Switching Controller Synthesis for Delay Hybrid Systems under Perturbations

Yunjun Bai
baiyj@ios.ac.cn
SKLCS, Institute of Software, CAS
& Univ. of CAS, Beijing, China

Ting Gan
ganting@whu.edu.cn
Wuhan University
Wuhan, China

Li Jiao
ljiao@ios.ac.cn
SKLCS, Institute of Software, CAS
& Univ. of CAS, Beijing, China

Bican Xia
xbc@math.pku.edu.cn
Peking University
Beijing,China

Bai Xue
xuebai@ios.ac.cn
SKLCS, Institute of Software, CAS
&Univ. of CAS, Beijing, China

Naijun Zhan
znj@ios.ac.cn
SKLCS, Institute of Software, CAS
&Univ. of CAS, Beijing, China

ABSTRACT

Delays are ubiquitous in modern hybrid systems, which exhibit both continuous and discrete dynamical behaviors. Induced by signal transmission, conversion, the nature of plants, and so on, delays may appear either in the continuous evolution of a hybrid system such that the evolution depends not only on the present state but also on its execution history, or in the discrete switching between its different control modes. In this paper we come up with a new model of hybrid systems, called *delay hybrid automata*, to capture the dynamics of systems with the aforementioned two kinds of delays. Furthermore, based upon this model we study the robust switching controller synthesis problem such that the controlled delay system is able to satisfy the specified safety properties regardless of perturbations. To the end, a novel method is proposed to synthesize switching controllers based on the computation of differential invariants for continuous evolution and backward reachable sets of discrete jumps with delays. Finally, we implement a prototypical tool of our approach and demonstrate it on some case studies.

CCS CONCEPTS

• **Security and privacy → Formal security models**; **Logic and verification**.

KEYWORDS

Delay hybrid systems, delay differential equations, differential invariants, switching controllers, safety

1 INTRODUCTION

With the broad applications of cyber-physical systems (CPS) in our daily life, the correct design of reliable CPS is getting increasingly important, especially in safety-critical domains such as automotive, medicine, etc. Due to the bidirectional conversion between analog and digital signals, the periodicity of collecting data by sensors, and executing the commands by actuators, and the data transmission through networks with different bandwidths, etc., time delay is becoming ubiquitous and inevitable in CPS, giving rise to the difficulty of CPS design, as delays may invalidate the certificates of stability and safety obtained with abstracting them away, even well annihilate control performance.

Generally, two kinds of delays appear commonly in CPS. One is in continuous evolution of systems, resulting in that the evolution not only depends on the current state, but also on the historical states. As an appropriate generalization of ordinary differential equations (ODEs), delay differential equations (DDEs) are widely used to capture time-delay continuous dynamical systems. The other one occurs at discrete jumps between different control modes of the underlying systems.

In this paper, we propose a new model of hybrid systems, called *delay hybrid automata* (dHA), which is an extension of classical hybrid automata (HA) [14], in order to capture the dynamics of systems involving the aforementioned two kinds of delays. Based on the proposed dHA, we investigate the safe switching controller synthesis problem for delay hybrid systems, i.e., given a dHA $\mathcal{H}$ and a safety property $\mathcal{S}$, to synthesize a refined dHA $\mathcal{H}^*$ by strengthening the invariant in each mode and the guard condition for each discrete jump such that $\mathcal{H}^*$ satisfies $\mathcal{S}$ robustly, with additional condition that $\mathcal{H}^*$ is *non-blocking* if $\mathcal{H}$ is non-blocking. Our approach is invariant-based, which is a classical approach to synthesizing safe switching controllers for HA [3, 35]. However, the computation of differential invariants (the definition will be given in Section 3) for the DDE in each mode as well as a global invariant (the definition will be given in Section 4.2) among these modes is much involved than the counterparts in HA when the two kinds of delays are considered. To compute differential invariants for DDEs, we propose a two-step approach: the first step is to reduce differential invariant generation problem to T-differential invariant generation problem using global ball-convergence condition derived in terms of Metzler matrix for a class of linear DDEs, where T is a bounded time horizon; the second step is to obtain an over-approximation of the T-bounded reachable set based on the *growth bound* adapted from [29]. Nonlinear DDEs can be reduced to the linear case by means of the

HSCC '21, May 19–21, 2021, Virtual

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

linearization technique, in case that global ball-convergence is replaced by local ball-convergence. A global invariant is generated based on fixed point iteration, and the computation of differential invariants for continuous evolution in each mode and backward reachable sets for discrete jumps by taking delays into account, which is similar to compute reachable sets of HA, e.g., with dReach [19]. Our approach is finally illustrated on some interesting case studies.

The main contributions of this work are summarized below:

(1) a new model language, called dHA, is proposed to model delay hybrid systems, which exhibit delays in both continuous- and discrete-time dynamics.
(2) in this new model dHA, a novel approach based on the computation of differential invariants is proposed to address the switching controller synthesis problem for delay hybrid systems, such that the controlled delay hybrid system is able to satisfy the specified safety property.

1.1 Related Work

Controller synthesis through correct-by-construction manner provides mathematical guarantees to the correctness and reliablity of (hybrid) systems. In the literature, this problem has been extensively studied and various approaches have been proposed, which can be categorized into abstraction based, e.g., [5, 12, 16, 24, 28, 29], and constraint solving based, e.g., [31, 35]. The basic idea of abstraction based approaches is to abstract the original system under consideration to a finite-state two-players game, and then solve reactive synthesis using automata-theoretic algorithms with respect to temporal control objectives. In contrast, the basic idea of constrains solving based approaches is to reduce the synthesis problem to an invariant generation problem, which can be further reduced to a constraint solving problem. As a generalization of [31], an optimal switching controller synthesis is investigated in [18] by solving an unconstrained numerical optimization problem. Based on reachable set computation and fixed point iteration, a general framework of controller synthesis for HA is proposed in [3, 32]. However, all these existing works focus on ODEs, therefore cannot be applied to DDEs, let alone delay hybrid systems directly. This is because ODEs are Markovian, but DDEs are non-Markovian, whose states are functionals with infinite dimension. In [7, 9], a controller synthesis problem for time-delay discrete dynamical systems was first investigated by reduction to solving imperfect two-player safety game, but it is unclear whether their approach can be extended to time-delay continuous dynamical systems and delay hybrid systems.

Recently, verification and synthesis for time-delay systems attract increasing attention, we just name a few below. Prajna and Jadbabaie extended the notion of *barrier certificate* to time-delay systems [27]. In [36], Zou et al. first proposed interval Taylor model for DDEs, and then discussed automatic stability analysis and safety verification based on interval Taylor model and stability analysis of discrete dynamical systems. However, their approach can only be applied to specific DDEs, whose right sides are independent of current states. Following this line, more efficient algorithms for analyzing Taylor models to inner and outer approximate reachable sets of more general DDEs in finite time horizon were given [13]. In [10], Feng et al. further considered how to utilize stability analysis of linear delay dynamical systems and linearization to reduce the unbounded verification to the bounded verification for a class of general DDEs. Based on [10], [4] investigated switching controller synthesis problem of delay hybrid systems, in which time-delay in discrete jumps is not taken into account. In contrast, the approach proposed in this paper can compute differential invariants for DDEs using ball-convergence based on Metzler matrix analysis, growth bound and linearization, it could be more powerful and applied to verify more DDEs (see Example 3). In [8], a simulation-based approach to approximate reachable sets of ODEs was extended to DDEs. Meanwhile, a topological homeomorphism-based approach was proposed to over- and under-approximate reachable sets of a class of DDEs [33]. Later, this approach was further extended to deal with perturbed DDEs in [34]. Like [13], these approaches can only be applied to compute reachable sets in finite time horizon. In addition, in [25, 26], Pola et al. proposed approaches how to construct symbolic abstractions for time-invariant and time-varying delay systems by approximating functional space using spline analysis. In [17], Huang et al. proposed a bounded verification method for nonlinear networks with discrete delays. Nonetheless, the dynamics of each subsystem modelled by ODEs and the analysis is done over a finite time horizon. Evidently, only one kind of delays is considered in all these existing works, either continuous or discrete. There is indeed a lack of appropriate formal models to handle both situations uniformly.

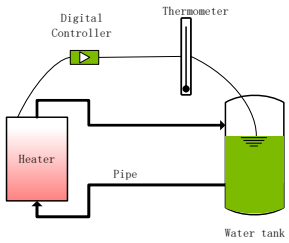


Figure 1: A heating system

1.2 A Motivating Example

To illustrate the main idea of our approach, we use a heating system as a motivating example, as depicted in Fig. 1, consisting of the following four components:

(1) a water tank with water,
(2) a heater with on and off two states,
(3) a thermometer monitoring the temperature of the water in the tank, and echoing warning signals whenever the temperature of the water is above or below certain thresholds,
(4) pipes connecting the heater and the tank.

Additionally, we add a controller that observes the signals produced in the thermometer, and computes a command to the heater in order to maintain the temperature of the water within a given range. The temperature of water in the tank is desired to stay between 20 and 90 degrees through switching the heating on and off. The behavior of the temperature of water in the tank is

mixed continuous evolution with discrete switches, which can be modelled by a hybrid automaton [2]. However, the delay impact of pipes and thermometer monitoring are both neglected in these models. In [30], it was pointed out that energy efficiency can be increased by $5-10\%$ if the delay impact of pipes is considered. Moreover, due to the delay possibly caused by measuring the thermometer, sending the signals, executing the control commands and so on, the temperature of water in the tank could be beyond the thresholds, which is definitely unsafe. Therefore, the delay impacts of the pipes and the thermometer have to be taken into account when we model the temperature of water in the tank.

