An example using multiple δ-GAS Lyapunov functions is also presented in the extended version. We also defer the proofs in §5.

2. SWITCHED SYSTEMS

The set of nonnegative real numbers is denoted by $\mathbb{R}^+$. We let $\|\_\|$ denote the usual Euclidean norm on $\mathbb{R}^n$.

Definition 2.1. (switched system). A *switched system* is a quadruple $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$ that consists of 1) a *state space* $\mathbb{R}^n$; 2) a finite set $P = \{1, 2, \ldots, m\}$ of *modes*; 3) a set of *switching signals* $\mathcal{P} \subseteq \mathcal{S}(\mathbb{R}^+, P)$, where $\mathcal{S}(\mathbb{R}^+, P)$ is the set of functions from $\mathbb{R}^+$ to P that are piecewise constant, continuous from the right and non-Zeno; and 4) a set of vector fields $F = \{f_1, f_2, \ldots, f_m\}$ indexed by $p \in P$, where each $f_p : \mathbb{R}^n \to \mathbb{R}^n$ is locally Lipschitz continuous.

A continuous and piecewise $\mathcal{C}^1$ function $\mathbf{x} : \mathbb{R}^+ \to \mathbb{R}^n$ is a *trajectory* of the switched system Σ if there exists a switching signal $\mathbf{p} \in \mathcal{P}$ such that $\dot{\mathbf{x}}(t) = f_{\mathbf{p}(t)}(x(t))$ holds at each time $t \in \mathbb{R}^+$ when $\mathbf{p}$ is continuous.

We let $\mathbf{x}(t, x, \mathbf{p})$ denote the point reached at time $t \in \mathbb{R}^+$, starting from the state $x \in \mathbb{R}^n$ (at $t = 0$), under the switching signal $\mathbf{p} \in \mathcal{P}$. In the special case where the switching signal is constant (i.e. $\mathbf{p}(s) = p$ for all $s \in \mathbb{R}^+$), it is denoted by $\mathbf{x}(t, x, p)$. The continuous subsystem of Σ

[2] Here *precision* means an upper bound for errors.

with the constant switching signal $\mathbf{p}(s) = p$ for all $s \in \mathbb{R}^+$ is denoted by Σ_p. If P is a singleton $P = \{p\}$, the system $\Sigma = \Sigma_p$ is a continuous system without switching.

Definition 2.2. (periodicity, switching delay). Let $0 \le \delta_0 < \tau$. A switching signal $\mathbf{p}$ is said to be *τ-periodic with switching delays within* δ_0 if there exists a sequence of nonnegative reals $t_0 < t_1 < t_2 < \cdots$ such that, for each $k \in \mathbb{N}$, $t_k \in [k\tau, k\tau+\delta_0]$ and the restriction of $\mathbf{p}$ to $[t_k, t_{k+1})$ is a constant function. The time instants $t_k \in \mathbb{R}^+$ are called *switching times*. A switched system $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$ is called *τ-periodic with switching delays within* δ_0 if all the switching signals in $\mathcal{P}$ are τ-periodic with switching delays within δ_0. Additionally, if $\delta_0 = 0$, a switching signal or a switched system is called *τ-periodic*.

Remark 2.3. Our results rely on $\delta_0 < \tau$, which we believe is a reasonable assumption. For example, in automotive applications, common switching periods are 4–8 milliseconds, while jitters arising from CAN (Controller Area Networking) latency can be bounded by 120 microseconds.

We focus on periodic switched systems with switching delays, and their difference from those without switching delays. More specifically, we consider two switched systems

$$\begin{array}{ll} \Sigma_{\tau,\delta_0} = (\mathbb{R}^n, P, \mathcal{P}_{\tau,\delta_0}, F) & \tau\text{-periodic with delays} \le \delta_0 \\ \Sigma_{\tau} = (\mathbb{R}^n, P, \mathcal{P}_{\tau}, F) & \tau\text{-periodic} \end{array} \quad (1)$$

that have $\mathbb{R}^n$, P and F in common. For the former system Σ_{τ,δ_0}, the set $\mathcal{P}_{\tau,\delta_0}$ consists of all τ-periodic signals with delays within δ_0; for the latter system Σ_τ the set $\mathcal{P}_\tau$ consists of all τ-periodic switching signals.

