Approximately Bisimilar Symbolic Models for Digital Control Systems

Rupak Majumdar¹ and Majid Zamani²

¹ Max Planck Institute for Software Systems, Germany
rupak@mpi-sws.org

² Department of Electrical Engineering, University of California at Los Angeles
zamani@ee.ucla.edu

Abstract. Symbolic approaches to control hybrid systems construct a discrete approximately-bisimilar abstraction of a continuous control system and apply automata-theoretic techniques to construct controllers enforcing given specifications. For the class of digital control systems (i.e., whose control signals are piecewise constant) satisfying incremental input-to-state stability (δ -ISS), existing techniques to compute discrete abstractions begin with a quantization of the state and input sets, and show that the quantized system is approximately bisimilar to the original if the sampling time is sufficiently large or if the Lyapunov functions of the system decrease fast enough. If the sampling time is not sufficiently large, the former technique fails to apply. While abstraction based on Lyapunov functions may be applicable, because of the conservative nature of Lyapunov functions in practice, the size of the discrete abstraction may be too large for subsequent analyses.

In this paper, we propose a technique to compute discrete approximately-bisimilar abstractions of δ -ISS digital control systems. Our technique quantizes the state and input sets, but is based on multiple sampling steps: instead of requiring that the sampling time is sufficiently large (which may not hold), the abstract transition system relates states multiple sampling steps apart.

We show on practical examples that the discrete state sets computed by our procedure can be several orders of magnitude smaller than existing approaches, and can compute symbolic approximate-bisimilar models even when other existing approaches do not apply or time-out. Since the size of the discrete state set is the main limiting factor in the application of symbolic control, our results enable symbolic control of larger systems than was possible before.

1 Introduction

Many cyber-physical systems involve the complex interplay between continuous controlled dynamical systems and discrete controllers. Correctness requirements for these systems involve temporal specifications about the evolution of the dynamics, which are not easily amenable to classical continuous controller synthesis techniques. As a result, in recent years, a lot of research has focused on *symbolic*

models of systems involving both continuous and discrete components (so called *hybrid systems*). A symbolic model is a discrete approximation of the continuous system such that controllers designed for the approximation can be refined to controllers for the original system. Symbolic models are interesting because they allow the algorithmic machinery for controller synthesis of discrete systems w.r.t. temporal specifications [5,22,14] to be used to automatically synthesize controllers for hybrid systems.

The key to this methodology is the existence of finite-state symbolic models that are *bisimilar* to the original system. When the continuous time model has very simple dynamics, such as clocks, one can show that finite-state bisimilar models exist and can be effectively computed [2]. Unfortunately, even for very simple dynamics such as stopwatches, finite-state bisimilar models may not exist [12]. The insight, developed over the past five years, is that for control of dynamical systems where there is a natural metric on the states, one can use ε -*approximations* of classical equivalence relations [8,9] to relate the original system and the symbolic model. An ε -approximate bisimulation relaxes the condition of bisimulation by requiring that two bisimilar states are within ε distance of each other, and guarantees that for each trajectory starting at one state, there is a trajectory starting at the other that is always within ε distance away. For many continuous dynamical systems, ε -approximate bisimulation relations of finite index have been shown to exist [20,10,17,18].

We focus on digital control systems, in which there is a fixed sampling time τ and the control action is chosen from a compact set and held constant for τ time units. Current approaches to building the symbolic model, such as [17,18,10], proceed as follows. First, they choose discretizations of the state and input sets. Then, they use either the incremental stability assumption or incremental Lyapunov functions to show that if the discretizations are sufficiently small, and the sampling time τ is sufficiently big, then the resulting discrete abstraction is ε -approximate bisimilar to the original system. If the sample time, which is usually not under the control of the verification engineer, is not sufficiently large, the technique will not apply. Even if the method applies, the resulting state space is often prohibitively large. This is usually the case for symbolic models built using conservative Lyapunov functions [10].

We show a construction of approximately bisimilar models for digital control systems that improves upon known algorithms. The insight in our construction is to consider a number of sampling steps instead of only one step. That is, we dilate the quantum of time of the control system and observe the system only every k steps, for some parameter k . Then, instead of requiring that the sampling time is sufficiently big, we only require that the number of steps is chosen sufficiently large, so that the technique is always applicable. Further, we demonstrate experimentally that our technique can give symbolic models that require a much coarser discretization of the state and input sets, resulting in symbolic models with many fewer states, while guaranteeing ε -approximate bisimulation with the original system.

We have implemented our algorithm on top of Pessoa [16], a tool that computes symbolic models and then performs controller synthesis on the symbolic models. We show on a set of benchmark examples that our technique produces symbolic models whose state sets are orders of magnitude smaller than previous approaches, and can finish computing the symbolic model and performing controller synthesis in seconds, when previous techniques either do not apply, or time-out after several hours.

2 Systems and Approximate Equivalences

Preliminaries: The symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{R}^+$, and $\mathbb{R}_0^+$ denote the set of natural, integer, real, positive, and non-negative real numbers, respectively. A *metric space* (Y, d) consists of a set Y and a metric $d : Y \times Y \rightarrow \mathbb{R}_0^+$ on Y . Given a vector $x \in \mathbb{R}^n$, we denote by x_i the i th element of x , and by $\|x\|$ the infinity norm of x , namely, $\|x\| = \max\{|x_1|, |x_2|, \dots, |x_n|\}$. Given a matrix $M = \{m_{ij}\} \in \mathbb{R}^{n \times m}$, we denote by $\|M\|$ the infinity norm of M , namely, $\|M\| = \max_{1 \leq i \leq n} \sum_{j=1}^m |m_{ij}|$. The symbol I_n denotes the identity matrix in $\mathbb{R}^{n \times n}$. The closed ball centered at $x \in \mathbb{R}^n$ with radius ε is defined by $\mathcal{B}_\varepsilon(x) = \{y \in \mathbb{R}^n \mid \|x - y\| \leq \varepsilon\}$.

Given a measurable function $f : \mathbb{R}_0^+ \rightarrow \mathbb{R}^n$, the (*essential*) *supremum* (sup norm) of f is denoted by $\|f\|_\infty$; we recall that $\|f\|_\infty = (\text{ess}) \sup \{\|f(t)\|, t \geq 0\}$. A continuous function $\gamma : \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+$ is said to belong to class $\mathcal{K}$ if it is strictly increasing and $\gamma(0) = 0$; γ is said to belong to class $\mathcal{K}_\infty$ if $\gamma \in \mathcal{K}$ and $\gamma(r) \rightarrow \infty$ as $r \rightarrow \infty$. A continuous function $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+$ is said to belong to class $\mathcal{KL}$ if, for each fixed s , the map $\beta(r, s)$ belongs to class $\mathcal{K}_\infty$ with respect to r and, for each fixed nonzero r , the map $\beta(r, s)$ is decreasing with respect to s and $\beta(r, s) \rightarrow 0$ as $s \rightarrow \infty$.