1.3 Basic Notations and Definitions

Notations. Let N, R and C be the set of natural, real and complex numbers, R_+ be the set of positive real numbers. For $z = a + ib \in \mathrm{C}$ with $a, b \in \mathrm{R}$, $\Re(z) = a$ and $\Im(z) = b$, respectively, denote the real and imaginary parts of z. $\mathrm{R}^{=}$ is the set of n-dimensional real vectors, denoted by boldface letters. Given a vector $\mathrm{x} \in \mathrm{R}^{=}$, x_β denotes the i-th coordinate of x for $i \in \{1, 2, \ldots, n\}$, and its maximal norm is $\|\mathrm{x}\|_\infty = \max_{1 \le \beta \le =} |x_\beta|$. For a vector $\mathrm{y} \in \mathrm{R}^{=}_{+}$, let $(\mathrm{y})_{\min} = \min_{1 \le \beta \le =} y_\beta$. Given two vectors $\mathrm{x}, \mathrm{y} \in \mathrm{R}^{=}$, we define $\mathrm{x} \ge \mathrm{y}$ iff $x_\beta \ge y_\beta$ for all $1 \le i \le n$, and $\mathrm{x} \ j \ \mathrm{y}$ iff $x_\beta \ j \ y_\beta$ for all $1 \le i \le n$. Given $\epsilon \ j \ 0$, we define $\mathrm{B}(\epsilon) = \{\mathrm{x} \in \mathrm{R}^{=} \mid \|\mathrm{x}\|_\infty \le \epsilon\}$ as the ϵ-closed ball around 0. Let $\mathrm{R}^{=\times<}$ be the set of real $n \times m$ matrices. The entry in the i-th row and j-th column of a matrix $M \in \mathrm{R}^{=\times<}$ is denoted as $m_{\beta\vartheta}$ with $1 \le i \le n$ and $1 \le j \le m$. For $t_1 \ \ddot{Y} \ t_2$, $C\{[t_1, t_2], \mathrm{R}^{=}\}$ is the space of continuous functions from $[t_1, t_2]$ to $\mathrm{R}^{=}$. For a set $\mathrm{A} \subseteq \mathrm{R}^{=}_{+}$, $\mathrm{a} = \sup \mathrm{A}$ iff for all $\mathrm{x} \in \mathrm{A}$, $\mathrm{x} \le \mathrm{a}$, and for any upper bound $\mathrm{y} \in \mathrm{R}^{=}_{+}$, then $\mathrm{y} \ge \mathrm{a}$. Finally, we denote $(x)^+ = \max(0, x)$ for any real number $x \in \mathrm{R}$.

In this paper, we consider a class of time-delay systems under perturbations described as follows:

$$\begin{aligned} \dot{\mathrm{x}}(t) &= \boldsymbol{f}(\mathrm{x}(t), \mathrm{x}(t - r_1), \ldots, \mathrm{x}(t - r_{:}), \mathrm{w}(t)), \quad && t \in [0, \infty) \\ \mathrm{x}(t) &= \boldsymbol{5}(t), && t \in [-r_{:}, 0] \end{aligned} \tag{1}$$

where $\mathrm{x} \in \mathrm{R}^{=}$ is the state vector, $t \in \mathrm{R}$ models time, The discrete delays are assumed to satisfy $0 \ \ddot{Y} \ r_1 \ \ddot{Y} \ r_2 \ \ddot{Y} \cdots \ddot{Y} \ r_{:}$. $\mathrm{w}(\cdot) : [0, \infty) \mapsto \mathrm{R}^{<}$ is external disturbance vector, which is unknown but assumed to be bounded by a given constant $w_{<0G}$, i.e., $\|\mathrm{w}(t)\|_\infty \le w_{<0G}$ for all $t \ge 0$. $\boldsymbol{5}(\cdot) \in C\{[-r_{:}, 0], \mathrm{R}^{=}\}$ is the initial condition. Suppose that $\boldsymbol{f}$ is continuous and satisfies the Lipschitz condition, then from a given initial condition $\boldsymbol{5}$ and $\mathrm{w}(t)$, there exists a unique solution $/^{\mathrm{w}}_{\boldsymbol{5}}(\cdot) : [-r_{:}, \infty) \mapsto \mathrm{R}^{=}$.

Definition 1 (Metzler matrix[6]). *A matrix $M \in \mathrm{R}^{=\times=}$ is called a Metzler matrix if all off-diagonal elements of M are non-negative, i.e., $m_{\beta\vartheta} \ge 0$ whenever $i < j$.*

Regarding Metzler matrices, the following proposition holds, please refer to [6] for the detail.

Proposition 1 ([6]). *For any Metzler matrix M, the following two properties are equivalent*

1. *$\mu(M) \ \ddot{Y} \ 0$, where $\mu(M) = \max\{\Re(\alpha) \mid \alpha \in \mathrm{C} : \det(\alpha\mathcal{I} - M) = 0)\}$, $\mathcal{I}$ is the $n \times n$ identity matrix.*
2. *there exists $' \in \mathrm{R}^{=}$ and $' \ j \ 0$ such that $M' \ \ddot{Y} \ 0$.*

The structure of this paper is organized as: the notion of delay hybrid automata and the safe switching controller synthesis problem of interest are defined in Section 2. After presenting an approach for invariant generation of delay hybrid systems in Section 3, Section 4 concentrates on the controller synthesis framework based on the global invariants generation for delay hybrid systems. We demonstrate our approach with two examples in Section 5. Finally Section 6 concludes this paper.

2 DELAY HYBRID AUTOMATA AND PROBLEM STATEMENT

Hybrid automata (HA) [14] are popular models for dynamical systems with complex mixed continuous-discrete behaviors. In order to characterize behaviors of hybrid systems with the two type of time delays aforementioned, we introduce an extension of HA, called *delay hybrid automata* (dHA), formally defined as follows:

Definition 2 (Delay hybrid automaton, dHA). *A dHA is a tuple $\mathcal{H} = (Q, X, U, I, \ , F, E, D, G, R)$, where,*

- *$Q = \{q_1, \ldots, q_<\}$ is a finite set of modes;*
- *X is a set of state variables;*
- *$U \subseteq C\{[t_1, t_2], \mathrm{R}^{=}\}$, where $t_1 \ \ddot{Y} \ t_2$, is a set of continuous functionals;*
- *$I : Q \mapsto 2^{\mathrm{R}^{=}}$ gives each mode $q \in Q$ an invariant $I(q) \subseteq \mathrm{R}^{=}$;*
- *$\ : Q \mapsto 2^{*}$ gives each mode $q \in Q$ its initial states set $(q) \subseteq U$;*
- *$F = \{\boldsymbol{f}_{@_1}, \ldots, \boldsymbol{f}_{@_<}\}$ is the set of vector fields, each mode $q \in Q$ has unique vector field $\boldsymbol{f}_{@}$, which is used to form a delayed differential equation (1) to model the continuous evolution, i.e.,*

$$\dot{\mathrm{x}}(t) = \boldsymbol{f}_{@}(\mathrm{x}(t), \mathrm{x}(t - r^{@}_1), \ldots, \mathrm{x}(t - r^{@}_{:}), \mathrm{w}(t));$$

- *$E \subseteq Q \times Q$ is the set of discrete transition relations between modes;*
- *$D : E \mapsto \mathrm{R}_+$ gives each discrete transition $e \in E$ a delay time $D(e) \in \mathrm{R}_+$;*
- *$G : E \mapsto 2^{\mathrm{R}^{=}}$ denotes guard conditions;*
- *$R : E \times X \ \mapsto U$ denotes reset functions.*

Compared with the definition of HA, there are several notable changes in Definition 2: a new item $U \ \subseteq \ C\{[-r^{@}_{:}, 0], \mathrm{R}^{=}\}$ is introduced to represent the set of all possible initial states. Note that the solution to a DDE is a functional, and correspondingly a state is a function standing the execution history up to the considered instant starting from the given initial state, rather than a point in $\mathrm{R}^{=}$ as for ODE. Additionally, another new item D is used to specify the delays in discrete transitions: for each $e = (q, q') \in E$, the delay is denoted by $D(e) \in \mathrm{R}_+$. Moreover, the reset function R is changed to $E \times X \ \mapsto U$ accordingly, where X is the set of reachable states satisfying the corresponding guard condition. Intuitively, when a mode switching happens, e.g., a transition from q to q' at time t, there exists time $\theta \in [-r^{@}_{:}, 0]$, the system has to satisfy: $\mathrm{x}_{\mathrm{C}}{}^{\boldsymbol{5}}(\theta) \in G(e)$, and the update state is $\boldsymbol{5}' = R(e, \mathrm{x}^{\boldsymbol{5}}_{\mathrm{C}+\ (4)}(\cdot))$.

Example 1. *For the heating system shown in the motivating example, it is straightforward to present its dHA textually as follows:*

- *$Q = \{q_1, q_2\}$; (two modes of discrete states, heater on and off);*
- *$X = \{x\}$; (the temperature of water in the tank);*
- *$U = C$; (all continuous functionals);*

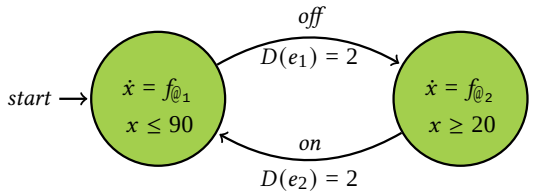


Figure 2: The dHA for the heating system

- $I(q_1) = \{x \in \mathrm{R} \mid 20 \le x \le 90\}$ *and* $I(q_2) = \{x \in \mathrm{R} \mid 20 \le x \le 90\}$;
- $(q_1) = \{x(t) \mid x(t) = 50 - 10\sin t, t \in [-1, 0]\}$ *and* $(q_2) = \{x(t) \mid x(t) = 85 - 5\sin t, t \in [-1, 0]\}$;
- $F = \{f_{@_1}, f_{@_2}\}$, *where* $f_{@_1} = K_1(h - x(t)) + K_2 x(t-1) + w_1$ *and* $f_{@_2} = -K_1 x(t) + K_2 x(t-1) + w_2$, K_1, K_2, h, w_1 *and* w_2 *are real constants. That is, the temperature rises and decreases following the respective DDE in* q_1 *and* q_2, *respectively;*
- $E = \{e_1 = (q_1, q_2), e_2 = (q_2, q_1)\}$;
- $D(e_1) = 2$ *and* $D(e_2) = 2$;
- $G(e_1) = \mathrm{R}$ *and* $G(e_2) = \mathrm{R}$;
- $R(e_1, x_{\mathbb{C}+\ (4_1)}(\cdot)) = x(\theta), \theta \in [t + D(e_1) - 1, t + D(e_1)]$ *with* $x(t) \in G(e_1)$ *and* $R(e_2, x_{\mathbb{C}+\ (4_1)}(\cdot)) = x(\theta), \theta \in [t + D(e_2) - 1, t + D(e_2)]$ *with* $x(t) \in G(e_2)$.