3. TRANSITION SYSTEMS AND APPROXIMATE BISIMULATION

We use approximate bisimulations from Girard and Pappas (2007) to formalize proximity between Σ_{τ,δ_0} (with delay) and Σ_τ (without). In this section we present our key definition (Def. 3.3) that allows such use of approximate bisimulation, in addition to a quick recap of a basic theory of approximate bisimulation.

Definition 3.1. (transition system). A *transition system* is a sextuple $T = (Q, L, \longrightarrow, O, H, I)$ consisting of 1) a set of states Q; 2) a set of labels L; 3) a transition relation $\longrightarrow \subseteq Q \times L \times Q$; 4) a set of outputs O; 5) an output function $H : Q \to O$; and 6) a set of initial states $I \subseteq Q$.

We let $q \xrightarrow{l} q'$ denote the fact that $(q, l, q') \in \longrightarrow$. In this paper, for a set X, a function $d : X \times X \to \mathbb{R}^+ \cup \{\infty\}$ that satisfies, for all $x, y, z \in X$, $d(x, y) \ge 0$ and $d(x, z) \le d(x, y) + d(y, z)$ is called a *premetric* on X. A transition system T is said to be *premetric* if the set O of outputs is equipped with a premetric d.

Approximate bisimulations are defined between transitions systems. It is a (co)inductive construct that guarantees henceforth proximity of behaviors of two states.

Definition 3.2. Let $T_i = (Q_i, L, \xrightarrow[i]{}, O, H_i, I_i)$ $(i = 1, 2)$ be two premetric transition systems, sharing the same sets of actions L and outputs O with a premetric d. Let $\varepsilon \in \mathbb{R}^+$ be a positive number; we call it a *precision*. A relation $R \subseteq Q_1 \times Q_2$ is called an *ε-approximate bisimulation relation* between T_1 and T_2 if the following three conditions hold for all $(q_1, q_2) \in R$.

- $d(H_1(q_1), H_2(q_2)) \le \varepsilon$;
- $\forall q_1 \xrightarrow[1]{l} q_1', \exists q_2 \xrightarrow[2]{l} q_2'$ such that $(q_1', q_2') \in R$; and
- $\forall q_2 \xrightarrow[2]{l} q_2', \exists q_1 \xrightarrow[1]{l} q_1'$ such that $(q_1', q_2') \in R$.

The transition systems T_1 and T_2 are *approximately bisimilar with precision* ε (which is denoted by $T_1 \sim_\varepsilon T_2$) if there exists an ε-approximate bisimulation relation R that satisfies the following conditions:

- $\forall q_1 \in I_1, \exists q_2 \in I_2$ such that $(q_1, q_2) \in R$;
- $\forall q_2 \in I_2, \exists q_1 \in I_1$ such that $(q_1, q_2) \in R$.

For the two switched systems $\Sigma_{\tau,\delta_0} = (\mathbb{R}^n, P, \mathcal{P}_{\tau,\delta_0}, F)$ and $\Sigma_\tau = (\mathbb{R}^n, P, \mathcal{P}_\tau, F)$ in (1), we shall construct associated transition systems $T(\Sigma_{\tau,\delta_0})$ and $T(\Sigma_\tau)$, respectively.

Definition 3.3. $(T(\Sigma_{\tau,\delta_0}), T(\Sigma_\tau))$. The transition system $T(\Sigma_{\tau,\delta_0}) = (Q_{\tau,\delta_0}, L, \xrightarrow[\tau,\,\delta_0]{}, O, H_{\tau,\delta_0}, I)$ associated with the switched system Σ_{τ,δ_0} with delays in (1), is defined as follows:

- the set of states is $Q_{\tau,\delta_0} := \mathbb{R}^n \times \bigcup_{k\in\mathbb{N}}[k\tau, k\tau+\delta_0] \times P$;
- the set of labels L is the set of modes, i.e. $L := P$;
- the transition relation $\xrightarrow[\tau,\,\delta_0]{} \subseteq Q_{\tau,\delta_0} \times L \times Q_{\tau,\delta_0}$ is defined by $(x, t, p) \xrightarrow[\tau,\,\delta_0]{p''} (x', t', p')$ if $p = p''$, $x' = \mathbf{x}(t' - t, x, p)$ and there exists $k \in \mathbb{N}$ such that $t \in [k\tau, k\tau + \delta_0]$ and $t' \in [(k + 1)\tau, (k + 1)\tau + \delta_0]$;
- the set of outputs is $O := \mathbb{R}^n \times \mathbb{R}^+ \times P$;
- the output function $H_{\tau,\delta_0} : Q_{\tau,\delta_0} \to O$ is the canonical embedding $\mathbb{R}^n \times \bigcup_{k\in\mathbb{N}}[k\tau, k\tau+\delta_0] \times P \to \mathbb{R}^n \times \mathbb{R}^+ \times P$; and
- the set of initial states is $I := \mathbb{R}^n \times \{0\} \times P$.

Intuitively, each state (x, t, p) of $T(\Sigma_{\tau,\delta_0})$ marks switching in the system Σ_{τ,δ_0}: $x \in \mathbb{R}^n$ is the (continuous) state at switching; t is time of switching; and p is the next mode. Note that, by the assumption on Σ_{τ,δ_0}, t necessarily belongs to the interval $[k\tau, k\tau + \delta_0]$ for some $k \in \mathbb{N}$.

The transition system $T(\Sigma_\tau) = (Q_\tau, L, \xrightarrow[\tau]{}, O, H_\tau, I)$ is constructed similarly from the switched system Σ_τ without delays in (1), by fixing δ_0 in the above definition to 0.

Note that in both $T(\Sigma_{\tau,\delta_0})$ and $T(\Sigma_\tau)$, the label p'' for a transition is uniquely determined by the mode component p of the transition's source (x, t, p). Therefore, mathematically speaking, we do not need transition labels.

In Girard et al. (2010), the state space Q of the transition system is just the continuous state space $\mathbb{R}^n$ of the switched system. In comparison, ours has time t and a mode p additionally. Moving a mode p from transition labels to states allows us to analyze what happens during switching delays, that is, when the system keeps operating under the mode p while it is not supposed to do so.

Definition 3.4. (premetric on outputs). The transition systems $T(\Sigma_{\tau,\delta_0})$ and $T(\Sigma_\tau)$ are premetric with the following d, defined on the common set of outputs $O = \mathbb{R}^n \times \mathbb{R}^+ \times P$:

$$d((x, t, p), (x', t', p')) := \begin{cases} \|x - \mathbf{x}(t - t', x', p)\| & \text{if } p = p', t' = k\tau \text{ and } t \in [t', t' + \delta_0] \text{ for some } k \in \mathbb{N} \\ \infty & \text{otherwise.} \end{cases}$$

4. INCREMENTAL STABILITY

After the pioneering work by Pola et al. (2008), a number of frameworks rely on the assumption of *incremental stability* for the construction of approximate bisimulations. Intuitively, a dynamical system is incrementally stable if, under any choice of an initial state, the resulting trajectory asymptotically converges to one reference trajectory. In this section, we review an incremental stability for switched systems, following Girard et al. (2010).

Definition 4.1. Let $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$ be a switched system. Σ is said to be *incrementally globally uniformly asymptotically stable (δ-GUAS)* if there exists a $\mathcal{KL}$ function[3] β such that for all $x, y \in \mathbb{R}^n$, $t \in \mathbb{R}^+$ and $\mathbf{p} \in \mathcal{P}$,

$$\|\mathbf{x}(t, x, \mathbf{p}) - \mathbf{x}(t, y, \mathbf{p})\| \leq \beta(\|x - y\|, t) \ .$$

Directly establishing that a system is δ-GUAS is often hard. A usual technique in the field is to let a Lyapunov-type function play the role of certificate for δ-GUAS.