A set $B \subseteq \mathbb{R}^n$ is called a *box* if $B = \prod_{i=1}^n [c_i, d_i]$, where $c_i, d_i \in \mathbb{R}$ with $c_i < d_i$ for each $i \in \{1, \dots, n\}$. The *span* of a box B is defined as $\text{span}(B) = \min \{|d_i - c_i| \mid i = 1, \dots, n\}$. For a box B and $\eta \leq \text{span}(B)$, define the η -approximation $[B]_\eta = \{b \in B \mid b_i = k_i \eta \text{ for some } k_i \in \mathbb{Z}, i = 1, \dots, n\}$. Note that $[B]_\eta \neq \emptyset$ for any $\eta \leq \text{span}(B)$. Geometrically, for any $\eta \in \mathbb{R}^+$ with $\eta \leq \text{span}(B)$ and $\lambda \geq \eta$ the collection of sets $\{\mathcal{B}_\lambda(p)\}_{p \in [B]_\eta}$ is a finite covering of B , i.e., $B \subseteq \bigcup_{p \in [B]_\eta} \mathcal{B}_\lambda(p)$. By defining $[\mathbb{R}^n]_\eta = \{a \in \mathbb{R}^n \mid a_i = k_i \eta, k_i \in \mathbb{Z}, i = 1, \dots, n\}$, the set $\bigcup_{p \in [\mathbb{R}^n]_\eta} \mathcal{B}_\lambda(p)$ is a countable covering of $\mathbb{R}^n$ for any $\eta \in \mathbb{R}^+$ and $\lambda \geq \eta/2$. We extend the notions of span and approximation to finite unions of boxes as follows. Let $A = \bigcup_{j=1}^M A_j$, where each A_j is a box. Define $\text{span}(A) = \min \{\text{span}(A_j) \mid j = 1, \dots, M\}$, and for any $\eta \leq \text{span}(A)$, define $[A]_\eta = \bigcup_{j=1}^M [A_j]_\eta$.

Digital Control Systems: We now define digital control systems, which are continuous time controlled dynamical systems with piecewise-constant inputs of a fixed duration.

Definition 1. A (digital) control system is a tuple $\Sigma = (\mathbb{R}^n, \tau, \mathcal{U}, \mathcal{U}_\tau, f)$ where:

- $\mathbb{R}^n$ is the state space;

- $\tau \in \mathbb{R}^+$ is the sampling time;
- $\mathbf{U} \subseteq \mathbb{R}^m$ is the input set, which is assumed to be a finite union of boxes containing the origin;
- $\mathcal{U}_\tau$ contains curves piecewise constant of duration τ , i.e.,

$$\mathcal{U}_\tau = \left\{ v : \mathbb{R}_0^+ \rightarrow \mathbf{U} \mid v(t) = v((l-1)\tau), t \in [(l-1)\tau, l\tau[, l \in \mathbb{N} \right\};$$

- $f : \mathbb{R}^n \times \mathbf{U} \rightarrow \mathbb{R}^n$ is a continuous map satisfying the following Lipschitz assumption: for every compact set $Q \subset \mathbb{R}^n$, there exists a constant $L \in \mathbb{R}^+$ such that for all $x, y \in Q$ and all $u \in \mathbf{U}$, we have: $\|f(x, u) - f(y, u)\| \leq L\|x - y\|$.

A curve $\xi :]a, b[\rightarrow \mathbb{R}^n$ is said to be a *trajectory* of Σ if there exists $v \in \mathcal{U}_\tau$ satisfying:

$$\dot{\xi}(t) = f(\xi(t), v(t)), \quad (1)$$

for almost all $t \in]a, b[$. We also write $\xi_{xv}(t)$ to denote the point reached at time t under the input v from initial condition $x = \xi_{xv}(0)$; this point is uniquely determined, since the assumptions on f ensure existence and uniqueness of trajectories [19]. Although we have defined trajectories over open domains, we shall refer to trajectories $\xi_{xv} : [0, \tau] \rightarrow \mathbb{R}^n$ and input curves $v : [0, \tau[\rightarrow \mathbf{U}$, with the understanding of the existence of a trajectory $\xi'_{xv'} :]a, b[\rightarrow \mathbb{R}^n$ and input curve $v' :]a, b[\rightarrow \mathbf{U}$ such that $\xi_{xv} = \xi'_{xv'}|_{[0, \tau]}$ and $v = v'|_{[0, \tau]}$. Note that by continuity of ξ , we have that $\xi_{xv}(\tau)$ is uniquely defined as the left limit of $\xi_{xv}(t)$ with $t \rightarrow \tau$.

A control system Σ is said to be *forward complete* if every trajectory is defined on an interval of the form $]a, \infty[$. Sufficient and necessary conditions for a system to be forward complete can be found in [4].

Stability: As in [17,18,10], we assume incremental input-to-state stability of the control system.

Definition 2. [3] A control system Σ is incrementally input-to-state stable (δ -ISS) if it is forward complete and there exist a $\mathcal{KL}$ function β and a $\mathcal{K}_\infty$ function γ such that for any $t \in \mathbb{R}_0^+$, any $x, x' \in \mathbb{R}^n$, and any $v, v' \in \mathcal{U}_\tau$ the following condition is satisfied:

$$\|\xi_{xv}(t) - \xi_{x'v'}(t)\| \leq \beta(\|x - x'\|, t) + \gamma(\|v - v'\|_\infty). \quad (2)$$

Remark 1. For linear control systems, the functions β and γ in Definition 2 can be explicitly computed as follows. It can be readily verified that any linear control system:

$$\dot{\xi} = A\xi + Bv, \quad \xi(t) \in \mathbb{R}^n, \quad v(t) \in \mathbf{U} \subseteq \mathbb{R}^m, \quad (3)$$

is δ -ISS if and only if A is globally asymptotically stable, i.e., every eigenvalue of A has strictly negative real part. Then, the functions β and γ can be chosen as:

$$\beta(r, t) = \|e^{At}\| r; \quad \gamma(r) = \left(\|B\| \int_0^\infty \|e^{As}\| ds \right) r, \quad (4)$$

where $\|e^{At}\|$ denotes the infinity norm of e^{At} .

The assumption of δ -ISS does not restrict the class of digital control systems significantly. If a control system Σ is not δ -ISS, one can design an internal control loop rendering Σ δ -ISS. Assume there exists a smooth controller $k(\xi, v)$ rendering control system Σ δ -ISS with respect to the input v . Note that by using the results in [21], there exists a positive number τ^* such that for any $\tau < \tau^*$, the digitized version of k makes the system Σ δ -ISS with respect to the input v . Now, one can drive v by designing another controller on top of k to satisfy some desired specifications, e.g., using the symbolic abstraction techniques explained in Section 3.