Pictorially, the dHA is shown in Fig. 2.

Definition 3 (Hybrid execution). *For a dHA* $\mathcal{H}$, *given an initial hybrid state* $(q_0, \mathbf{/}^{\mathrm{w}}_{\boldsymbol{5}_0}(0))$ *and* $\mathrm{w}(\cdot) : [0, \infty) \mapsto \mathrm{R}^{<}$, *an execution* π *of the delay hybrid automaton* $\mathcal{H}$ *is a sequence of* $\langle t_\beta, q_\beta, \mathbf{/}^{\mathrm{w}}_{\boldsymbol{5}_\beta}(t_\beta)\rangle$, *for* $i \in \mathrm{N}$ *and* $q_\beta \in Q$, *satisfying that any transition* $\langle t_\beta, q_\beta, \mathbf{/}^{\mathrm{w}}_{\boldsymbol{5}_\beta}(t_\beta)\rangle \mapsto \langle t_{\beta+1}, q_{\beta+1}, \mathbf{/}^{\mathrm{w}}_{\boldsymbol{5}_{\beta+1}}(t_{\beta+1})\rangle$ *is either :*

- the continuous evolution: $q_\beta = q_{\beta+1}, \boldsymbol{5}_\beta = \boldsymbol{5}_{\beta+1}, t_\beta \ddot{Y} t_{\beta+1}$, *and for all* $t \in [t_\beta, t_{\beta+1}]$, *the solution of DDE* $\dot{\mathrm{x}} = \boldsymbol{f}_{@_\beta}$ *is* $\mathbf{/}^{\mathrm{w}}_{\boldsymbol{5}_\beta}(\cdot) : [t_\beta, t_{\beta+1}] \mapsto \mathrm{R}^{=}$, *and* $\mathbf{/}^{\mathrm{w}}_{\boldsymbol{5}_\beta}(t) \in I(q_\beta)$;
- the discrete transition: $e = (q_\beta, q_{\beta+1}) \in E$, $t_\beta = t_{\beta+1}$, *and there exists* t *such that* $t_{\beta+1} = t + D(e)$ *and* $\mathbf{/}^{\mathrm{w}}_{\boldsymbol{5}_\beta}(t) \in G(e)$ *and* $\boldsymbol{5}_{\beta+1} = R(e, \mathrm{x}^{\boldsymbol{5}_\beta}_{\mathbb{C}+\ (4)}(\cdot))$.

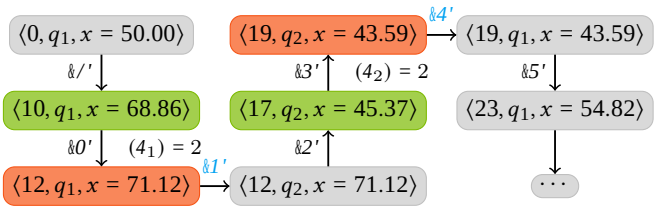
An execution π is called *finite* if it is a finite sequence ending with a closed time interval. Otherwise, if the execution π is called *infinite* if it is an infinite sequence or if $\sum^{\#}_{\beta=0}(t_{\beta+1} - t_\beta) = \infty$, where $N \in \mathrm{N}$. A dHA $\mathcal{H}$ is called *non-blocking* if there exists at least one infinite execution starting from any initial state.

Definition 4 (Reachable set). *Given a dHA* $\mathcal{H}$, *the reachable set* $\mathrm{R}_{\mathcal{H}}(t)$ *for the delay hybrid system within* $[-r^{@_0}_{\cdot}, t]$ *is*

$$\mathrm{R}_{\mathcal{H}}(t) = \left\{ \mathrm{x}(t) \;\middle|\; \begin{array}{c} \forall\, q_0 \in Q, \forall\, \mathbf{/}^{\mathrm{w}}_{\boldsymbol{5}_0}(0) \in (q_0), \\ \exists\, \pi = \langle t_0, q_0, \mathbf{/}^{\mathrm{w}}_{\boldsymbol{5}_0}(0)\rangle, \cdots, \langle t, q_\beta, \mathbf{/}^{\mathrm{w}}_{\boldsymbol{5}_\beta}(t)\rangle \\ s.t.\ \mathrm{x}(t) = \mathbf{/}^{\mathrm{w}}_{\boldsymbol{5}_\beta}(t) \end{array} \right\}.$$

Example 2. *An execution for the heating system in the motivating example is given below.*

From the initial state $(q_1, x = 50.00)$, *the system reaches the state* $(q_1, x = 68.86)$ *in green after* 10*s*, *which is indicated by transition* (1). *Assume that the state* $(q_1, x = 68.86)$ *in green satisfies the guard condition, the system chooses to jump from mode* q_1 *to mode* q_2. *However, there is a delay* $D(e_1) = 2$ *incurred by the edge* e_1. *The system keeps evolving in mode* q_1 *until hitting the state* $(q_1, x = 71.12)$ *revealed by transition* (2), *and completes the switching by reaching the state* $(q_2, x = 71.12)$ *displayed by transition* (3) *in blue. Continue this execution as above.*



Definition 5 (Safety). *Given a dHA* $\mathcal{H}$ *with a safe set* $\mathcal{S} = \cup_{@\in\&}\mathcal{S}_@$, *where* $\mathcal{S}_@ \subseteq \mathrm{R}^{=}$, *the automaton* $\mathcal{H}$ *is* T-safe *with respect to* $\mathcal{S}$ *in time* T, *if for any time* $t \in [-r^{@}_{\cdot}, T]$, *all reachable states* $\mathrm{R}_{\mathcal{H}}(t)$ *of the system starting from any initial states are contained in* $\mathcal{S}$, *i.e.,*

$$\mathrm{R}_{\mathcal{H}}(t) \subseteq \mathcal{S}, \forall t \in [-r^{@}_{\cdot}, T].$$

If T *is infinite, then the dHA is* safe *over the infinite-time horizon.*

Now, the problem of interest can be formally formulated as follows:

Problem 1 (**Safe Switching Controller Synthesis Problem**). *Given a dHA* $\mathcal{H} = (Q, X, U, I, \ , F, E, D, G, R)$ *and a safety property* $\mathcal{S}$, *the switching controller problem is to synthesize a new dHA* $\mathcal{H}^* = (Q, X, U^*, I^*, \ ^*, F, E, D, G^*, R)$ *such that* $\mathcal{H}^*$ *satisfies:*

(r1) $\mathcal{H}^*$ *is safe, i.e. in* $[-r^{@}_{\cdot}, \infty)$, *the reachable set* $\mathrm{R}_{\mathcal{H}^*} \subseteq \mathcal{S}$.

(r2) $\mathcal{H}^*$ *is a refinement of* $\mathcal{H}$, *i.e., it holds:* $^* \subseteq \ \cap \mathcal{S}$, $I^* \subseteq I$, $U^* \subseteq U$, *and for any* $e \in E$, *it holds:* $\forall \mathrm{x}(t) \in G^*(e)$, $\mathrm{x}(t + D(e)) \in G(e) \cap I^*(q)$.

(r3) *if* $\mathcal{H}$ *is non-blocking in the safe set* $\mathcal{S}$, *then* $\mathcal{H}^*$ *is non-blocking.*

$SC = \{G^*(e) \subseteq \mathrm{R}^{=} \mid e \in E\}$ *is called a* safe switching controller *of* $\mathcal{H}$, *if* $\mathcal{H}^*$ *satisfies above three requirements. We call* SC *is a* trivial switching controller *of* $\mathcal{H}$, *if there exists one mode* $q \in Q$ *or one edge* $e \in E$ *with* $I^*(q) = \emptyset$ *or* $G^*(e) = \emptyset$.

3 DIFFERENTIAL INVARIANT GENERATION

Differential invariant generation plays a central role in our framework to synthesize switching controllers for delay hybrid systems with perturbations. In this section, inspired by the work in [10], we present a two-step procedure to synthesize differential invariants for a delay dynamical system. The first step is to calculate a bounded horizon T using ball convergence analysis, which reduces the differential invariant generation problem to the T-differential invariant generation problem. The second step is to compute an over-approximation of the reachable set in time T, which is a T-differential invariant.

We first develop the aforementioned two-step method for linear delay dynamical systems, and then generalize it to nonlinear delay dynamical systems.

Definition 6 (Differential invariant). *Given a mode* $q \in Q$ *of a delay hybrid automaton* $\mathcal{H}$: $(\ (q), \boldsymbol{f}_@, I(q))$ *and time* T, *a*

set $I^*(q)$ is called a T- invariant if for any trajectory starting from a given initial function $\boldsymbol{5}(t) \in \ (q)$, $t \in [-r_{\cdot}^{@}, 0]$, the following condition holds for $\mathrm{w}(\cdot) : [-r_{\cdot}^{@}, T] \mapsto \mathrm{R}^{<}$:

$$\forall t \in [-r_{\cdot}^{@}, T],\ /_{\boldsymbol{5}}^{\mathrm{w}}(t) \in I(q) \implies \forall t \in [-r_{\cdot}^{@}, T], /_{\boldsymbol{5}}^{\mathrm{w}}(t) \in I^*(q).$$

If T is infinite, then $I^*(q)$ is a differential invariant of mode q.