Definition 4.2. Let $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$ be a single-mode switched system with $P = \{p\}$. A smooth function $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^+$ is a *δ-GAS Lyapunov function for* Σ if there exist $\mathcal{K}_\infty$ functions[3] $\underline{\alpha}$, $\overline{\alpha}$ and $\kappa > 0$ such that the following hold for all $x, y \in \mathbb{R}^n$.

$$\underline{\alpha}(\|x - y\|) \leq V(x, y) \leq \overline{\alpha}(\|x - y\|) \qquad (2)$$

$$\frac{\partial V}{\partial x}(x, y) f_p(x) + \frac{\partial V}{\partial y}(x, y) f_p(y) \leq -\kappa V(x, y) \qquad (3)$$

A sufficient condition for a switched system to be δ-GUAS is the existence of a common δ-GAS Lyapunov function.

Theorem 4.3. (Girard et al. (2010)). Let Σ be a switched system. Assume that all continuous subsystems $\Sigma_p (p \in \mathcal{P})$ have a δ-GAS Lyapunov function V in common (with the same κ). Then, V is called *a common δ-GAS Lyapunov function for* Σ, and Σ is δ-GUAS. □

5. APPROXIMATE BISIMULATION FOR DELAYS

We have reviewed that a common δ-GAS Lyapunov function is a certificate for the incremental stability δ-GUAS. A common δ-GAS Lyapunov function has been previously used mainly for discrete-state abstraction of switched systems (see §7). It is our main contribution to use the same incremental stability assumption to derive upper bounds for errors caused by switching delays. We focus on periodic switched systems; our translation of them to transition systems (Def. 3.3) plays an essential role.

The proofs in this section are omitted. See Appendix A in the extended version (Kido et al. (2017)) for the proofs.

We will be using the following assumption.

Assumption 5.1. (bounded intermode derivative). Let Σ be a switched system $(\mathbb{R}^n, P, \mathcal{P}, F)$ with $P = \{1, 2, \ldots, m\}$ and $F = \{f_1, f_2, \ldots, f_m\}$. We say a function $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^+$ has *bounded intermode derivatives* if there exists a real number $\nu \geq 0$ such that, for any distinct $p, p' \in P$, the following inequality holds for each $x, y \in \mathbb{R}^n$:

$$\frac{\partial V}{\partial x}(x, y) f_p(x) + \frac{\partial V}{\partial y}(x, y) f_{p'}(y) \leq \nu \ . \qquad (4)$$

Remark 5.2. Assumption 5.1 is not assumed in the previous works on approximate bisimulation for switched systems. However, it is not a severe restriction. In Girard et al. (2010) they make the assumption

$$\exists \gamma \in \mathbb{R}^+.\ \forall x, y, z \in \mathbb{R}^n.\ |V(x, y) - V(x, z)| \leq \gamma(\|y - z\|) \qquad (5)$$

(we do not need this assumption in the current work). It is claimed in Girard et al. (2010) that (5) is readily guaranteed if the dynamics of the system is confined to a compact set $C \subseteq \mathbb{R}^n$, and if V is class $\mathcal{C}^1$ in C. We can use the same compactness argument to ensure Assumption 5.1.

Definition 5.3. (the function V'). Let $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$ be a switched system, and $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^+$ be a common δ-GAS Lyapunov function for Σ. We define a function $V' : (\mathbb{R}^n \times \mathbb{R}^+ \times P) \times (\mathbb{R}^n \times \mathbb{R}^+ \times P) \to \mathbb{R}^+$ by

$$V'\big((x, t, p), (x', t', p')\big) := \begin{cases} V\big(x, \mathbf{x}(t - t', x', p')\big) & \text{if } p = p' \text{ and } t \in [t', t' + \delta_0] \\ \infty & \text{otherwise.} \end{cases}$$

Recall that $\mathbf{x}(t - t', x', p')$ is the state reached from x' after time $t - t'$ following the vector field $f_{p'}$.

The function V' defined above is an intermediate construct that connects a Lyapunov function V and an approximate bisimulation R_ϵ. Note that it can take ∞ as its value.

Here is our main technical lemma.

Lemma 5.4. Let $\Sigma_\tau = (\mathbb{R}^n, P, \mathcal{P}_\tau, F)$ be a τ-periodic switched system, and $\Sigma_{\tau,\delta_0} = (\mathbb{R}^n, P, \mathcal{P}_{\tau,\delta_0}, F)$ be a τ-periodic switched system with delays within δ_0. Assume that there exists a common δ-GAS Lyapunov function V for Σ_τ, and that V satisfies Assumption 5.1.