If Σ is a linear control system, one can use the results in control theory [13] to design a state feedback gain k rendering Σ globally asymptotically stable and, hence, δ -ISS. If Σ is a nonlinear control system, one can use the results in [23] to design controllers rendering Σ δ -ISS.

Metric Systems and Approximate Relations: We now recall the notions of metric systems that we will use as abstract models for control systems as well as approximate bisimulation relations on metric systems that will be central to our abstractions.

Definition 3. A metric system S is a quintuple $S = (X, U, \rightarrow, (Y, d), H)$ consisting of a (possibly infinite) set of states X ; a set of inputs U ; a transition relation $\rightarrow \subseteq X \times U \times X$; an output metric space (Y, d) ; and an output function $H : X \rightarrow Y$.

A transition $(x, u, x') \in \rightarrow$ is written by $x \xrightarrow{u} x'$. If $x \xrightarrow{u} x'$, state x' is called a u -successor, or simply, successor, of state x . A metric system is *countable* (resp. *finite*) if X is countable (resp. finite). A metric system is *deterministic* if for any state $x \in X$ and any input $u \in U$, there exists at most one u -successor (there may be none).

Metric systems capture the dynamics of a system through the transition relation: for states $x, x' \in X$ and $u \in U$, if $x \xrightarrow{u} x'$ then it is possible to evolve from state x to state x' under the input labeled by u . Given a control system $\Sigma = (\mathbb{R}^n, \tau, \mathcal{U}, \mathcal{U}_\tau, f)$, define the metric system $S(\Sigma) = (\mathbb{R}^n, \mathcal{U}_\tau, \rightarrow, (\mathbb{R}^n, \|\cdot\|), \lambda x.x)$ where $x \xrightarrow{u} x'$ if there is a trajectory $\xi_{xu} : [0, \tau] \rightarrow \mathbb{R}^n$ such that $x' = \xi_{xu}(\tau)$, and (with abuse of notation) we define the metric $\|\cdot\| : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}_0^+$ as $\|x - y\|$ for any $x, y \in \mathbb{R}^n$.

Intuitively, the metric system captures all the behaviors of the original control system. The notion of capturing all behaviors is formalized using (approximate) bisimulation relations [15,9], that we define below.

Definition 4. Let $S = (X, U, \rightarrow, (Y, d), H)$ and $S' = (X', U', \rightarrow', (Y', d'), H')$ be metric systems with the same output metric spaces $(Y, d) = (Y', d')$. For each $\varepsilon \geq 0$, a binary relation $R \subseteq X \times X'$ is said to be an ε -approximate simulation relation from S to S' , if the following three conditions are satisfied:

- (i) for every $x \in X$, there exists $x' \in X'$ with $(x, x') \in R$;
- (ii) for every $(x, x') \in R$ we have $d(H(x), H'(x')) \leq \varepsilon$;

(iii) for every $(x, x') \in R$ and $u \in U$, if $x \xrightarrow{u} y$ in S then there exists some $u' \in U'$ such that $x' \xrightarrow{u'} y'$ and $(y, y') \in R$.

System S is ε -approximately simulated by S' , denoted by $S \preceq^\varepsilon S'$, if there exists an ε -approximate simulation relation from S to S' .

An ε -approximate simulation relation $R \subseteq X \times X'$ is an ε -approximate bisimulation relation between S and S' if R is an ε -approximate simulation relation from S to S' and R^{-1} is an ε -approximate simulation relation from S' to S .

System S and S' are ε -approximate bisimilar, denoted by $S \cong^\varepsilon S'$, if there exists an ε -approximate bisimulation relation R between S and S' .

When $\varepsilon = 0$, the condition (ii) above becomes $(x, x') \in R$ if and only if $H(x) = H'(x')$, and R becomes an exact simulation relation [15]. Similarly, a 0-approximate bisimulation relation R is an exact bisimulation relation.

We next consider constructing *countable* abstractions that are ε -approximate bisimilar to the time discretization of Σ for a given parameter $\varepsilon \in \mathbb{R}^+$.

3 Symbolic Models for Control Systems

3.1 Main Construction

This section contains the main contribution of the paper. We show that a δ -ISS digital control system Σ admits a countable symbolic abstraction. First, we consider a variant of the metric system $S(\Sigma)$ which relates two states if the second is reached from the first in $k \cdot \tau$ time for a parameter $k \in \mathbb{N}$.

Given a constant $k \in \mathbb{N}$ and a digital control system $\Sigma = (\mathbb{R}^n, \tau, \mathbf{U}, \mathcal{U}_\tau, f)$, define the metric system $S_{k\tau}(\Sigma) = (\mathbb{R}^n, \mathcal{U}_\tau, \rightarrow, (\mathbb{R}^n, \|\cdot\|), \lambda x.x)$ where $x \xrightarrow{u} x'$ if there exists a trajectory $\xi_{xu} : [0, k\tau] \rightarrow \mathbb{R}^n$ of Σ satisfying $\xi_{xu}(k\tau) = x'$. Although the metric system $S_{k\tau}(\Sigma)$ relates states of Σ that are k sampling steps apart, this system is not less accurate than $S(\Sigma)$ relating states of Σ one sampling time apart in the sense that for any initialized run with k transitions in the latter there is one transition in the former and vice versa.

Now, assume that Σ is δ -ISS. Consider a triple $\mathbf{q} = (\eta, \mu, k)$, where $\eta \in \mathbb{R}^+$ is the *state space quantization* which determines a discretization of the state space, $\mu \in \mathbb{R}^+$ is the *input set quantization* which determines a discretization of the inputs, and $k \in \mathbb{N}$ is a design parameter. Given Σ and $\mathbf{q}$, consider the following metric system:

$$S_{\mathbf{q}}(\Sigma) = \left([\mathbb{R}^n]_\eta, \prod_{i=1}^k [\mathbf{U}]_\mu, \rightarrow, (\mathbb{R}^n, \|\cdot\|), H' \right), \quad (5)$$

where $x \xrightarrow{u} x'$ if there is a trajectory $\xi_{xu} : [0, k\tau] \rightarrow \mathbb{R}^n$ such that $\|\xi_{xu}(k\tau) - x'\| \leq \eta/2$ and $H' : [\mathbb{R}^n]_\eta \rightarrow \mathbb{R}^n$ is the natural inclusion map mapping $x \in [\mathbb{R}^n]_\eta$ to itself. We have abused notation by identifying $v \in [\mathbf{U}]_\mu$ with the constant input curve with domain $[0, \tau]$ and value v and identifying $u \in \prod_{i=1}^k [\mathbf{U}]_\mu$ with the

concatenation of k control inputs $v^i \in [\mathbf{U}]_\mu$ (i.e., $u(t) = v^i$ for any $t \in [(i-1)\tau, i\tau]$) for $i = 1, \dots, k$. The set of states of $S_q(\Sigma)$ is countable in general, and finite when the set of states of Σ is restricted to a compact set.

