# AN APPROXIMATE SIMULATION APPROACH TO SYMBOLIC CONTROL

PAULO TABUADA

Abstract. This paper introduces a methodology for the symbolic control of nonlinear systems based on an approximate notion of simulation relation. This notion generalizes existing exact simulation relations and is completely characterized in terms of known stabilizability concepts. Equipped with this notion we show how, under certain stabilizability assumptions, we can construct finite or symbolic models for nonlinear control systems. Synthesizing controllers for the original control system can then be done on the finite models, by using supervisory control techniques, and the resulting finite controllers can be refined to hybrid controllers enforcing the specification on the continuous control system. The proposed design methodology can be seen as a correct by design way of obtaining both the feedback control laws as well as the control software responsible for deciding which law is executed and when.



## 1. Introduction

Hybrid systems have been introduced more than 10 years ago [GNRR93] ago in order to describe systems possessing both discrete and continuous behavior. This mixed dynamical nature still poses many challenges today since most continuous or discrete analysis and synthesis techniques fail to generalize to the hybrid case. One possible justification for the unequivocally difficult analysis and design of hybrid systems is provided by the large diversity of systems that can be described as hybrid. This observation motivates us to focus on particular classes of hybrid systems, and in this paper, on the class characterized by having an underlying continuous control system over which control software creates hybrid dynamics by switching among different control strategies. Current practice in the design of these systems still relies on carefully engineered ad-hoc methods to generate the control software. The resulting hybrid system is then verified by resorting to extensive simulation or, for simpler continuous dynamics, by resorting to formal verification. We advocate a different approach in which the software is synthesized using *correct by design* methods. Instead of emphasizing the verification of already designed systems as is done today, we regard the synthesis of software as a control problem to be solved in conjunction with the synthesis of feedback control laws. Since the resulting design is guaranteed to enforce the specification by construction, the need for verification can be substantially reduced.

In this paper we present a concrete methodology for the synthesis of correct by design control software through the use of approximate simulations and symbolic control. The main idea consists in constructing a *symbolic or finite abstraction* of the continuous control system in the form of a finite transition system. Synthesis of control software is then regarded as the synthesis of a supervisor acting on the finite abstraction. Provided that this abstraction is correctly constructed, we can refine the discrete supervisor into a hybrid controller that will enforce the desired behavior on the original continuous control system. The heart of the approach lies on the construction of the finite abstraction which is the central theme of this paper although the remaining design steps will also be briefly discussed.

At the technical level, we introduce a notion of approximate simulation relation generalizing existing notions of (exact) simulation relations. We show that such notion can be described in terms of existing stabilizability concepts from which we immediately obtain a characterization in terms of Lyapunov functions. We also show how approximate simulation relations are an essential ingredient in the above outlined correct by design approach to the synthesis of control software. We then focus on the construction of finite abstractions by adopting a quantized input approach (we compare our results with the existing literature on quantized control

This research was partially supported by the National Science Foundation CAREER award 0446716.

systems below). Although the reachable space of a quantized control system fails to be a lattice, in general, we show that we can always construct an abstraction of a control system, having a lattice for state space, under a certain stabilizability assumption. It then follows trivially, by working on a compact subset of the state space, that the resulting abstraction is finite.

The results presented in this paper were strongly inspired by three different lines of work:

**Quantized control systems -** The construction of the finite abstraction proposed in this paper is done in the setting of quantized control systems [BMP02, PLPB02, BMP06]. We assume that a certain finite subset of the inputs is given and we consider only piece-wise constant input trajectories assuming values on this set. As argued in the quantized control systems literature, this reduction of inputs results in a simplification of several control design problems. This is even more apparent for quantized control systems whose reachable set has the structure of a lattice. Our contribution consists in showing that even if the reachable set fails to have a lattice structure, such structure can be imposed provided that: the resulting model is related to the original (unquantized) control system not by a simulation relation but by an approximate simulation relation; a certain stabilizability assumption holds. Moreover, this lattice structure is independent of the chosen input quantization which makes our results useful even if the quantized control system admits a lattice structure on the reachable set *for some but not for all* input quantizations. In this paper, however, this lattice structure is only exploited to obtain a finite abstraction of the original control system whereas in the quantized control literature it has been used to obtain efficient motion planning algorithms [PLPB02].