We define a relation $R_\varepsilon \subseteq (\mathbb{R}^n \times \mathbb{R}^+ \times P) \times (\mathbb{R}^n \times \mathbb{R}^+ \times P)$, using V' from Def. 5.3, by

$$(q, q') \in R_\varepsilon \overset{\text{def.}}{\iff} V'(q, q') \leq \underline{\alpha}(\varepsilon) \ . \qquad (6)$$

If we fix $\varepsilon = \underline{\alpha}^{-1}\left(\frac{\nu\delta_0}{1 - e^{-\kappa(\tau - \delta_0)}}\right)$ where ν is from Assumption 5.1, the relation R_ε is an approximate bisimulation between the transition systems $T(\Sigma_{\tau,\delta_0})$ and $T(\Sigma_\tau)$. □

In the following theorem we compare the trajectories of Σ_{τ,δ_0} and Σ_τ from the same initial state x. It is a direct consequence from the previous lemma.

Theorem 5.5. Assume the same assumptions as in Lem. 5.4. Let $\mathbf{p}_\tau$ be a τ-periodic switching signal, and $\mathbf{p}_{\tau,\delta_0}$ be the same signal but with delays within δ_0. That is, for each $s \in \mathbb{R}^+$,

$$\mathbf{p}_{\tau,\delta_0}(s) = \begin{cases} \mathbf{p}_\tau(s) \text{ or } \mathbf{p}_\tau(s - \delta_0) & \text{if } s \in \bigcup_{k \in \mathbb{N}, k \geq 1} [k\tau, k\tau + \delta_0) \\ \mathbf{p}_\tau(s) & \text{otherwise.} \end{cases}$$

We have, for each $t \in \mathbb{R}^+$,

$$\big\|\mathbf{x}(t, x, \mathbf{p}_{\tau,\delta_0}) - \mathbf{x}(t, x, \mathbf{p}_\tau)\big\| \ \leq \ \underline{\alpha}^{-1}\left(\frac{\nu\delta_0}{1 - e^{-\kappa(\tau - \delta_0)}}\right) \ .$$

□

Note that, for any desired precision ε, there always exists a small enough delay bound δ_0 that achieves the precision ε (i.e. $\frac{\nu\delta_0}{1 - e^{-\kappa(\tau - \delta_0)}} \leq \varepsilon$).

[3] A continuous function $\gamma : \mathbb{R}^+ \to \mathbb{R}^+$ is in *class* $\mathcal{K}$ if it is strictly increasing and $\gamma(0) = 0$. A $\mathcal{K}$ function is in *class* $\mathcal{K}_\infty$ if $\gamma(x) \to \infty$ when $x \to \infty$. A continuous function $\beta : \mathbb{R}^+ \times \mathbb{R}^+ \to \mathbb{R}^+$ is in *class* $\mathcal{KL}$ if 1) the function defined by $x \mapsto \beta(x, t)$ is a $\mathcal{K}_\infty$ function for any fixed t; and 2) for any fixed x, the function defined by $t \mapsto \beta(x, t)$ is strictly decreasing, and $\beta(x, t) \to 0$ when $t \to \infty$.

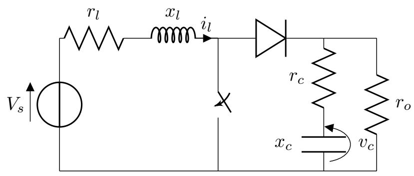

Fig. 2. The boost DC-DC converter circuit.

Remark 5.6. It turns out that the upper bound $\overline{\alpha}$ of a δ-GAS Lyapunov function V (see (2)) is not used in the above results (nor their proofs). In Girard et al. (2010), $\overline{\alpha}$ is used to define the state space discretization parameter η so that, for each initial state $q_1 \in I_1$, there would be an approximately bisimilar initial state in I_2 and vice versa. This is not necessary in our current setting where there is an obvious correspondence between the initial states.

6. EXAMPLE

We demonstrate our framework using the example of the boost DC-DC converter from Beccuti et al. (2005). It is a common example of switched systems. For this example we have a common δ-GAS Lyapunov function V, and therefore we appeal to the results in §5. We also demonstrate the control synthesis workflow in Fig. 1.