T- invariant $I^*(q)$ requires that every trajectory starting from initial set $\ (q)$ in time T remains inside the differential invariant $I^*(q)$ if it remains in the domain $I(q)$. A *safe* differential invariant requires $I^*(q) \subseteq \mathcal{S}_{@}$.

3.1 Linear Systems

We consider linear DDEs with the form (1) first, i.e.,

$$\begin{array}{ll} \dot{\mathrm{x}}(t) = A\mathrm{x}(t) + B\mathrm{x}(t-r) + C\mathrm{w}(t), & t \in [0, \infty) \\ \mathrm{x}(t) = \boldsymbol{5}(t), & t \in [-r, 0] \end{array}, \quad (2)$$

where $A, B \in \mathrm{R}^{=\times=}$ and $C \in \mathrm{R}^{=\times<}$ are real matrices with appropriate dimensions.

Definition 7 (Global ball-convergence). *Given a* r ¡ 0, (2) *is called* globally exponentially convergent *within the ball* B(r)*, if there exist a constant* γ ¡ 0 *and a non-decreasing function* $\kappa(\cdot)$ *such that*

$$\|/_{\boldsymbol{5}}^{\mathrm{w}}(t)\|_\infty \le \mathrm{r} + \kappa(\|\boldsymbol{5}\|_\infty)\mathrm{e}^{-WC},\ \forall t \ge 0$$

holds for all $\boldsymbol{5} \in C\{[-r, 0], \mathrm{R}^{=}\}$ *and* $\|\mathrm{w}(t)\|_\infty \le w_{<0G}, \forall t \ge 0$.

In Definition 7, γ represents the rate of decay, i.e., an estimate of how quickly the solution of (2) converges to the ball B(r). Especially, when the radius r = 0, the definition of ball convergence is consistent with Lyapunov exponential stability [22]. Moreover, in [15], it was proved that

Theorem 1 ([15]). *Suppose in* (2) $M = A + B$ *is a Metzler matrix satisfying one of the properties in Proposition 1. Then, there exist positive constants $\beta, \gamma, \delta, \eta$ such that for all initial functions* $\boldsymbol{5}$ *and* $\|\mathrm{w}(t)\|_\infty \le w_{<0G}, \forall t \ge 0$

$$\|/_{\boldsymbol{5}}^{\mathrm{w}}(t)\|_\infty \le \frac{C_{<0G} w_{<0G}}{\eta} + \beta(\|\boldsymbol{5}\|_\infty - \frac{C_{<0G} w_{<0G}}{\delta})^{+}\mathrm{e}^{-WC},\ \forall t \ge 0$$

holds, where $C_{<0G} = \max_{\beta \in =} \sum_{\vartheta=1}^{<} C_{\beta\vartheta}$.

In Theorem 1, based on the notion of Metzler matrix, (2) is globally exponentially convergent to the ball $\mathrm{B}(\frac{<0G F<0G}{l})$ for all perturbations $\|\mathrm{w}(t)\|_\infty \le w_{<0G}, \forall t \ge 0$. Moreover, the size of the ball increases as the perturbation bound increases. Particularly, without perturbation by letting $\mathrm{w}(t) = 0$ for all $t \in [-r, \infty)$, the equilibrium 0 is exponentially stable. [15] also provides the way to obtain the constants $\beta, \gamma, \delta, \eta$ in Theorem 1, which can be sketched as: let $' \ ¡ \ 0$ with $\|'\|_\infty = 1$ and $M' \ \ddot{Y} \ 0$, then $\beta = (')^{-1}_{<\beta=}$, $\eta = (-M')_{<\beta=}$, $\delta = \eta(')^{-1}_{<\beta=}$, $\gamma = \min_{\beta \in =} \gamma_\beta$, where γ_β is the solution of the equation

$$H_\beta(\gamma) = \gamma\zeta_\beta + \sum_{\vartheta=1}^{\tilde{\Theta}} \zeta_\vartheta B_{\beta\vartheta}(e^{WA-1}) - \eta = 0.$$

Algorithm 1 Safe Differential Invariant Synthesis

```
procedure DInvariant( (q), f_@, T*, τ, 1, S_@, r_1, ϵ)
    P_0(q) ← (q) ∩ S_@; i ← 0; t ← 0
    while t ≤ T* do
        R_%_β(@) ← ∅
        P_β(q) ← select a C ∈ C(P_β(q), 1)
        for each x ∈ P_β(q) do
            R_x ← SafeR(1, x, τ, S_@)
            if R_x < ∅ then
                R_%_β(@) ← R_%_β(@) ∪ R_x
            end if
        end for
        if R_%_β(@) < ∅ then
            if R_%_β(@) ⊆ P_β(q) ∪ B(r_1 + ϵ) then
                return P_β(q) ∪ (B(r_1 + ϵ) ∩ S_@)
            else
                P_β+1(q) ← P_β(q) ∪ R_%_β(@)
                i ← i + 1; t ← t + τ
            end if
        else
            Break;
        end if
    end while
    return P_β(q) ∪ (B(r_1 + ϵ) ∩ S_@)
end procedure
procedure SafeR(1, x, τ, S_@)
    compute R_x over t ∈ [0, τ]
    if R_x ⊆ S_@ then
        return R_x
    else if R_x ∩ S_@ < ∅ ∧ 1/2 ≥ 1_C then
        Ŷ ← C(x, 1/2)
        R_x ← ∅
        for each y ∈ Ŷ do
            R~ ← SafeR(1/2, y, τ, S_@ )
            R_x ← R_x ∪ R~
        end for
    else
        return ∅
    end if
    return R_x
end procedure
```

Pcbsagle rm T+bgẽcpclrg_j glt_pg_lr eclcp_rgml npm`jckβ
According to Theorem 2, the first step of differential invariant generation can be achieved by the following theorem:

Theorem 2. *Suppose $M = A + B$ is a Metzler matrix in* (2) *satisfying one of the properties in Proposition 1. Given an initial function* $\boldsymbol{5}$ *and a disturbance* w *with* $\|\mathrm{w}(t)\|_\infty \le w_{<0G}, \forall t \ge 0$, *let* $\mathrm{r}_1 = \frac{<0G F<0G}{l}$ *and* $\mathrm{r}_2 = \beta(\|\boldsymbol{5}\|_\infty - \frac{<0G F<0G}{X})$, *for any* ϵ ¡ 0, *let*

$$T^* = \max\{0, \inf\{T \mid \forall t \ge T : \mathrm{r}_2^{+}\mathrm{e}^{-WC}\ \ddot{Y}\ \epsilon\}\},$$

then $\|/_{\boldsymbol{5}}^{\mathrm{w}}(T)\|_\infty - \mathrm{r}_1\ \ddot{Y}\ \epsilon$ *for any $T \ge T^*$, where β, γ, δ and η satisfy the condition in Theorem 1.*

Proof. The proof for the *necessity* part is straightforward. For the *sufficiency* part, by Theorem 1, $\|\phi^{w}_{\boldsymbol{5}}(t)\|_\infty \le r_1 + r_2^+ e^{-Wt}$ for any $t \ge 0$, $\boldsymbol{5}$ and $w(t)$. Moreover, $r_2^+ e^{-Wt}$ is strictly monotonically decreasing w.r.t t, hence there exists an upper bound T^* such that for any $t \ge T^*$, $r_2^+ e^{-Wt}$ is exponentially close to the ball $B(r_1)$ within a prescribed precision ϵ. Therefore, for the given precision ϵ, for any $t \ge T^*$, all trajectories starting from $\boldsymbol{5}$ are exponentially convergent to the ball $B(r_1)$.

Lemma 3. *Suppose in* (2) $M = A + B$ *is a Metzler matrix with one of the properties in Proposition 1. Given* $\epsilon > 0$, *the ball* $B(r_1 + \epsilon)$ *is an attractor, i.e., any trajectory originating from a state in* $B(r_1 + \epsilon)$ *is guaranteed to evolve into* $B(r_1 + \epsilon)$.

Theorem 2 and Lemma 3 set up a sound guarantee that synthesizing differential invariant problem can be reduced to synthesizing T-differential invariant problem. Now we are ready to introduce the second step of synthesizing differential invariants.

Amknsrgle_lmtcp+_nnpmvgk_rgmlmdpc_af_`jcqcrugrfgl $T^*\beta$ we adapt the method in [29] for ODEs to compute an over-approximation of the reachable set for (2) with a *growth bound* defined below.

Definition 8 (Growth bound). *Given* $t > 0$, $\boldsymbol{1} \in \mathbb{R}^{=}_{+}$ *and a compact set* $K \subseteq I(q)$, *a growth bound is a map* $\quad : \mathbb{R}^{=}_{+} \times \mathbb{R}_{+} \mapsto \mathbb{R}^{=}_{+}$ *satisfying the following conditions:*

- $(\boldsymbol{1}, t) \ge (\boldsymbol{1}', t)$ *whenever* $\boldsymbol{1} \ge \boldsymbol{1}'$,
- *given* $\boldsymbol{5}(t) \in C\{[-r, 0], K\}$, *then*

$$\sup_{\theta_1, \theta_2 \in [-A, 0]} |x^{\boldsymbol{5}}_C(\theta_1) - x^{\boldsymbol{5}}_C(\theta_2)| \le (\sup_{\theta_1, \theta_2 \in [-A, 0]} |\boldsymbol{5}(\theta_1) - \boldsymbol{5}(\theta_2)|, t),$$

where $|\cdot|$ *represents the element-wise absolute value.*

Theorem 4 below tells how to construct a specific growth bound $(\cdot, \cdot)$.