The transition relation of $S_q(\Sigma)$ is well defined in the sense that for every $x \in [\mathbb{R}^n]_\eta$ and every $u \in \prod_{i=1}^k [\mathbf{U}]_\mu$ there always exists $x' \in [\mathbb{R}^n]_\eta$ such that $x \xrightarrow{u} x'$. This can be seen by noting that by definition of $[\mathbb{R}^n]_\eta$, for any $\hat{x} \in \mathbb{R}^n$ there always exists a state $\hat{x}' \in [\mathbb{R}^n]_\eta$ such that $\|\hat{x} - \hat{x}'\| \leq \eta/2$. Hence, for $\xi_{xu}(k\tau)$ there always exists a state $x' \in [\mathbb{R}^n]_\eta$ satisfying $\|\xi_{xu}(k\tau) - x'\| \leq \eta/2$.

We can now present the main result of the paper.

Theorem 1. *Let $\Sigma = (\mathbb{R}^n, \tau, \mathbf{U}, \mathcal{U}_\tau, f)$ be a δ -ISS digital control system, and let functions β and γ satisfy (2). For any $\varepsilon \in \mathbb{R}^+$ and any triple $\mathbf{q} = (\eta, \mu, k)$ of quantization parameters, we have $S_q(\Sigma) \cong^\varepsilon S_{k\tau}(\Sigma)$ if $\mu \leq \text{span}(\mathbf{U})$ and*

$$\beta(\varepsilon, k\tau) + \gamma(\mu) + \eta/2 \leq \varepsilon. \quad (6)$$

Before giving the proof, we point out that if Σ is δ -ISS, there always exists a triple $\mathbf{q} = (\eta, \mu, k)$ satisfying condition (6). Since β is a $\mathcal{KL}$ function, there exists sufficiently large $k \in \mathbb{N}$ such that $\beta(\varepsilon, k\tau) < \varepsilon/2$; for this value of k , by choosing sufficiently small values of η and μ , condition (6) can be fulfilled.

Proof. For notational simplicity, fix $S_{k\tau}(\Sigma) = (X_{k\tau}, U_{k\tau}, \rightarrow_{k\tau}, (\mathbb{R}^n, \|\cdot\|), H_{k\tau})$ and $S_q(\Sigma) = (X_q, U_q, \rightarrow_q, (\mathbb{R}^n, \|\cdot\|), H_q)$.

We start by proving $S_{k\tau}(\Sigma) \preceq^\varepsilon S_q(\Sigma)$. Consider the relation $R \subseteq X_{k\tau} \times X_q$ defined by $(x_{k\tau}, x_q) \in R$ if and only if $\|H_{k\tau}(x_{k\tau}) - H_q(x_q)\| = \|x_{k\tau} - x_q\| \leq \varepsilon$. Since $X_{k\tau} \subseteq \bigcup_{p \in [\mathbb{R}^n]_\eta} \mathcal{B}_{\eta/2}(p)$ and by (6), for every $x_{k\tau} \in X_{k\tau}$ there always exists $x_q \in X_q$ such that:

$$\|x_{k\tau} - x_q\| \leq \eta/2 \leq \varepsilon. \quad (7)$$

Hence, $(x_{k\tau}, x_q) \in R$ and condition (i) in Definition 4 is satisfied. Now consider any $(x_{k\tau}, x_q) \in R$. Condition (ii) in Definition 4 is satisfied by the definition of R . Let us now show that condition (iii) in Definition 4 holds.

Consider any $v_{k\tau} \in U_{k\tau}$ of duration $k\tau$. Choose an input $u_q \in U_q$ satisfying:

$$\|v_{k\tau}|_{[(l-1)\tau, l\tau]} - u_q|_{[(l-1)\tau, l\tau]}\|_\infty = \|v_{k\tau}((l-1)\tau) - u_q((l-1)\tau)\| \leq \mu, \quad (8)$$

for any $l = 1, \dots, k$. Note that the existence of such u_q is guaranteed by the special shape of $\mathbf{U}$, described in Definition 1, and by the inequality $\mu \leq \text{span}(\mathbf{U})$ which guarantees that $\mathbf{U} \subseteq \bigcup_{p \in [\mathbf{U}]_\mu} \mathcal{B}_\mu(p)$. Now, we have:

$$\|v_{k\tau} - u_q\|_\infty = \max_{l=1, \dots, k} \left\| v_{k\tau}|_{[(l-1)\tau, l\tau]} - u_q|_{[(l-1)\tau, l\tau]} \right\|_\infty \leq \mu. \quad (9)$$

Consider the unique transition $x_{k\tau} \xrightarrow{v_{k\tau}}_{k\tau} x'_{k\tau} = \xi_{x_{k\tau} v_{k\tau}}(k\tau)$ in $S_{k\tau}(\Sigma)$. It follows from the δ -ISS assumption on Σ and (9) that the distance between $x'_{k\tau}$ and $\xi_{x_q u_q}(k\tau)$ is bounded as:

$$\|x'_{k\tau} - \xi_{x_q u_q}(k\tau)\| \leq \beta(\|x_{k\tau} - x_q\|, k\tau) + \gamma(\|v_{k\tau} - u_q\|_\infty) \leq \beta(\varepsilon, k\tau) + \gamma(\mu). \quad (10)$$

Since $X_{k\tau} \subseteq \bigcup_{p \in [\mathbb{R}^n]_\eta} \mathcal{B}_{\eta/2}(p)$, there exists $x'_q \in X_q$ such that:

$$\|\xi_{x_q u_q}(k\tau) - x'_q\| \leq \eta/2, \quad (11)$$

which, by the definition of $S_q(\Sigma)$, implies the existence of $x_q \xrightarrow{u_q}_{\mathbf{q}} x'_q$ in $S_q(\Sigma)$. Using the inequalities (6), (10), (11), and triangle inequality, we obtain:

$$\begin{aligned} \|x'_{k\tau} - x'_q\| &\leq \|x'_{k\tau} - \xi_{x_q u_q}(k\tau) + \xi_{x_q u_q}(k\tau) - x'_q\| \\ &\leq \|x'_{k\tau} - \xi_{x_q u_q}(k\tau)\| + \|\xi_{x_q u_q}(k\tau) - x'_q\| \\ &\leq \beta(\varepsilon, k\tau) + \gamma(\mu) + \eta/2 \leq \varepsilon. \end{aligned}$$

Therefore, we conclude $(x'_{k\tau}, x'_q) \in R$ and condition (iii) in Definition 4 holds.