System Description The boost DC-DC converter system is presented in Fig. 2. Here we extend the analysis in Girard et al. (2010). The circuit includes a capacitor with capacitance $x_c = 70$ p.u. and an inductor with inductance $x_l = 3$ p.u. The capacitor has the equivalent series resistance $r_c = 0.005$ p.u. and the inductor has the internal resistance $r_l = 0.05$ p.u. The input voltage is $v_s = 1$ p.u., and the resistance $r_o = 1$ p.u. is the output load resistance. The state $x(t) = \begin{bmatrix} i_l(t) \\ v_c(t) \end{bmatrix}$ of this system consists of the inductor current i_l and the capacitor voltage v_c.

The system has two modes $\{ON, OFF\}$ [4], depending on whether the switch in the circuit is on or off. By elementary circuit theory, the dynamics in each mode is modeled by

$$\dot{x}(t) = A_p x(t) + b \quad \text{for } p \in \{ON, OFF\} \ , \text{ where}$$

$$A_{ON} = \begin{bmatrix} -\frac{r_l}{x_l} & 0 \\ 0 & -\frac{1}{x_c(r_o+r_c)} \end{bmatrix}, \quad b = \begin{bmatrix} \frac{v_s}{x_l} \\ 0 \end{bmatrix} \text{ and}$$

$$A_{OFF} = \begin{bmatrix} -\frac{r_l r_o + r_l r_c + r_o r_c}{x_l(r_o+r_c)} & -\frac{r_l r_o + r_l r_c + r_o r_c}{x_l(r_o+r_c)} \\ \frac{r_o}{x_c(r_o+r_c)} & -\frac{1}{x_c(r_o+r_c)} \end{bmatrix} .$$

Analysis Our ultimate goal is to synthesize a switching signal that keeps the dynamics in a safe region $\mathcal{S} := [1.3, 1.7] \times [5.7, 5.8]$. We shall follow the two-step workflow in Fig. 1.

Before analyzing the system, following Girard et al. (2010), we rescale the second variable of the system and redefine the state $x(t) = \begin{bmatrix} i_l(t) \\ 5v_c(t) \end{bmatrix}$ for better numerical conditioning. The ODEs are updated accordingly.

Girard et al. (2010) show that the dynamics in each mode is δ-GAS, finding by SDP optimization a common δ-GAS Lyapunov function $V(x, y) = \sqrt{(x-y)^T M (x-y)}$ with $M = \begin{bmatrix} 1.0224 & 0.0084 \\ 0.0084 & 1.0031 \end{bmatrix}$, such that $\underline{\alpha}(s) = s, \overline{\alpha}(s) = 1.0127s$ and $\kappa = 0.014$. We use the same function V as an ingredient for our approximate bisimulation.

Let us first use Thm. 5.5 and derive a bound ε_1 for errors caused by switching delays. We set the switching period $\tau = 0.5$ and the maximum delay $\delta_0 = \frac{\tau}{1000}$. On top of the analysis in Girard et al. (2010), we have to verify the condition we additionally impose (namely Assumption 5.1). Let us now assume that the dynamics stays in the safe region $\mathcal{S} = [1.3, 1.7] \times [5.7, 5.8]$—this assumption will be eventually discharged when we synthesize a safe controller. We checked $\nu = 0.41$ indeed satisfies the inequality (4), relying on techniques including QE. By Thm. 5.5, we obtain that the error between Σ_{τ,δ_0} (the boost DC-DC converter with delays) and Σ_τ (the one without delays) is bounded by $\varepsilon_1 = 0.0294176$.

Then we combine the above analysis with that in Girard et al. (2010), in the way prescribed in Fig. 1. Girard et al. (2010) use the same Lyapunov function V to derive a discrete symbolic model T_τ^{symb} and establish an approximate bisimulation between $T(\Sigma_\tau)$ and T_τ^{symb}. Their symbolic model T_τ^{symb} can be constructed so that any desired error bound ε_2 is guaranteed (a smaller ε_2 calls for a finer grid for discretization and hence a bigger symbolic model).