Theorem 4. *Given a* $\boldsymbol{1} \in \mathbb{R}^{=}_{+}$, *let* $t > 0$, *the map* $\quad (\boldsymbol{1}, t)$, *defined by*

$$(\boldsymbol{1}, t) = e^{tC}\boldsymbol{1} + \int_0^t e^{s(C-B)}|B| \quad (\boldsymbol{1}, s - r)\, ds,$$

is a growth bound *of* (2), *where* L *satisfies*

$$L_{ij} \ge \begin{cases} A_{ij}, & i = j \\ |A_{ij}|, & otherwise \end{cases}.$$

Proof. Given any states $x(t), y(t) \in I(q)$, let $z(t) = y(t) - x(t)$. From (2), $\dot{z}(t) = \dot{y}(t) - \dot{x}(t) = Az(t) + Bz(t - r)$. Hence, by Lemma 6 in [29], we get

$$|z(t)| \le e^{tC}\boldsymbol{1} + \int_0^t e^{s(C-B)}|B|z(s - r)ds.$$

A *hyper-rectangle* $[[a, b]]$ with $a, b \in (\mathbb{R} \cup \{\pm\infty\})^{=}$ defines the set $\{x \in \mathbb{R}^{=} \mid a_i \le x_i \le b_i \text{ for } i \in \{1, \ldots, n\}\}$; it is non-empty if $a \le b$ (element-wise). For $\boldsymbol{1} \in \mathbb{R}^{=}_{+}$, we say that a hyper-rectangle $[[a, b]]$ has the diameter $\boldsymbol{1}$ if $\frac{|b-a|}{2} = \boldsymbol{1}$. Given a set $K \in \mathbb{R}^{=}$, we denote by $C(K, \boldsymbol{1})$ the set of covers of K, each of which is a cover of K, and consists of a set of hyper-rectangles with diameter $\boldsymbol{1}$.

Algorithm 1 summarizes the second step to construct a *safe* differential invariant: it repeats to compute the reachable set over time horizon $[0, T^*]$ in a forward way with step size τ (line 3-22); in each iteration, it first finds a hyper-rectangle cover of the initial set, and any element in the cover stands for an abstract state, that is a hyper-rectangle with diameter $\boldsymbol{1}$ (line 5). Then for each abstract state, SafeR is invoked to compute the set of reachable states from the abstract state within τ (line 6-11). If the reachable set is not contained in the safe set, the abstract state will be refined, and SafeR is recursively invoked until either the computed reachable set is contained in the safe set or the diameter of the abstract state is smaller than the given threshold $\boldsymbol{1}_C$ (line 25-40); this procedure terminates whenever a fixed point is reached (line 13) or the accumulated time is greater than T^*, and returns the union of the computed reachable set before T^* (i.e., $P_\beta(q)$) and the over-approximation of the reachable set after T^* (i.e., $B(r_1 + \epsilon) \cap \mathcal{S}_@$).

Theorem 5. *Given a delay dynamical system* $(\quad (q), \boldsymbol{f}_@, I(q))$ *and a safety requirement* $\mathcal{S}_@$, *where* $\boldsymbol{f}_@$ *is with the form* (2) *such that* $M = A + B$ *is a Metzler matrix satisfying one of the properties in Proposition 1. Let* T^*, ϵ *and* r_1 *be defined by Theorem 2,* $\boldsymbol{1}$ *and* τ *be the discretization parameter and step size, then Algorithm 1 terminates and returns a differential invariant for* (2).

Proof. **Termination**: Obviously.

Soundness: (i) If the algorithm returns the result at line 14, we have $R_{\%_\beta(@)} \subseteq P_\beta(q) \cup B(r_1 + \epsilon)$, then

$$\begin{aligned} P_{\beta+1}(q) \cup B(r_1 + \epsilon) &= P_\beta(q) \cup R_{\%_\beta(@)} \cup B(r_1 + \epsilon) \\ &\subseteq P_\beta(q) \cup B(r_1 + \epsilon). \end{aligned}$$

By recursion, $P_\beta(q) \cup B(r_1 + \epsilon)$ is an over-approximation of the reachable set over the infinite time horizon from the initial set for (2), i.e., $P_\beta(q) \cup (B(r_1 + \epsilon) \cap \mathcal{S}_@)$ is a safe differential invariant of (2). (ii) If the algorithm terminates at line 23, evidently $P_\beta(q)$ is an over-approximation of the reachable set over time $[0, T^*]$ from the initial set of (2). By Theorem 2 and Lemma 3, $P_\beta(q) \cup (B(r_1 + \epsilon) \cap \mathcal{S}_@)$ is a safe differential invariant for (2).

3.2 Nonlinear Systems

In this subsection, we generalize the two-step method in Section 3.1 for nonlinear systems by means of linearization techniques.

For simplifying the presentation, we first consider the form of DDE (1) with one single delay, i.e.,

$$\begin{cases} \dot{x}(t) = \boldsymbol{f}(x(t), x(t - r), w(t)), & t \in [0, \infty) \\ x(t) = \boldsymbol{5}(t), & t \in [-r, 0] \end{cases}. \tag{3}$$

Let

$$A = \frac{\partial \boldsymbol{f}}{\partial x(t)}_{(0,0)} \text{ and } B = \frac{\partial \boldsymbol{f}}{\partial x(t - r)}_{(0,0)}$$

be the Jacobian matrices of DDE (3) with respect to $x(t)$ and $x(t-r)$, evaluated at the origin $(0, 0)$, respectively. Thus, we can linearize DDE (3) as

$$\begin{cases} \dot{x}(t) = Ax(t) + Bx(t - r) + Cw(t) \\ \qquad\qquad + g(x(t), x(t - r)), & t \in [0, \infty) \\ x(t) = \boldsymbol{5}(t), & t \in [-r, 0] \end{cases}, \tag{4}$$

where $g(\cdot, \cdot)$ is the higher-order term, which is very closed to zero when x is sufficiently close to the equilibrium. By dropping the higher-order term in (4), we can obtain the approximation of (3), which is exactly the same linear system specified in (2).

Definition 9 (Local ball-convergence). *Given a* $\mathrm{r} > 0$, (3) *is called* locally exponentially convergent *within the ball* $\mathrm{B}(\mathrm{r})$, *if there exist constant* $\gamma > 0$, $\iota > 0$ *and a non-decreasing function* $\kappa(\cdot)$ *such that for all* $\|\mathrm{w}(t)\|_\infty \le w_{<OG}$

$$\|\boldsymbol{5}(t)\|_\infty \le \iota \implies \|\varphi^{\mathrm{w}}_{\boldsymbol{5}}(t)\|_\infty \le \mathrm{r} + \kappa(\|\boldsymbol{5}\|_\infty)\mathrm{e}^{-\mathcal{WC}},\ \forall t \ge 0$$

holds.

Theorem 6. *Suppose that* $M = A + B$ *is a Metzler matrix in* (4) *satisfying one of two properties in Proposition 1, then there exist positive constants* $\iota, \beta, \gamma, \delta$ *and* η *such that for all* $\|\mathrm{w}(t)\|_\infty \le w_{<OG}$

$$\|\boldsymbol{5}(t)\|_\infty \le \iota \implies \|\varphi^{\mathrm{w}}_{\boldsymbol{5}}(t)\|_\infty \le \frac{\mathcal{G}}{\eta} + \beta(\|\boldsymbol{5}\|_\infty - \frac{\mathcal{G}}{\delta})^+\mathrm{e}^{-\mathcal{WC}},\ \forall t \ge 0$$

holds, where $C_{<OG} = \max_{\mathcal{g}\in=}\{\sum_{\mathcal{g}=1}^{<} C_{\mathcal{g}\mathcal{g}}\}$.

Proof. Let $\mathcal{G} = C_{<OG} w_{<OG} + g_{<OG}$, where $\|\mathrm{g}(\mathrm{x}(t), \mathrm{x}(t-r))\|_\infty \le g_{<OG}$, and $\iota \le \frac{\mathcal{G}}{l} + \beta(\|\boldsymbol{5}\|_\infty - \frac{\mathcal{G}}{X})^+$, then it can be proved similar to that of Theorem 1.

Similarly, Theorem 7 says that the differential invariant generation problem for nonlinear DDEs can be equivalently reduced to to the T-invariant generation problem.

Theorem 7. *Given an initial function* $\boldsymbol{5}$ *and a disturbance* w *with* $\|\mathrm{w}(t)\|_\infty \le w_{<OG}, \forall t \ge 0$, *for* (1), *suppose that the positive constants* $\iota, \beta, \gamma, \delta, \eta$ *and* $g_{<OG}$ *satisfy the condition in Theorem 6, let* $\mathrm{r}_1 = \frac{\mathcal{G}}{l}$ *and* $\mathrm{r}_2 = \beta(\|\boldsymbol{5}\|_\infty - \frac{\mathcal{G}}{X})$, *and for any* $\epsilon > 0$, *let* $T^* = \max\{0, \inf\{T \mid \forall t \ge T : \mathrm{r}_2^+\mathrm{e}^{-\mathcal{WC}} \ddot{Y} \epsilon\}\}$, *then for any* $\|\boldsymbol{5}(t)\|_\infty \le \iota$ *and any* $T \ge T^*$ *it follows* $\|\varphi^{\mathrm{w}}_{\boldsymbol{5}}(T)\|_\infty - \mathrm{r}_1 \ddot{Y} \epsilon$. *That is, a differential invariant of* (1) *exactly corresponds to one of its* T*-differential invariant.*

Proof. Similar to the proof of Theorem 2.

Remark 1. *The fact that Theorem 7 holds with the condition* $\|\boldsymbol{5}(t)\|_\infty \le \iota$ *implies the locality of linearization. Moreover, in order to alleviate conservativeness of linearization, we need to compute a tighter parameter* $g_{<OG}$, *which is used to bound the high-order terms discarded during linearization.*

Note that the above discussion can be straightforwardly extended to DDEs (1) *with multiple delays by just letting* $M = A + \sum_1^{\vdots} B_{\mathcal{g}}$.