**Approximate bisimulations between control systems -** The results in this paper, and in particular the proposed notion of approximate simulation relation, are quite close to recent results on approximate equivalence of control systems introduced by Girard and Pappas in [GP05b]. In both cases the approximate notion of simulation[1] is obtained from the existing exact one by relaxing equality between observations to boundedness with respect to a certain metric. The notion introduced in this paper can be seen as a strengthening of the notion introduced in [GP05b]. This strengthening is justified by the conceptual enlightenment it brings: approximate simulations are completely characterized in terms of existing stabilizability notions. This result immediately provides Lyapunov characterizations of approximate simulations and clarifies the relationship between bisimulation functions, introduced in [GP05b], and standard Lyapunov functions. Despite the similarity between the concepts, they are used in very different ways. In [GP05b], approximate simulations provide relations between continuous systems while in this paper we relate continuous with symbolic or finite systems.

**Finite abstractions of control systems -** This paper extends previous results by the author presented in [Tab06a] for linear control systems. When linearity reigns, the stabilizability assumptions made in this paper reduce to stabilizability and asymptotic stabilizability of the origin: the working assumptions in [Tab06a]. The construction of finite abstractions possessing lattices as state spaces is, however, new. The results in this paper complement previous work on finite abstractions of control systems [TP06, Tab06b] which focused on discrete-time systems.

This paper can also be seen as an offspring of the folk view of hybrid systems in which a discrete supervisor emits symbols to be interpreted as control specifications enforced by continuous controllers acting on the physical plant. Different interpretations of this view include [KPS01, MRO02, FDF05] among many other references. Some recent work along these lines is reported on the special issue [EFP06].

Finally, we would like to mention that the relevance of the proposed results is substantiated by several examples, presented in Section 7, of control designs leading to hybrid controllers for the unicycle, one of the simplest and yet nontrivial nonlinear control systems.



[1]The authors of [GP05b] only discuss approximate bisimulations but one can easily derive the corresponding notion of approximate simulation.

## 2. Definitions, control systems and stability notions

2.1. **Definitions.** The following definitions and notations will be used throughout the paper. Given a map $f : A \to B$ we denote by $\Gamma(f)$ the graph of $f$, that is, the set $\Gamma(f) = \big\{(a, b) \in A \times B \mid b = f(a)\big\}$. If $A$ is a subset of $B$ we denote by $\imath_A : A \hookrightarrow B$ or simply by $\imath$ the natural inclusion map taking any $a \in A$ to $\imath(a) = a \in B$. The identity map on a set $A$ is denoted by $1_A$. For $x \in \mathbb{R}^n$ we denote by $x_i$ the $i$th element of the vector $x$. Let now $A \subseteq \mathbb{R}^n$ and $\mu \in \mathbb{R}$. We will use the notation $[A]_\mu$ to denote the subset of $A$ defined by all the vectors whose elements are integer multiples of $\mu$ or equivalently $[A]_\mu = \big\{a \in A \mid a_i = k_i\mu \text{ for some } k_i \in \mathbb{Z} \text{ and } i = 1, \ldots, n\big\}$. The set $[A]_\mu$ is thus a subset of the lattice $[\mathbb{R}^n]_\mu$. When $x \in \mathbb{R}^n$, $\lceil x \rceil$ will denote the smallest integer $n \in \mathbb{N}$ such that $x \leq n$. We will say that $a \in \mathbb{R}$ integrally divides $b \in \mathbb{R}$ when $b/a \in \mathbb{Z}$. The standard Euclidean norm of $x \in \mathbb{R}^n$ is denoted by $\|x\|$ while $\|x\|_S$ denotes the usual point to set distance defined by:

$$\|x\|_S = \inf_{s \in S} \|x - s\|$$

We can thus recover $\|x\|$ as $\|x\|_{\{0\}}$. The closed ball centered at $x \in \mathbb{R}$ with radius $\varepsilon$ is denoted by $\mathcal{B}_\varepsilon(x)$ or equivalently:

$$\mathcal{B}_\varepsilon(x) = \big\{y \in \mathbb{R} \mid \|x - y\| \leq \varepsilon\big\}$$