Now we prove $S_q(\Sigma) \preceq^\varepsilon S_{k\tau}(\Sigma)$ implying that R^{-1} is a suitable ε -approximate simulation relation. Consider the relation $R \subseteq X_{k\tau} \times X_q$, defined in the first part of the proof. For every $x_q \in X_q$, by choosing $x_{k\tau} = x_q$, we have $(x_{k\tau}, x_q) \in R$ and condition (i) in Definition 4 is satisfied. Now consider any $(x_{k\tau}, x_q) \in R$. Condition (ii) in Definition 4 is satisfied by the definition of R . Let us now show that condition (iii) in Definition 4 holds. Consider any $u_q \in U_q$. Choose the input $v_{k\tau} = u_q$ and consider the unique $x'_{k\tau} = \xi_{x_{k\tau} v_{k\tau}}(k\tau)$ in $S_{k\tau}(\Sigma)$. Using δ -ISS assumption for Σ , we bound the distance between $x'_{k\tau}$ and $\xi_{x_q u_q}(k\tau)$ as:

$$\|x'_{k\tau} - \xi_{x_q u_q}(k\tau)\| \leq \beta(\|x_{k\tau} - x_q\|, k\tau) \leq \beta(\varepsilon, k\tau). \quad (12)$$

Using the definition of $S_q(\Sigma)$, the inequalities (6), (12), and the triangle inequality, we obtain:

$$\begin{aligned} \|x'_{k\tau} - x'_q\| &\leq \|x'_{k\tau} - \xi_{x_q u_q}(k\tau) + \xi_{x_q u_q}(k\tau) - x'_q\| \\ &\leq \|x'_{k\tau} - \xi_{x_q u_q}(k\tau)\| + \|\xi_{x_q u_q}(k\tau) - x'_q\| \\ &\leq \beta(\varepsilon, k\tau) + \eta/2 \leq \varepsilon. \end{aligned}$$

Therefore, we conclude that $(x'_{k\tau}, x'_q) \in R$ and condition (iii) in Definition 4 holds. $\square$

Remark 2. Although we assume the set $\mathbf{U}$ is infinite, Theorem 1 still holds when the set $\mathbf{U}$ is finite, with the following modifications. First, the system Σ is required to satisfy the property (2) for $v = v'$. Second, take $U_q = \prod_{i=1}^k \mathbf{U}$ in the definition of $S_q(\Sigma)$. Finally, in the condition (6), set $\mu = 0$.

A concern that arises when using $S_q(\Sigma)$ is the inter-samples behavior: can a specification be violated for $t \in]0, k\tau[$ even though it is satisfied at $t = 0$ and $t = k\tau$? This concern arises already in existing approaches to compute discrete abstractions [17,18,10] (setting $k = 1$).

In the absence of any bounds on inter-samples behaviors, the results of controller synthesis on $S_q(\Sigma)$ can be interpreted in the following way. If there is no controller satisfying a safety or co-Büchi specification on $S_q(\Sigma)$, respectively, then we can conclude that there is no controller satisfying the same safety or

co-Büchi specification on Σ , respectively. Dually, if there is a controller satisfying a reachability or Büchi specification on $S_q(\Sigma)$, respectively, then we can conclude that the refinement of that controller satisfies the same reachability or Büchi specification on Σ , respectively.

In practice, the parameter τ is chosen to be sufficiently small, and if $k \in \mathbb{N}$ is also small, the specification is directly verified against $S_q(\Sigma)$ ignoring inter-samples behaviors. If it is important to include the effects of inter-samples behaviors, e.g., when τ or k are large, there is a naive way to solve the inter-samples behaviors, especially in terms of synthesizing a controller. In the process of constructing abstract transition system $S_q(\Sigma)$, every transition can be labeled not only with the input but also with the sequence of the states visited at times $\tau, 2\tau, \dots, (k-1)\tau$. Now, one can find a symbolic controller for the constructed abstract transition system with the knowledge of what is happening in the inter-samples. By doing this, we shrink the inter-samples behaviors in only one sample time $]0, \tau[$.

Furthermore, one can over-approximate the reachable states between two sample points using techniques incorporating zonotopes [7,20] or support functions [11,6]. We illustrate the bounding technique using zonotopes. A transition $x_q \xrightarrow{u_q} x'_q$ in $S_q(\Sigma)$ implies the existence of a trajectory $\xi_{x_q u_q}$ of Σ satisfying $\|\xi_{x_q u_q}(k\tau) - x'_q\| \leq \eta/2$. We can thus enclose x_q in a zonotope Z_1 , enclose $\mathcal{B}_{\eta/2}(x'_q)$ in a different zonotope Z_2 , and use results in [7] (see also Proposition 7.31 in [20]) for a given $u_q \in U_q$ to obtain another zonotope $Z_{k\tau}(x_q, u_q, x'_q)$ containing all the states $\xi_{x_q u_q}(t)$ for $t \in [0, k\tau]$.

Fix an ε and $\mathbf{q}$ such that $S_q(\Sigma) \cong^\varepsilon S_{k\tau}(\Sigma)$. Let Z be the smallest zonotope enclosing Z_1 and Z_2 . Let $\varepsilon_0(x_q, u_q, x'_q)$ be an upper bound on the Hausdorff distance between Z and $Z_{k\tau}(x_q, u_q, x'_q)$, and let ε_0 be the supremum over all choices of $x_q \xrightarrow{u_q} x'_q$. Then, if $S_q(\Sigma) \cong^{\varepsilon - \varepsilon_0} S_{k\tau}(\Sigma)$, then we know that any trajectory of $S_q(\Sigma)$ is at most ε away from a trajectory of $S(\Sigma)$. If $\varepsilon_0 > \varepsilon$, then one needs to reduce the original precision ε and compute a new $\mathbf{q}$, and iterate. This represents the tradeoff between choosing larger k 's and bounding the deviations of inter-samples behaviors: choosing a larger k makes satisfying (6) easier, but can make ε_0 larger.