4 SWITCHING CONTROLLER SYNTHESIS WITH DELAYS AND PERTURBATIONS

In this section we present our synthesis framework based on invariant generation for delay hybrid systems with perturbations modelled by dHA.

4.1 Computing Guards of Discrete Jumps

In this subsection, by computing a reachable set from the set of states reachable to the edge without the jump delay backwards, we focus on how to synthesize a new guard $G^*(e)$ of each discrete jump e in order to guarantee the safety when taking the jump delay into consideration.

Definition 10 (Backward reachable set). *For a mode* q *of the dHA* $\mathcal{H} : (\ (q), \boldsymbol{f}_{@}, I^*(q))$, *given a target region* $\mathcal{G}(e)$ *and a finite time* $t = D(e)$, *the reachable set* $G^*(e)$ *from the target region* $\mathcal{G}(e)$ *backwards after* t *time units is defined as*

$$G^*(e) = \{\mathrm{x}_0 \mid \forall\, t \in [0, D(e)], \forall\, \mathrm{w}(t).\ \varphi^{\mathrm{w}}_{\mathrm{x}_0}(D(e)) \in \mathcal{G}(e) \wedge \varphi^{\mathrm{w}}_{\mathrm{x}_0}(t) \in I^*(q)\}.$$

Now, we present an algorithm, which is presented in Algorithm 2, to under-approximate the backward reachable set based on discretization in a symbolic way. The basic idea is: Given a discretization step size $\boldsymbol{1} \in \mathrm{R}^{=}_{+}$, let $\mathbb{P}^*(q)$ be in $\mathrm{C}(I^*(q), \boldsymbol{1})$, and $\mathrm{d} \in \mathrm{R}^{=}$ be $|\sup_{\mathrm{x}\in\ ^*(@)\cdot\|\mathrm{w}(\mathbb{C})\|_\infty \le F_{<OG}} \boldsymbol{f}| \cdot D(e)$, standing for the maximal distance following the DDE from $I^*(q)$ within the time delay $D(e)$ subject to any disturbance. So, a necessary condition that an abstract state in $\mathbb{P}^*(q)$ can reach $\mathcal{G}$ within $D(e)$ is that the distance from the state to $\mathcal{G}$ is less than or equal to d, i.e., in the following set

$$\mathcal{G}(e) \uplus \mathrm{d} = \{\mathbb{x} \in \mathbb{P}^*(q) \mid \mathbb{x} \in \mathcal{G}(e) \vee \exists\, \mathbb{x}' \in \mathcal{G}(e) : |ctr(\mathbb{x}) - ctr(\mathbb{x}')| \le \mathrm{d} + 4\boldsymbol{1}\},$$

where $ctr(\mathbb{x})$ is the *center* of the abstract state $\mathbb{x}$, standing for the hyper-rectangle $[[\mathrm{a}, \mathrm{b}]]$, i.e., the point $(\frac{1}{2}(b_1 - a_1), \ldots, \frac{1}{2}(b_= - a_=))$. Obviously, all trajectories starting from the set $\mathbb{P}^*(q) \setminus (\mathcal{G}(e) \uplus \mathrm{d})$ are impossible to reach to $\mathcal{G}(e)$ within $D(e)$. Therefore, we only need to consider the set $\mathcal{G}(e) \uplus \mathrm{d}$. For each abstract state $\mathbb{x} \in \mathcal{G}(e) \uplus \mathrm{d}$, the over-approximation of the backward reachable set $\mathrm{R}_{\mathbb{x}}$ is calculated by checking whether it keeps $I^*(q)$ satisfied over $[0, D(e)]$ and all elements of $\mathrm{R}_{\mathbb{x}}(D(e))$ should satisfy $\mathcal{G}(e)$. If the answer is *yes*, then it is done; otherwise, if some of reachable states in $\mathrm{R}_{\mathbb{x}}(D(e))$ satisfy $\mathcal{G}(e)$, then refine the abstract state $\mathbb{x}$ with a smaller discretization parameter $\boldsymbol{1}'$, say $\boldsymbol{1}' = \boldsymbol{1}/2$. Repeat the above procedure until all abstract states in the set $\mathcal{G}(e) \uplus \mathrm{d}$ are done.

Algorithm 2 Backward Reachable Set Computation

```
1:  procedure BackReach(𝒢(e), D(e), I*(q), 1, τ)
2:      G*(e) ← ∅
3:      ℙ*(q) ← C(I*(q), 1)
4:      d ← |sup_{x∈ *(@)·‖w(C)‖∞ ≤ F_{<OG}} f| · D(e)
5:      for each 𝕩 ∈ 𝒢(e) ⊎ d do
6:          compute R_𝕩(t) for t ∈ [0, D(e)] with step size τ
7:          if R_𝕩(D(e)) ⊆ 𝒢(e) Ó R_𝕩(t) ⊆ I*(q),
                                   ∀t ∈ [0, D(e)] then
8:              G*(e) ← G*(e) ∪ 𝕩
9:          end if
10:         if R_𝕩(D(e)) ∩ 𝒢(e) < ∅ Ó R_𝕩(t) ⊆ I*(q),
                                   ∀t ∈ [0, D(e)] then
11:             refine 𝕩 with 1′ ← 1/2, (1′ ≥ 1_C )
12:         end if
13:     end for
14:     return G*(e)
15: end procedure
```

4.2 Switching Controller Synthesis

To present our approach on switching controller synthesis, we need to introduce the notion of *global invariant*, which can be formally defined as follows.

Algorithm 3 Switching Controller Synthesis

Require: $\mathcal{H} = (Q, X, U, I, \ , F, E, D, G, R)$, $\mathcal{S}$, $\mathbf{1}$, τ, $\{T^*_{@} \mid q \in Q\}$, $\{\mathrm{r}^{@}_{1} \mid q \in Q\}$, $\{\epsilon_{@} \mid q \in Q\}$

1: $K_0 \leftarrow \ $; $I_0 \leftarrow \emptyset$; *flag* $\leftarrow$ **true**; $\mathcal{G}_0 \leftarrow \emptyset$; $n \leftarrow 0$
2: **while** *flag* **do**
3: $n \leftarrow n + 1$
4: **for** each $q \in Q$ **do**
5: $K_{=}(q) \leftarrow K_{=-1}(q) \cup \{\mathbf{5} \mid \exists e = (q', q) \in E, \exists t \ i \ 0, \exists \theta \in [-r^{@}_{\cdot}, 0].\ \mathbf{5} = R(e, \mathrm{x}^{\mathbf{5}}_{C}(\cdot)) \wedge \mathrm{x}^{\mathbf{5}}_{C}(\theta) \in \mathcal{G}_{=-1}(e)\}$
6: $I_{=}(q) \leftarrow$ **DInvariant**$(K_{=}(q), \boldsymbol{f}_{@}, T^*_{@}, \tau, \mathbf{1}, \mathcal{S}_{@}, \mathrm{r}^{@}_{1}, \epsilon_{@})$
7: $(q) \leftarrow \ (q) \cap \mathcal{S}_{@}$
8: **end for**
9: **for** each $e = (q, q') \in E$ **do**
10: $\mathcal{G}_{=}(e) \leftarrow G(e) \cap I_{=}(q) \cap \{\mathrm{x}^{\mathbf{5}}_{C}(\theta) \in I_{=}(q) \mid \exists t \ i \ 0, \forall \theta \in [-r^{@}_{\cdot}, 0].\ R(e, \mathrm{x}^{\mathbf{5}}_{C}(\cdot)) \in U_{@'}\}$
11: $G^*_{=}(e) \leftarrow$ **BackReach**$(\mathcal{G}_{=}(e), D(e), I_{=}(q), \mathbf{1}, \tau)$
12: **end for**
13: **if** $I_{=} == I_{=-1}$ **then**
14: *flag* $\leftarrow$ **false**
15: **end if**
16: **end while**
17: $^* \leftarrow \{ \ (q) \mid q \in Q\}$
18: $I^* \leftarrow \{I_{=}(q) \mid q \in Q\}$
19: $U^* \leftarrow \{\mathrm{x}^{\mathbf{5}}_{C}(\cdot) \in U \mid \exists q \in Q,\ \mathrm{x}^{\mathbf{5}}_{C}(\theta) \in I^*(q), \forall \theta \in [-r^{@}_{\cdot}, 0]\}$
20: $G^* \leftarrow \{(e, G^*_{=}(e)) \mid e \in E\}$
21: **if** $\forall e \in E, G^*(e) < \emptyset$ **then**
22: **return** $\mathcal{H}^* \leftarrow (Q, X, U^*, I^*, \ ^*, F, E, D, G^*, R)$
23: **end if**

Definition 11 (Global invariant). *Given a dHA $\mathcal{H}$, $I^* = \cup_{@ \in \&} I^*(q)$ is* global invariant *of $\mathcal{H}$, if I^* satisfies the following conditions:*

(c1) *for each $q \in Q$, the set $I^*(q)$ is a differential invariant of $(\ (q), \boldsymbol{f}_{@}, I(q))$,*

(c2) *for each $e = (q, q') \in E$, if $\mathrm{w}_{\mathbf{5}}(t) \in G^*(e)$, then*

$$\forall \theta \in [t' - r^{@'}_{\cdot}, t'],\ \mathbf{5}'(\theta) \in I^*(q'),$$

where $\mathbf{5}'(\cdot) = R(e, \mathrm{x}^{\mathbf{5}}_{C'}(\cdot))$ and $t' = t + D(e)$.

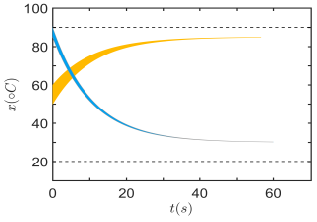


Figure 3: The over-approximate reachable sets for two modes of the heating system. Black dashed lines denote the safety set.