A continuous function $\gamma : \mathbb{R}_0^+ \to \mathbb{R}_0^+$, is said to belong to class $\mathcal{K}_\infty$ if it is strictly increasing, $\gamma(0) = 0$ and $\gamma(r) \to \infty$ as $r \to \infty$. A continuous function $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$ 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 $r$, the map $\beta(r, s)$ is decreasing with respect to $s$ and $\beta(r, s) \to 0$ as $s \to \infty$.

We now review some formal language concepts. Given a set $S$ we denote by $S^*$ the set of all finite strings obtained by concatenating elements in $S$. An element $s$ of $S^*$ is therefore given by $s = s_1 s_2 \ldots s_n$ with $s_i \in S$ for $i = 1, \ldots, n$. Given a string $s$ belonging to $S^*$ we denote by $s(i)$ the $i$th element of $s$. The length of a string $s \in S^*$ is denoted by $|s|$ and a subset of $S^*$ is called a language. Given a map $f : A \to B$ we shall use the same letter to denote the extension of $f$ to $f : A^* \to B^*$ defined by:

$$f\big(s(1)s(2)\ldots s(n)\big) = f\big(s(1)\big)f\big(s(2)\big)\ldots f\big(s(n)\big)$$

2.2. **Control Systems.** One the main objects of study in this paper are control systems defined as follows:

**Definition 2.1.** A control system is a quadruple $\Sigma = (\mathbb{R}^n, U \subset \mathbb{R}^m, \mathcal{U}, f)$ where:

- $U$ is a compact subset of $\mathbb{R}^m$ containing the origin;
- $\mathcal{U}$ is a subset of the set of all measurable functions from intervals of the form $]a, b[ \subseteq \mathbb{R}$ to $U$ with $a < 0$ and $b > 0$;
- $f : \mathbb{R}^n \times U \to \mathbb{R}^n$ is a continuous map satisfying the following Lipschitz assumption: for every compact set $K \subset \mathbb{R}^n$, there exists a constant $L > 0$ such that $\|f(x, u) - f(y, u)\| \leq L\|x - y\|$ for all $x, y \in K$ and all $u \in U$.

A $C^1$ curve $\mathbf{x} : ]a, b[ \to \mathbb{R}^n$ is said to be a trajectory of $\Sigma$ if there exists $\mathbf{u} \in \mathcal{U}$ satisfying:

$$\dot{\mathbf{x}}(t) = f(\mathbf{x}(t), \mathbf{u}(t)) \tag{2.1}$$

for almost all $t \in ]a, b[$. Control system $\Sigma$ is said to be forward complete if every trajectory is defined on an interval of the form $]a, \infty[$.

Although we have defined trajectories over open domains, we shall refer to trajectories $\mathbf{x} : [0, \tau] \to \mathbb{R}^n$ defined on closed domains $[0, \tau]$, $\tau \in \mathbb{R}^+$ with the understanding of the existence of a trajectory $\mathbf{x}' : ]a, b[ \to \mathbb{R}^n$ such that $\mathbf{x} = \mathbf{x}'|_{[0,\tau]}$. We will also write $\mathbf{x}(\tau, x, \mathbf{u})$ to denote the point reached at time $\tau$ under the input $\mathbf{u}$ from initial condition $x$. This point is uniquely determined since the assumptions on $f$ ensure existence and uniqueness of trajectories. For certain results we will need to assume that $\Sigma$ is control affine meaning that

$f(x,u)$ can be written as:

$$f(x,u) = f_0(x) + \sum_{i=1}^{m} f_i(x)u_i$$

where the $f_i$ satisfy the same regularity conditions as $f$ and $(u_1,\ldots,u_m) \in U$.