Remark 3. For linear control systems and safety (or co-Büchi) specifications, we can compute bounds on inter-samples behaviors in the following way. Assume $W \in \mathbb{R}^n$ is a compact and convex polyhedron with h vertices $x^1, \dots, x^h$. Assume Σ is a globally asymptotically stable linear control system, defined in (3), with a compact input set U and $S_q(\Sigma)$ is its symbolic abstraction. Assume there exists a symbolic controller on $S_q(\Sigma)$ satisfying¹ $\Box W$. What can we say about the existence of a controller on $S(\Sigma)$? It can be readily verified that there exists a controller satisfying $\Box \widehat{W}$ on $S(\Sigma)$, where $\widehat{W}$ is the polyhedron with vertices $\widehat{x}^1, \dots, \widehat{x}^k$, defined by:

$$\widehat{x}^i = e^{A l^* \tau} x^i + A^{-1} (e^{A \tau} - I_n) \left[e^{A(l^*-1)\tau} B u_1^* + \dots + e^{A \tau} B u_{l^*-1}^* + B u_{l^*}^* \right], \quad (13)$$

¹ Note that the semantics of LTL would be defined over the output behaviors of $S_q(\Sigma)$.

where l^* and u^* are computed by:

$$(l^*, u_1^*, \dots, u_{l^*}^*) = \arg \max_{l=1, \dots, k-1} \min_{u_1, \dots, u_l \in \mathcal{U}} \|\tilde{x}^i\|_W, \quad (14)$$

where the symbol $\|\cdot\|_W$ denotes the point-to-set distance, *viz.* $\|x\|_W = \min_{w \in W} \|x - w\|$, and

$$\tilde{x}^i = e^{A\tau} x^i + A^{-1} (e^{A\tau} - I_n) \left[e^{A(l-1)\tau} B u_1 + \dots + e^{A\tau} B u_{l-1} + B u_l \right]. \quad (15)$$

If $\widehat{W} \subseteq W$, then no new states are introduced through inter-samples behaviors. A similar analysis can be performed for co-Büchi objectives.

3.2 Comparison with Previous Techniques

We now compare our result (Theorem 1) with existing results on computing ε -approximate bisimilar discrete abstractions for δ -ISS digital control systems.

The construction in Pola, Girard, and Tabuada [17] essentially fixes $k = 1$. That is, it computes the metric system $S(\Sigma)$ and shows that $S_q(\Sigma)$ is ε -approximate bisimilar to it if $\mu \leq \text{span}(\mathcal{U})$ and $\beta(\varepsilon, \tau) + \gamma(\mu) + \eta/2 \leq \varepsilon$. This inequality may not hold for a choice of τ and in that case, the technique fails to construct an ε -approximate bisimilar abstraction. In contrast, we are guaranteed that for every given ε and τ , we can choose parameters η , μ , and k such that $S_q(\Sigma)$ is ε -approximate bisimilar to $S_{k\tau}(\Sigma)$.

Next, we compare with the construction in Girard, Pola, and Tabuada [10]. First, we need the notion of δ -ISS Lyapunov functions.

Definition 5. [3] Fix a control system Σ . A smooth function $V : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}_0^+$ is called a δ -ISS Lyapunov function for Σ if there exist $\mathcal{K}_\infty$ functions $\underline{\alpha}$, $\overline{\alpha}$, and σ , and a positive real $\kappa \in \mathbb{R}^+$ such that:

- (i) for any $x, x' \in \mathbb{R}^n$, $\underline{\alpha}(\|x - x'\|) \leq V(x, x') \leq \overline{\alpha}(\|x - x'\|)$;
- (ii) for any $x, x' \in \mathbb{R}^n$ and for any $u, u' \in \mathcal{U}$,

$$\frac{\partial V}{\partial x} f(x, u) + \frac{\partial V}{\partial x'} f(x', u') \leq -\kappa V(x, x') + \sigma(\|u - u'\|).$$

The following result characterizes δ -ISS in terms of δ -ISS Lyapunov functions.

Theorem 2. [3] Consider the digital control system $\Sigma = (\mathbb{R}^n, \tau, \mathcal{U}, \mathcal{U}_\tau, f)$. If $\mathcal{U}$ is convex, compact, contains the origin, and $f(0, 0) = 0$, then Σ is δ -ISS iff it admits a δ -ISS Lyapunov function.

The results in [10] additionally assume:

$$|V(x, y) - V(x, z)| \leq \widehat{\gamma}(\|y - z\|), \quad (16)$$

for any $x, y, z \in \mathbb{R}^n$, and some $\mathcal{K}_\infty$ function $\widehat{\gamma}$. As explained in [10], this assumption is not restrictive provided V is smooth and we are interested in the dynamics of Σ on a compact subset of $\mathbb{R}^n$, which is often the case in practice. The main result of [10] is as follows.

Table 1. Parameters of $S_q(\Sigma)$ and overall required time for constructing $S_q(\Sigma)$ and synthesizing controllers. The notation N/A means not applicable. We use the notation ∞ to indicate that the size of $S_q(\Sigma)$ is too large for **Pessoa** to finish constructing the abstraction.

Control Systems	τ	ε	Parameters of $S_q(\Sigma)$ $\mu=0.5$			Time		
			[17] η	[10] η	Our approach (η, k)	[17]	[10]	Our approach
DC motor	0.02	1	N/A	0.012	(0.5, 2)	N/A	∞	1.42s
Robot	0.002	0.075	0.0027	0.0022	(0.01, 4)	∞	∞	45.29s
Pendulum	0.02	0.25	N/A	0.0007	(0.1, 2)	N/A	∞	33s

Theorem 3. [10] Let Σ be a δ -ISS digital control system admitting a δ -ISS Lyapunov function V . For any $\varepsilon \in \mathbb{R}^+$ and parameters $\mathbf{q} = (\eta, \mu, 1)$, we have $S_q(\Sigma) \cong^\varepsilon S(\Sigma)$ if $\mu \leq \text{span}(\mathbf{U})$ and

$$\eta/2 \leq \min \left\{ \hat{\gamma}^{-1} \left((1 - e^{-\kappa\tau}) \underline{\alpha}(\varepsilon) - \frac{1}{\kappa} \sigma(\mu) \right), \bar{\alpha}^{-1}(\underline{\alpha}(\varepsilon)) \right\}, \quad (17)$$

For a given sampling time $\tau \in \mathbb{R}^+$, there always exist $\eta, \mu \in \mathbb{R}^+$ satisfying the condition (17). However, it can be readily verified that if the sampling time τ is very small, the right hand side of the inequality (17) is very small as well. Therefore, the upper bound on η will be very small, resulting in a large symbolic abstraction. On the other hand, we can always choose $k \in \mathbb{N}$ in (6) appropriately, to control the size of the symbolic model, justifying advantage of our proposed approach in comparison with the approach in [10]. In the next section, we demonstrate experimentally that our approach can result in discrete abstractions with orders of magnitude fewer states than the abstractions using Theorem 3.

4 Examples

We now experimentally demonstrate the effectiveness of our new construction. In the examples below, the computation of the abstractions $S_q(\Sigma)$ was performed using the tool **Pessoa** [16] on a laptop with CPU Intel Core 2 Duo @ 2.4GHz. We assume that control inputs are piecewise constant of duration τ and that $\mathcal{U}_\tau$ is finite and contains curves taking values in $[\mathbf{U}]_{0.5}$. Hence, as explained in Remark 2, $\mu = 0$ in the conditions (6) and (17). In the examples below, all constants and variables use SI units. Controllers enforcing the specifications were found by using standard algorithms from game theory, see e.g. [14,20], as implemented in **Pessoa**. Table 1 summarizes the experimental results.