Now we employ an algorithm from supervisory control in Ramadge and Wonham (1987), and synthesize a set of safe switching signals that confine the dynamics of T_τ^{symb} to a shrunk safe region $\mathcal{S}_{\varepsilon_1+\varepsilon_2} := [1.3+(\varepsilon_1+\varepsilon_2), 1.7-(\varepsilon_1+\varepsilon_2)] \times [5.7+(\varepsilon_1+\varepsilon_2), 5.8-(\varepsilon_1+\varepsilon_2)]$. Let $\mathbf{p}$ be any such safe switching signal. By the second approximate bisimulation in Fig. 1, the signal $\mathbf{p}$ is guaranteed to keep the dynamics of Σ_τ in the region $\mathcal{S}_{\varepsilon_1} := [1.3 + \varepsilon_1, 1.7 - \varepsilon_1] \times [5.7 + \varepsilon_1, 5.8 - \varepsilon_1]$. Finally, the first approximate bisimulation in Fig. 1 guarantees that the signal $\mathbf{p}$ keeps the dynamics of Σ_{τ,δ_0}, the system with switching delays, in $\mathcal{S}$.

Remark 6.1. On the choice of a safe region used in control synthesis for the symbolic model T_τ^{symb}, our current choice $\mathcal{S}_{\varepsilon_1+\varepsilon_2} \subsetneq \mathcal{S}$ is more conservative than the choice in Girard et al. (2010), where they in fact expand (rather than shrink) the original safe region $\mathcal{S}$. We believe our conservative choice is required in the current workflow (Fig. 1) where two approximation steps are totally separated. Tighter integration of the two steps can lead to relaxation of this conservative choice.

7. RELATED WORK

Time delays are addressed also in Pola et al. (2010a,b). Pola et al. (2010b) deals with fixed time delays, and Pola et al. (2010a) considers unknown time delays. The goal of these works, which is different from ours, is to construct a comprehensive symbolic (discretized) model that encompasses all possible delays and switching signals. In particular, possible delays are thought of as disturbances (i.e. demonic/adversarial nondeterminism) and consequently they use *alternating* approximate bisimulations. The main technical gadget in doing so is spline-based finitary approximation of continuous-time signals.

[4] In the formalization of §2, the set P of modes is declared as $\{1, \cdots, m\}$. Here we instead use $P = \{ON, OFF\}$ for readability.

Towards control synthesis for switched systems with unknown switching delays, our workflow (Fig. 1) is two-step while a workflow based on Pola et al. (2010a) is one-step. The latter works as follows. The results in Pola et al. (2010a) yields a symbolic model for a switched system with delays; it is given by a two-player finite-state game $\mathcal{G}$ where angelic moves switching signals and demonic moves are time delays. By solving the game $\mathcal{G}$ (e.g. by the algorithm in Jurdzinski (2000)) one obtains a control strategy. It seems that our two-step workflow has an advantage in complexity: by collecting the spline-based approximations of all possible delays and switching signals, the game $\mathcal{G}$ in Pola et al. (2010a) tends to have a large number of transitions. It has to be noted, however, that the workflow following Pola et al. (2010a) applies to a greater variety of systems (than switched systems) and a resulting control strategy can be more fine-grained (reacting to delays, while our controller always assumes the worst time delays).

Another related work that refers to time delays is Liu and Ozay (2016). The biggest difference between Liu and Ozay (2016) and our work is that their framework is based on the invariance assumption of atomic formulas (δ in the paper): as long as errors due to delays do not exceed δ, the system satisfies the same set of LTL formulas. In contrast, our results bound distances between trajectories; the use of such bounds of ours is not restricted to satisfaction of LTL specifications.

The works Borri et al. (2012); Zamani et al. (2017) study symbolic abstraction of networked control systems, taking into account issues including time delays. The main difference from the current work is that their delays are assumed to be always multiples $(0, \tau, 2\tau, \dots)$ of the period τ; this assumption is enforced in their framework by system components called the *zero-order hold (ZOH)*. Their game-based frameworks are based on alternating approximate bisimulations, much like in Pola et al. (2010a), but the above assumption leads to simpler games for control synthesis. We note that our current setting—where delays are within a fixed bound $\delta_0 < \tau$—is outside the scope of Borri et al. (2012); Zamani et al. (2017).