2.3. **Stability notions.** The results presented in this paper will assume certain stabilizability assumptions that we now recall. We will say that a set $S \subseteq \mathbb{R}^n$ is invariant under a control system $\Sigma$ if for any trajectory $\mathbf{x}$ of $\Sigma$, $\mathbf{x}(0) \in S$ implies $\mathbf{x}(t) \in S$ for all $0 \leq t < b$. We will also need to refer to the diagonal set on $\mathbb{R}^{2n}$, denoted by $\Delta$, and defined by $\Delta = \big\{(x,y) \in \mathbb{R}^n \times \mathbb{R}^n \mid x = y\big\}$.

**Definition 2.2.** A control system $\Sigma = (\mathbb{R}^n, U \subset \mathbb{R}^m, \mathcal{U}, f)$ is uniformly globally stable with respect to a closed invariant set $S$ if it is forward complete and there exists a class $\mathcal{K}_\infty$ function $\gamma$ such that the following estimate holds for all $x \in \mathbb{R}^n$, $\mathbf{u} \in \mathcal{U}$ and $t \geq 0$:

$$\|\mathbf{x}(t,x,\mathbf{u})\|_S \leq \gamma(\|x\|_S) \tag{2.2}$$

**Definition 2.3.** A control system $\Sigma = (\mathbb{R}^n, U \subset \mathbb{R}^m, \mathcal{U}, f)$ is uniformly globally asymptotically stable with respect to a closed invariant set $S$ if it is forward complete and there exists a class $\mathcal{KL}$ function $\beta$ such that the following estimate holds for all $x \in \mathbb{R}^n$, $\mathbf{u} \in \mathcal{U}$ and $t \geq 0$:

$$\|\mathbf{x}(t,x,\mathbf{u})\|_S \leq \beta(\|x\|_S, t) \tag{2.3}$$

Uniform global asymptotical stability implies uniform global stability since from (2.3) we can recover (2.2) by defining $\gamma(\|x\|_S)$ as $\beta(\|x\|_S, 0)$ which is a $\mathcal{K}_\infty$ function.

**Definition 2.4** (Stabilizability Assumption I)**.** A control system $\Sigma = (\mathbb{R}^n, U \subset \mathbb{R}^m, \mathcal{U}, f)$ is said to satisfy Stabilizability Assumption I (SAI) if there exists a function $k : \mathbb{R}^n \times \mathbb{R}^n \times U \to U$ satisfying:

(1) $k$ is continuously differentiable on $\mathbb{R}^{2n}\backslash\Delta$;
(2) $k(y,x,u) = u$ for $(x,y) \in \Delta$,

and rendering control system $(\mathbb{R}^n \times \mathbb{R}^n, U \subset \mathbb{R}^m, \mathcal{U}, f \times_k f)$ with $f \times_k f$ defined by:

$$(f \times_k f)((x,y),u) = \big(f(x,u), f(y,k(y,x,u))\big) \tag{2.4}$$

uniformly globally stable with respect to $\Delta$, that is, enforcing the following estimate for all $x, y \in \mathbb{R}^n$, $\mathbf{u} \in \mathcal{U}$ and $t \geq 0$:

$$\|\mathbf{x}(t,x,\mathbf{u}) - \mathbf{y}(t,y,k(\mathbf{y},\mathbf{x},\mathbf{u}))\| \leq \gamma(\|x-y\|) \tag{2.5}$$

The possible lack of regularity of $k$ on $\Delta$ does not pose a problem with respect to existence and uniqueness of trajectories. On the open set $\mathbb{R}^{2n}\backslash\Delta$ existence and uniqueness of trajectories is guaranteed by the regularity assumptions on $k$ and $f$. On the set $\Delta$, the requirement $k(y,x,u) = u$ ensures that $\Delta$ is an invariant set since $f \times_k f$ degenerates into $(f(x,u), f(x,u))$ which guarantees existence and uniqueness of trajectories.

When a control system satisfies SAI the action of the controller $k$ ensures that trajectories starting from close initial conditions will remain close for all future time as expressed by (2.5). The next assumption strengthens this requirement with asymptotic convergence of trajectories.