Fig. 1. Upper and central panels: evolution of ξ_1 and ξ_2 with initial condition $(0, 0)$. Lower panel: input signal.

4.1 DC Motor

Model: Consider a linear DC motor (from [1]) described by:

$$\Sigma : \begin{cases} \dot{\xi}_1 = -\frac{b}{J}\xi_1 + \frac{K}{J}\xi_2, \\ \dot{\xi}_2 = -\frac{K}{L}\xi_1 - \frac{R}{L}\xi_2 + \frac{1}{L}v, \end{cases} \quad (18)$$

where ξ_1 is the angular velocity of the motor, ξ_2 is the current through the inductor, v is the source voltage, $b = 10^{-4}$ is the damping ratio of the mechanical system, $J = 10^{-4}$ is the moment of inertia of the rotor, $K = 5 \times 10^{-2}$ is the electromotive force constant, $L = 2 \times 10^{-3}$ is the electric inductance, and $R = 1$ is the electric resistance. Using Remark 1, it is readily seen that Σ is δ -ISS.

Abstraction: We assume that $U = [-1, 1]$. We work on the subset $D = [-10, 10] \times [-10, 10]$ of the state space of Σ . For a sampling time $\tau = 0.02$, the function β in (4) is given by $\beta(\varepsilon, \tau) = 1.26\varepsilon$. Hence, the results in [17] cannot be applied because the condition (6) of Theorem 1 cannot be fulfilled when $k = 1$. On the other hand, by choosing $k = 2$, we have $\beta(\varepsilon, k\tau) = 0.73\varepsilon$ implying that the condition (6) of Theorem 1 can be fulfilled. For a precision $\varepsilon = 1$, we construct a symbolic model $S_q(\Sigma)$. The parameters of $S_q(\Sigma)$ based on the results in this paper as well as the construction in [10] are given in Table 1. The proposed state space quantization parameter in [10] is roughly 42 times smaller than our quantization parameter. Since Σ is a 2 dimensional system, the size of our abstraction is 42^2 times smaller than the one in [10].

Example control problem: Consider the objective to design a controller forcing the trajectories of Σ to reach and stay within $W = [9, 10] \times [-1, 1]$ thereafter while always remaining within $Z = [-10, 10] \times [-1, 1]$, that is, the LTL specification $\Diamond \Box W \wedge \Box Z$. Using the result in Remark 3, we compute $\widehat{Z}$ and $\widehat{W}$ and note that in this case, $\widehat{Z} \subseteq Z$ and $\widehat{W} \subseteq W$. Hence, the existence of a symbolic controller on $S_q(\Sigma)$ satisfying $\Diamond \Box W \wedge \Box Z$ implies the existence of a controller satisfying $\Diamond \Box W \wedge \Box Z$ on Σ . In Figure 1, we show the closed-loop trajectory stemming from the initial condition $(0, 0)$ as well as the evolution of the input signal. It

Fig. 2. Evolution of the robot and the input signals with initial condition $(0.9, 0.9)$

is readily seen that the specifications are satisfied in the sense that trajectories of Σ reach and stay within $W^\varepsilon = [9 - \varepsilon, 10] \times [-1 - \varepsilon, 1 + \varepsilon]$ thereafter while always remaining within $Z^\varepsilon = [-10, 10] \times [-1 - \varepsilon, 1 + \varepsilon]$.

4.2 Motion Planing

Model: Consider a linear model of a robot described by:

$$\Sigma : \begin{cases} \dot{\xi}_1 = -10\xi_1 - \xi_2 + 10v_1, \\ \dot{\xi}_2 = -\xi_1 - 10\xi_2 + 10v_2. \end{cases} \quad (19)$$

The position of the robot is given by the pair (ξ_1, ξ_2) . The pair (v_1, v_2) are the control inputs, expressing the velocity of the wheels. Using Remark 1, it is readily seen that Σ is δ -ISS.

Abstraction: We assume that $(v_1, v_2) \in \mathcal{U} = [-1, 1] \times [-1, 1]$. We work on the subset $D = [-1, 1] \times [-1, 1]$ of the state space of Σ . For a sampling time $\tau = 0.002$, the function β in (4) is given by $\beta(\varepsilon, \tau) = 0.982\varepsilon$. Hence, the results in [17] can be applied. On the other hand, by choosing $k = 4$, we have $\beta(\varepsilon, k\tau) = 0.93\varepsilon$ implying that the condition (6) of Theorem 1 can also be fulfilled. For a

Fig. 3. Finite system describing the schedulability constraints. The lower part of the states are labeled with the outputs **a** and **u** denoting availability and unavailability of the microprocessor, respectively.

precision $\varepsilon = 0.075$, we construct a symbolic model $S_q(\Sigma)$. The parameters of $S_q(\Sigma)$ based on the results in this paper and those from [17,10] are given in Table 1. The state space quantization parameters in [17,10] are roughly four times smaller than our η . Therefore, the size of our abstraction is roughly 4^2 times smaller than the ones in [17,10].

Example control problem: Consider the problem of designing a controller navigating the robot to reach the target set $W = [-1, -0.9] \times [-0.1, 0.1]$, indicated with a target box in the far left hand side in Figure 2, while avoiding the obstacles, indicated as rectangular boxes in Figure 2, and then remain indefinitely inside W . If we denote by ϕ and ψ the predicates representing the target and obstacles, respectively, this specification can also be expressed by the LTL formula $\Diamond\Box\phi \wedge \Box\neg\psi$. If we express the non-obstacle area in Figure 2 as the union of l polyhedra Z_i , for $i = 1, \dots, l$, then using the result in Remark 3, we compute $\widehat{Z}_i$ and $\widehat{W}$, and note that for this example, $\widehat{Z}_i \subseteq Z_i$, for each $i = 1, \dots, l$, and $\widehat{W} \subseteq W$. Hence, a symbolic controller on $S_q(\Sigma)$ satisfying $\Diamond\Box\phi \wedge \Box\neg\psi$ implies there exists a controller satisfying the specification on Σ . In Figure 2, we show the closed-loop trajectory stemming from the initial condition $(0.9, 0.9)$ and the evolution of the input signals. It is readily seen that the specification is satisfied.

4.3 Pendulum with Resource Constraints

Model: Consider a nonlinear model of a pendulum on a cart (from [17]) described by:

$$\Sigma : \begin{cases} \dot{\xi}_1 = \xi_2, \\ \dot{\xi}_2 = -\frac{g}{l} \sin(\xi_1) - \frac{h}{m} \xi_2 + v, \end{cases} \quad (20)$$

where ξ_1 and ξ_2 are the angular position and velocity of the point mass, v is the torque applied to the cart, $g = 9.8$ is acceleration due to gravity, $l = 5$ is the length of the rod, $m = 0.5$ is the mass, and $h = 3$ is the coefficient of friction. As shown in [17], Σ is δ -ISS.