A recent line of works by Khatib et al. (2016, 2017) take *timing contracts* as specifications; and study verification and scheduling problems. A crucial difference from the current work is that they assume linear dynamics, while we can deal with nonlinear dynamics.

8. CONCLUSIONS AND FUTURE WORK

In this paper we introduced an approximate bisimulation framework to provide upper bounds for errors arising from switching delays in periodic switched systems. It uses δ-GUAS as an ingredient for an approximate bisimulation. This is an advantage in the control synthesis workflow (Fig. 1), in which we separate two concerns of time delays and discretization of state spaces.

Adaptation of the current framework to (τ, ε)-closeness in Abbas et al. (2014) is imminent future work. As we mentioned in §7, this adaptation will likely not be hard.

Extending the current results to a wider class of systems is also future work. In particular, we are interested in disturbances and the consequent use of alternating approximate bisimulation by Pola and Tabuada (2009).

REFERENCES

Abbas, H., Mittelmann, H.D., and Fainekos, G.E. (2014). Formal property verification in a conformance testing framework. In *MEMOCODE* '14, 155–164.

Beccuti, A.G., Papafotiou, G., and Morari, M. (2005). Optimal control of the boost dc-dc converter. In *CDC* '05, 4457–4462.

Borri, A., Pola, G., and Di Benedetto, M.D. (2012). A symbolic approach to the design of nonlinear networked control systems. In *HSCC* '12, 255–264.

Girard, A. (2010). Synthesis using approximately bisimilar abstractions: state-feedback controllers for safety specifications. In *HSCC* '10, 111–120.

Girard, A. and Pappas, G.J. (2007). Approximation metrics for discrete and continuous systems. *IEEE Trans. Automat. Contr.*, 52(5), 782–798.

Girard, A. and Pappas, G.J. (2011). Approximate bisimulation: A bridge between computer science and control theory. *Eur. J. Control*, 17(5-6), 568–578.

Girard, A., Pola, G., and Tabuada, P. (2010). Approximately bisimilar symbolic models for incrementally stable switched systems. *IEEE Trans. Automat. Contr.*, 55(1), 116–126.

Jurdzinski, M. (2000). Small progress measures for solving parity games. In *STACS*, 290–301.

Khatib, M.A., Girard, A., and Dang, T. (2016). Verification and synthesis of timing contracts for embedded controllers. In *HSCC* '16, 115–124.

Khatib, M.A., Girard, A., and Dang, T. (2017). Scheduling of embedded controllers under timing contracts. In *HSCC* '17, 131–140.

Kido, K., Sedwards, S., and Hasuo, I. (2017). Bounding errors due to switching delays in incrementally stable switched systems (extended version). *CoRR*, abs/1712.06311.

Liu, J. and Ozay, N. (2016). Finite abstractions with robustness margins for temporal logic-based control synthesis. *Nonlinear Analysis: Hybrid Systems*, 22(Supplement C), 1 – 15.

Pola, G., Girard, A., and Tabuada, P. (2008). Approximately bisimilar symbolic models for nonlinear control systems. *Automatica*, 44(10), 2508–2516.

Pola, G., Pepe, P., and Benedetto, M.D.D. (2010a). Alternating approximately bisimilar symbolic models for nonlinear control systems with unknown time-varying delays. In *CDC* '10, 7649–7654.

Pola, G., Pepe, P., Benedetto, M.D.D., and Tabuada, P. (2010b). Symbolic models for nonlinear time-delay systems using approximate bisimulations. *Systems & Control Letters*, 59(6), 365–373.

Pola, G. and Tabuada, P. (2009). Symbolic models for nonlinear control systems: Alternating approximate bisimulations. *SIAM J. Control Optim.*, 48(2), 719–733.

Ramadge, P.J. and Wonham, W.M. (1987). Supervisory control of a class of discrete event processes. *SIAM J. Control Optim.*, 25(1), 206–230.

Zamani, M., Jr, M.M., Khaled, M., and Abate, A. (2017). Symbolic abstractions of networked control systems. *IEEE Transactions on Control of Network Systems*, PP(99), 1–1.