Algorithm 3 presents a procedure to compute a global invariant repeatedly until the safety requirement can be guaranteed by a computed global invariant (when *flag* holds, line 2-16), then a switching controller solving Problem 1 can be defined by the global invariant (line 17-23). In each iteration, for each mode (line 4-8), we compute a new mode invariant (line 5), a new differential invariant that can guarantee the safety requirement (line 6) by invoking Algorithm 1 (line 6), and a new initial condition satisfying the safety requirement (line 7); for each discrete transition (line 9-12), we compute a new guard condition without considering the discrete delay (line 10), and then a new guard condition considering the discrete delay by calling Algorithm 2 (line 11); then we test whether a global invariant that can guarantee the safety requirement is achieved (line 13-15).

The soundness of our approach is guaranteed by the following theorem.

Theorem 8 (Soundness). *Given a hybrid automaton $\mathcal{H} = (Q, X, U, I, \ , F, E, D, G, R)$ and its safety property $\mathcal{S}$, a dHA $\mathcal{H}^* = (Q, X, U^*, I^*, \ ^*, F, E, D, G^*, R)$ constructed by Algorithm 3 fulfills the three requirements (r1)-r(3) in Problem 1.*

Proof. We first prove that I^* is a safe global invariant of $\mathcal{H}^*$ if Algorithm 3 terminates and returns $\mathcal{H}^* = (Q, X, U^*, I^*, \ ^*, F, E, D, G^*, R)$, i.e., the conditions (c1) and (c2) in Definition 11 with restriction of safety requirement $\mathcal{S}$ hold. From line 6 in Algorithm 3, Definition 6 and the soundness of Algorithm 1, we have $I^*(q)$ is a safe differential invariant of $(\ ^*(q), f_{@}, I(q))$, then (c1) holds. Let $e = (q, q') \in E$, and $\mathrm{w}_{\mathbf{5}}(t) \in G^*(e)$. From line 5, 6 in Algorithm 3, we have

$$\left(\mathbf{5} \;\middle|\; \begin{array}{c} \exists e = (q', q) \in E, \exists t \ i \ 0, \exists \theta \in [-r^{@}_{\cdot}, 0]. \\ \mathbf{5} = R(e, \mathrm{x}^{\mathbf{5}}_{C}(\cdot)) \wedge \mathrm{x}^{\mathbf{5}}_{C}(\theta) \in \mathcal{G}(e) \end{array}\right) \subseteq I^*(q).$$

From line 11, it follows

$$G^*_{=}(e) = \textbf{BackReach}(\mathcal{G}_{=}(e), D(e), I_{=}(q), \mathbf{1}, \tau),$$

which implies (c2) holds. Now, we prove that (r1), (r2) and (r3) in Problem 1 are satisfied. Since each $I_{=}(q)$ is calculated by Algorithm 1, which can guarantee $I_{=}(q)$ is safe, thus $\mathcal{H}^*$ is safe, i.e., (r1) holds. In Algorithm 3, line 7 makes $^* \subseteq \ \cap \mathcal{S}$, line 6 makes $I^* \subseteq I$. From line 19, and $I^* \subseteq I$, it follows $U^* \subseteq U$. For any $e \in E$, as there exists $\theta \in [-r^{@}_{\cdot}, 0]$ such that $\mathrm{x}^{\mathbf{5}}_{C}(\theta) \in G^*(e)$, hence $\mathrm{x}^{\mathbf{5}}_{C+\ (4)}(\theta) \in \mathcal{G}(e)$. From line 10 and 11, it follows $\mathrm{x}^{\mathbf{5}}_{C+\ (4)}(\theta) \in G(e) \cap I^*(q)$. Thus, (r2) holds. Clearly, I^* contains all safe trajectories of $\mathcal{H}$, so if $\mathcal{H}$ is non-blocking with respect to the safe requirement $\mathcal{S}$, then $\mathcal{H}^*$ is also non-blocking, i.e., (r3) holds.

Example 3. *We continue to consider the heating system example. Let $K_1 = 0.25$, $K_2 = 0.15$, $h = 32$, $w_1 = 0.5$, and $w_2 = 3$ for the dHA of the heating system in Example 1. For mode q_1, $M_{@_1} = -0.1$ is trivially a Metzler matrix. Applying Theorem 2, we have $T^*_{@_1} = 56.567s$. The same procedure applies to mode q_2, we have $T^*_{@_2} = 60.043s$. By Algorithm 3, we obtain differential invariants $I^*(q_1) = \{x \mid 30 \leq x \leq 84.91\}$ and $I^*(q_2) = \{x \mid 30.2056 \leq x \leq 90\}$. Also, strengthened guarded conditions on e_1 and e_2 can be easily computed as $G^*(e_1) = \{x \mid 30 \leq x \leq 84.30\}$ and $G^*(e_2) = \{x \mid 34.5 \leq x \leq 90\}$. The over-approximation of the reachable sets from the initial sets in the two modes respectively are displayed in Figure 3.*

Mode	ϵ	ζ	β	η	γ	δ
q_1	0.001	$\begin{matrix}1\\1\end{matrix}$	1	12.58	5.1642	12.58
q_2	0.001	$\begin{matrix}1\\1\end{matrix}$	1	24.66	4.2270	24.66

Table 1: The value of parameters in Section 5.1

Mode	ϵ	ζ	β	η	γ	δ	$g_{<0G}$	$\mathcal{G}$	ι
q_1	10^{-4}	$\begin{matrix}1\\1\end{matrix}$	1	0.8	0.626	0.8	0.008	0.078	0.2
q_2	10^{-4}	$\begin{matrix}1\\1\end{matrix}$	1	1.85	0.88	1.85	0.0046	0.0746	0.2

Table 2: The value of parameters in Section 5.2

5 EXPERIMENTAL RESULTS

We implement our algorithms [1] in Matlab, based upon the interval data-structure in CORA [1]. We adopt the discretization parameters from [1] and [11] for the two examples, respectively. All experiments are performed on an Intel(R) Core(TM) i5-8265U CPU (1.60GHz) with 8GB RAM.

5.1 Low-pass Filter System

We first consider a low-pass filter system with delays, adapted from CORA [1]. It includes two first order low-pass filters q_1 and q_2, represented by

$$q_1: \begin{cases} \dot{x}_1(t) = -14.58x_1(t) + 2x_1(t-0.1) + 0.5\sin(t) \\ \dot{x}_2(t) = -20.05x_2(t) + 2x_2(t-0.1) + 0.5\sin(t) \\ (q_1) = [-1,1]\times[-2,2] \\ I(q_1) = \mathrm{R}^2, \end{cases}$$

$$q_2: \begin{cases} \dot{x}_1(t) = -32.66x_1(t) + 8x_1(t-0.1) + 0.5\sin(t) \\ \dot{x}_2(t) = -47.25x_2(t) + 8x_2(t-0.1) + 0.5\sin(t) \\ (q_2) = [-2.25,2.5]\times[-2.5,2.5] \\ I(q_2) = \mathrm{R}^2. \end{cases}$$

There are two discrete transitions $e_1 = (q_1, q_2)$ and $e_2 = (q_2, q_1)$ between q_1 and q_2, and the corresponding guard conditions are $G(e_1) = \{(x_1, x_2) \in \mathrm{R}^2 \mid x_1 \geq 0.7\}$, $G(e_2) = \{(x_1, x_2) \in \mathrm{R}^2 \mid x_2 \geq 0.6\}$. Reset functions are identity mappings. Moreover, both discrete transitions are taken with delays $D(e_1) = 0.02$ and $D(e_2) = 0.02$, respectively. The safety requirement is $\mathcal{S} = \{(x_1, x_2) \in \mathrm{R}^2 \mid -2.7 \leq x_1 \leq 2.7 \wedge -2.6 \leq x_2 \leq 2.6\}$.

For mode q_1, $M_{@_1} = \begin{matrix}-12.58 & 0\\ 0 & -18.05\end{matrix}$ is obviously a Metzler matrix satisfying the two properties listed in Proposition 1. By Theorem 2, the differential invariant synthesis problem is reduced to a $T^*_{@_1}$-differential invariant synthesis problem, where $T^*_{@_1} = 0.5782s$ is computed with the parameters listed in Table 1. Similarly, for mode q_2, $M_{@_2} = \begin{matrix}-4.66 & 0\\ 0 & -39.25\end{matrix}$ is also a Metzler matrix satisfying the two properties listed in Proposition 1. $T^*_{@_2} = 0.7605s$ is computed with the parameters listed in Table 1. The computed over-approximation of the reachable set within $T^*_{@_1}$ for mode q_1 using our approach is given in Fig. 4(a) and 4(b). The over-approximation of the reachable set in $T^*_{@_2}$ for mode q_2 is shown in Figure 4(c) and 4(d) with our approach. Clearly, the delay dynamical system in this mode satisfies the ball convergence property. The guard conditions without discrete delays are $\mathfrak{G}(e_1) = \{(x_1, x_2) \in \mathrm{R}^2 \mid 0.7 \leq x_1 \leq 1 \wedge -2 \leq x_2 \leq 2\}$ and $\mathfrak{G}(e_2) = \{(x_1, x_2) \in \mathrm{R}^2 \mid -1 \leq x_1 \leq 1 \wedge 0.6 \leq x_2 \leq 2\}$. Finally, applying Algorithm 2, the strengthened guard conditions $G^*(e_1)$ and $G^*(e_2)$, that can guarantee the safety, are computed as showed in Fig. 5.

[1] Available at https://github.com/YunjunBai/Inv_DHA.