Abstraction: We assume that $U = [-1.5, 1.5]$. We work on the subset $D = [-1, 1] \times [-1, 1]$ of the state space of Σ . As shown in [17], the function β in (2) is given by $\beta(\varepsilon, \tau) = 6.17e^{-2.08\tau}\varepsilon$, so for a sampling time $\tau = 0.5$, we have $\beta(\varepsilon, \tau) = 2.18\varepsilon$. Hence, the results in [17] cannot be applied because the condition (6) of Theorem 1 cannot be fulfilled when $k = 1$. On the other hand,

Fig. 4. Upper and central panels: evolution of ξ_1 and ξ_2 with initial condition $(-0.9, -1)$. Lower panel: input signal.

by choosing $k = 2$, we have $\beta(\varepsilon, k\tau) = 0.77\varepsilon$, so the condition (6) of Theorem 1 is fulfilled. For a precision $\varepsilon = 0.25$, we construct a symbolic model $S_q(\Sigma)$. The parameters of $S_q(\Sigma)$ based on the results in this paper and [10] are given in Table 1. The state space quantization parameter in [10] is roughly 147 times smaller than our quantization parameter. Therefore, the size of the symbolic model computed by our algorithm is roughly $147^2 \sim 2 \times 10^4$ times smaller than the one in [10].

Example control problem: Suppose our objective is to design a controller forcing the trajectories of the system to reach the target set $W = [-0.7, -0.6] \times [-1, 1]$ and to remain indefinitely inside W . Furthermore, to add a discrete component to the problem, we assume that the controller is implemented on a microprocessor, executing other tasks in addition to the control task. We consider a schedule with epochs of four time slots in which the first two slots are allocated to the control task and the rest of them to other tasks. The expression time slot refer to a time interval of the form $[k'\tau, (k' + 1)\tau[$ with $k' \in \mathbb{N}$ and where τ is the sampling time. Therefore, the microprocessor schedule is given by:

$$|aauu|aauu|aauu|aauu|aauu|aauu|aauu|\dots,$$

where **a** denotes a slot available for the control task and **u** denotes a slot allotted to other tasks. The symbol **|** separates each epoch of four time slots. The schedulability constraint on the microprocessor can be represented by the finite system in Figure 3. Initial states of the finite system are distinguished by being the target of a sourceless arrow. In Figure 4, we show the closed-loop trajectory stemming from the initial condition $(-0.9, -1)$, and the evolution of the input signal, where the finite system initialized from state q_3 .

References

1. Control tutorial for Matlab and Simulink. Electronically available at, <http://www.library.cmu.edu/ctms/ctms/>

2. Alur, R., Dill, D.L.: A theory of timed automata. *Theoretical Computer Science* 126, 183–235 (1994)
3. Angeli, D.: A Lyapunov approach to incremental stability properties. *IEEE Transactions on Automatic Control* 47(3), 410–421 (2002)
4. Angeli, D., Sontag, E.D.: Forward completeness, unboundedness observability, and their Lyapunov characterizations. *Systems and Control Letters* 38, 209–217 (1999)
5. Emerson, E.A., Jutla, C.S.: Tree automata, mu-calculus and determinacy. In: *FOCS 1991: Foundations of Computer Science*, pp. 368–377. IEEE (1991)
6. Frehse, G., Le Guernic, C., Donzé, A., Cotton, S., Ray, R., Lebeltel, O., Ripado, R., Girard, A., Dang, T., Maler, O.: SpaceEx: Scalable Verification of Hybrid Systems. In: Gopalakrishnan, G., Qadeer, S. (eds.) *CAV 2011. LNCS*, vol. 6806, pp. 379–395. Springer, Heidelberg (2011)
7. Girard, A.: Reachability of Uncertain Linear Systems Using Zonotopes. In: Morari, M., Thiele, L. (eds.) *HSCC 2005. LNCS*, vol. 3414, pp. 291–305. Springer, Heidelberg (2005)
8. Girard, A.: Approximately Bisimilar Finite Abstractions of Stable Linear Systems. In: Bemporad, A., Bicchi, A., Buttazzo, G. (eds.) *HSCC 2007. LNCS*, vol. 4416, pp. 231–244. Springer, Heidelberg (2007)
9. Girard, A., Pappas, G.J.: Approximation metrics for discrete and continuous systems. *IEEE Transactions on Automatic Control* 25(5), 782–798 (2007)
10. Girard, A., Pola, G., Tabuada, P.: Approximately bisimilar symbolic models for incrementally stable switched systems. *IEEE Transactions on Automatic Control* 55(1), 116–126 (2009)
11. Le Guernic, C., Girard, A.: Reachability analysis of linear systems using support functions. *Nonlinear Analysis: Hybrid Systems* 4(2), 250–262 (2010)
12. Henzinger, T.A.: Hybrid Automata with Finite Bisimulations. In: Fülöp, Z. (ed.) *ICALP 1995. LNCS*, vol. 944, pp. 324–335. Springer, Heidelberg (1995)
13. Kailath, T.: *Linear systems*. Prentice-Hall, Inc. (1980)
14. Maler, O., Pnueli, A., Sifakis, J.: On the Synthesis of Discrete Controllers for Timed Systems. In: Mayr, E.W., Puech, C. (eds.) *STACS 1995. LNCS*, vol. 900, pp. 229–242. Springer, Heidelberg (1995)
15. Milner, R.: *Communication and Concurrency*. Prentice-Hall, Inc. (1989)
16. Pessoa (2009), <http://www.cyphylab.ee.ucla.edu/pessoa>
17. Pola, G., Girard, A., Tabuada, P.: Approximately bisimilar symbolic models for nonlinear control systems. *Automatica* 44(10), 2508–2516 (2008)
18. Pola, G., Tabuada, P.: Symbolic models for nonlinear control systems: alternating approximate bisimulations. *SIAM Journal on Control and Optimization* 48(2), 719–733 (2009)
19. Sontag, E.D.: *Mathematical control theory*, 2nd edn. Springer (1998)
20. Tabuada, P.: *Verification and Control of Hybrid Systems, A symbolic approach*. Springer, US (2009)
21. Teel, A.R., Nesic, D., Kokotovic, P.V.: A note on input-to-state stability of sampled-data nonlinear systems. In: *CDC 1998: Conference on Decision and Control*, pp. 2473–2478. IEEE (1998)
22. Thomas, W.: On the Synthesis of Strategies in Infinite Games. In: Mayr, E.W., Puech, C. (eds.) *STACS 1995. LNCS*, vol. 900, pp. 1–13. Springer, Heidelberg (1995)
23. Zamani, M., Tabuada, P.: Backstepping design for incremental stability. *IEEE Transaction on Automatic Control* 56(9), 2184–2189 (2011)