5.2 Predator-prey Populations

We consider a nonlinear predator-prey population dynamics under seasonal succession: a hybrid Lotka–Volterra competition model with delays adapted from [21]. Two modes for two seasons are modelled as follows:

$$q_1: \begin{cases} \dot{x}_1(t) = -x_1(t)(1 - \frac{G_1(C)}{100}) + 0.2d_1 + w_{11}(t) \\ \dot{x}_2(t) = -1.5x_2(t)(1 - \frac{G_2(C)}{100}) + 0.1d_2 + w_{12}(t) \\ (q_1) = [-0.2,0.2]\times[-0.1,0.1] \\ I(q_1) = \mathrm{R}^2. \end{cases}$$

$$q_2: \begin{cases} \dot{x}_1(t) = -2.5x_1(t) + 0.2x_1(t-0.01)(1+x_2(t)) + w_{21}(t) \\ \dot{x}_2(t) = -2x_2(t) + 0.15x_2(t-0.01)(1+x_2(t)) + w_{22}(t) \\ (q_2) = [-0.2,0.2]\times[-0.2,0.2] \\ I(q_2) = \mathrm{R}^2. \end{cases}$$

where q_1 and q_2 represent two seasons, $d_1 = x_1(t-0.1)(1+x_1(t))$, $d_2 = x_2(t-0.1)(1+x_2(t))$, x_1 is the number of prey (for example, rabbits), x_2 is the number of some predator (for example, foxes), $w_{ij}(t) = 0.07\cos 2t$ $(i, j = 1, 2)$ denote the perturbations. The real coefficients describe the interaction of the two species, the intrinsic growth rate and the environment capacity of the population in season i, respectively. There are two discrete transitions $e_1 = (q_1, q_2)$ and $e_2 = (q_2, q_1)$ between mode q_1 and mode q_2, and their corresponding guard conditions initially are $G(e_1) = \{(x_1, x_2) \in \mathrm{R}^2 \mid -0.06 \leq x_1 \leq 0.06 \wedge -0.06 \leq x_2 \leq 0.07\}$, $G(e_2) = \{(x_1, x_2) \in \mathrm{R}^2 \mid -0.05 \leq x_1 \leq 0.05 \wedge -0.06 \leq x_2 \leq 0.06\}$. Reset functions are identity mappings. Moreover, both discrete transitions are taken with delays $D(e_1) = 1$ and $D(e_2) = 0.55$, respectively. The safety requirement is $\mathcal{S} = \{(x_1, x_2) \in \mathrm{R}^2 \mid -0.20 \leq x_1 \leq 0.21 \wedge -0.21 \leq x_2 \leq 0.22\}$.

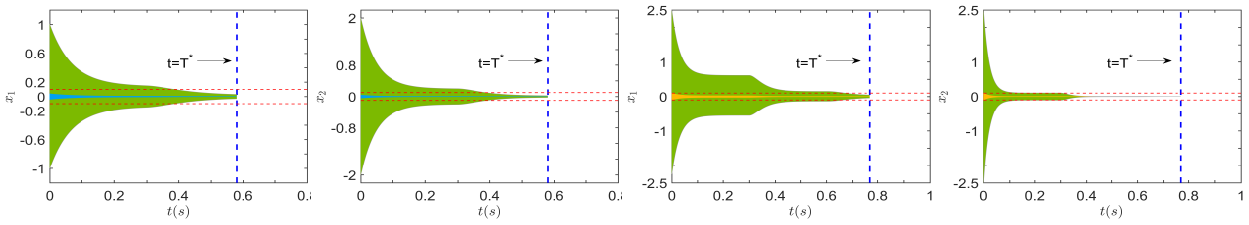
By linearizing mode q_1, we have:

$$\begin{matrix} \dot{x}_1(t) = -x_1(t) + 0.2x_1(x-0.1) + w_{11}(t) \\ \dot{x}_2(t) = -1.5x_2(t) + 0.1x_2(x-0.1) + w_{12}(t) \end{matrix}.$$

Clearly, $M_{@_1} = \begin{matrix}-0.8 & 0\\ 0 & -1.4\end{matrix}$ is a Metzler matrix satisfying the two properties listed in Proposition 1. By Theorems 6 and 7, the differential invariant synthesis problem for mode q_1 is reduce to a $T^*_{@_1}$-differential invariant synthesis problem, where $T^*_{@_1} = 4.6825$s is computed using our approach with the parameters listed in Table 2.

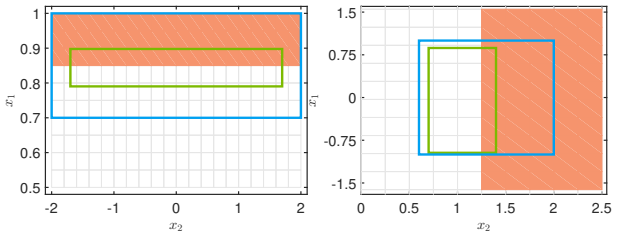
Here it is noteworthy that $\iota = 0.2$, covering the entire initial set. Similarly, for mode q_2, the linearization of its dynamics is :

$$\begin{matrix} \dot{x}_1(t) = -2.5x_1(t) + 0.2x_1(t-0.01) + w_{21}(t) \\ \dot{x}_2(t) = -2x_2(t) + 0.15x_2(t-0.01) + w_{22}(t) \end{matrix}.$$



(a) (b) (c) (d)

Figure 4: In the low-pass filter system, the over-approximation of the reachable set of mode q_1 is shown in (a)&(b), and the one of mode q_2 is shown in (c)&(d). All trajectories, marked with blue for mode q_1 (yellow for mode q_2), starting from the states contained in the first ball $\mathrm{B}(\frac{w<0G}{\delta})$, are always enclosed in the second ball $\mathrm{B}(\frac{w<0G}{\eta})$ denoted by two red dashed lines.



(a) 4_1 (b) 4_2

Figure 5: The synthesized switching controller on the edge e_1 and e_2 of the low-pass filter system. $\mathcal{G}$ is indicated by the blue box, and G^* is indicated by the red region. The green box stands for the forward reachable set in 0.01s from $G^*(e_1)$ (0.02s from $G^*(e_2)$).

Clearly, $M_{@_2} = \begin{matrix} -2.3 & 0 \\ 0 & -1.85 \end{matrix}$ is also a Metzler matrix satisfying the two properties listed in Proposition 1. With the parameters listed in Table 2, a bounded time $T^*_{@_2} = 3.3326$s is computed. The computed over-approximation of the reachable set within $t \geq T^*_{@_1}$ for mode q_1 is showed in Fig. 6(a)&6(b). And the computed over-approximation of the reachable set within $t \geq T^*_{@_2}$ for mode q_2 are shown in Fig. 6(c)&6(d) using our approach. The guard conditions without discrete delays are computed as $\mathcal{G}(e_1) = \{(x_1, x_2) \in \mathrm{R}^2 \mid -0.06 \leq x_1 \leq 0.06 \wedge -0.06 \leq x_2 \leq 0.07\}$ and $\mathcal{G}(e_2) = \{(x_1, x_2) \in \mathrm{R}^2 \mid -0.05 \leq x_1 \leq 0.05 \wedge -0.06 \leq x_2 \leq 0.06\}$. Finally, applying Algorithm 2, the strengthened guard conditions $G^*(e_1)$ and $G^*(e_2)$, which can guarantee the safety requirement, are obtained as shown in Fig. 7.

6 CONCLUSION

We introduced the notion of delay hybrid automata (dHA) in order to model continuous delays and discrete delays in cyber-physical systems uniformly. Based on dHA, we proposed an approach on how to automatically synthesize a switching controller for a delay hybrid system with perturbations against a given safety requirement. To the end, we presented a new approach for over-approximating a nonlinear DDE with perturbation using ball-convergence analysis based on Metzler matrix. Two case studies were provided to indicate the effectiveness and efficiency of the proposed approach.

For future work, it deserves to investigate how to synthesize a switching controller for a dHA against much richer properties defined e.g. by signal temporal logic [23] or metric temporal logic [20]. In addition, it is interesting to consider our method to deal with more general forms of DDEs. Besides, it is a challenge how to guarantee the completeness of our approach, which essentially corresponds to a long-standing problem on how to compute reachable sets of hybrid systems in the infinite time horizon.

ACKNOWLEDGEMENTS

We thank Prof. Martin Fränzle, Dr. Mingshuai Chen and Mr. Shenghua Feng for fruitful discussions on this topic, and also thank the anonymous referees for their constructive comments and criticisms that improve this paper very much.

The first, third and sixth authors are partly funded by NSFC-61625206 and NSFC-61732001, the second author is partly funded by NSFC-61902284, the fourth author is partly funded by NSFC-61732001, and the fifth author is partly funded by NSFC-61872341, NSFC-61836005 and the CAS Pioneer Hundred Talents Program.

REFERENCES

[1] M. Althoff and D. Grebenyuk. Implementation of interval arithmetic in CORA 2016. In *Proc. of the 3rd International Workshop on Applied Verification for Continuous and Hybrid Systems*, 2016.
[2] R. Alur, C. Courcoubetis, N. Halbwachs, T. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138(1):3 – 34, 1995. Hybrid Systems.
[3] E. Asarin, O. Bournez, T. Dang, O. Maler, and A. Pnueli. Effective synthesis of switching controllers for linear systems. *Proc. IEEE*, 88(7):1011–1025, 2000.
[4] Y. Bai, T. Gan, L. Jiao, B. Xue, and N. Zhan. Switching controller synthesis for time-delayed hybrid systems. *Science China Mathematica*, 51(1(1-2)):97–114, 2021. in Chinese.
[5] C. Belta, B. Yordanov, and E. A. Gol. *Formal Methods for Discrete-Time Dynamical Systems*. Springer, 2017.
[6] A. Berman and R. J. Plemmons. *Nonnegative matrices in the mathematical sciences*, volume 9. Siam, 1994.
[7] M. Chen, M. Fraenzle, Y. Li, P. N. Mosaad, and N. Zhan. Indecision and delays are the parents of failure – taming them algorithmically by synthesizing delay-resilient control. *Acta Informatica*, 2020.
[8] M. Chen, M. Fränzle, Y. Li, P. Mosaad, and N. Zhan. Validated simulation-based verification of delayed differential dynamics. In *FM 2016*, volume 9995 of *LNCS*,