**Definition 2.5** (Stabilizability Assumption II)**.** A control system $\Sigma = (\mathbb{R}^n, U \subset \mathbb{R}^m, \mathcal{U}, f)$ is said to satisfy Stabilizability Assumption II (SAII) if there exists a function $k : \mathbb{R}^n \times \mathbb{R}^n \times U \to U$ satisfying:

(1) $k$ is continuously differentiable on $\mathbb{R}^{2n}\backslash\Delta$;
(2) $k(y,x,u) = u$ for $(x,y) \in \Delta$,

and rendering control system $(\mathbb{R}^n \times \mathbb{R}^n, U \subset \mathbb{R}^m, \mathcal{U}, f \times_k f)$ with $f \times_k f$ defined by:

$$(f \times_k f)((x,y),u) = \big(f(x,u), f(y,k(y,x,u))\big) \tag{2.6}$$

uniformly globally asymptotically stable with respect to $\Delta$, that is, enforcing the following estimate for all $x, y \in \mathbb{R}^n$, $\mathbf{u} \in \mathcal{U}$ and $t \geq 0$:

$$\|\mathbf{x}(t,x,\mathbf{u}) - \mathbf{y}(t,y,k(\mathbf{y},\mathbf{x},\mathbf{u}))\| \leq \beta(\|x-y\|,t) \tag{2.7}$$

A control system satisfying SAII is able to track its own trajectories since for any trajectory $\mathbf{x}$ defined by an input curve $\mathbf{u}$, the feedback controller $k$ will guarantee that the trajectory $\mathbf{y}$ starting at any initial condition and defined by the input curve $k(\mathbf{y},\mathbf{x},\mathbf{u})$ will asymptotically converge to $\mathbf{x}$. Assumptions SAI and SAII describe a class of control systems for which an error in initial conditions can be compensated by feedback so that: it remains bounded in the case of SAI; and it converges to zero in the case of SAII.

In general, the inequalities (2.5) and (2.7) are difficult to check directly. Fortunately, these can be given dissipative characterizations in terms of Lyapunov functions:

**Proposition 2.6.** *A control system $\Sigma = (\mathbb{R}^n \times \mathbb{R}^n, U \subset \mathbb{R}^m, \mathcal{U}, f)$ satisfies SAI iff there exist a function $k : \mathbb{R}^n \times \mathbb{R}^n \times U \to U$ satisfying:*

1. *$k$ is continuously differentiable on $\mathbb{R}^{2n} \backslash \Delta$;*
2. *$k(y,x,u) = u$ for $(x,y) \in \Delta$,*
3. *$f \times_k f$ defined in (2.4) is forward complete,*

*a function $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_0^+$ and class $\mathcal{K}_\infty$ functions $\underline{\alpha}, \overline{\alpha}$ for which the following inequalities hold for all $x, y \in \mathbb{R}^n$ and $\mathbf{u} \in \mathcal{U}$:*

1. *$\underline{\alpha}(\|x-y\|) \leq V(x,y) \leq \overline{\alpha}(\|x-y\|)$;*
2. *$t_2 \geq t_1 \geq 0 \quad \Longrightarrow \quad V(\mathbf{x}(t_2,x,\mathbf{u}|_{[0,t_2]}), \mathbf{y}(t_2,y,\mathbf{u}|_{[0,t_2]})) \leq V(\mathbf{x}(t_1,x,\mathbf{u}|_{[0,t_1]}), \mathbf{y}(t_1,y,\mathbf{u}|_{[0,t_1]}))$.*

*and where $(\mathbf{x},\mathbf{y})$ is the solution of $f \times_k f$.*

*Proof.* Sufficiency is obvious. Regarding necessity, note that we are not requiring any regularity on $V$ and thus can define it as:

$$V(x,y) = \sup_{t \geq 0} \sup_{\mathbf{u} \in \mathcal{U}} \|\mathbf{x}(t,x,\mathbf{u}) - \mathbf{y}(t,y,k(\mathbf{y},\mathbf{x},\mathbf{u}))\|$$

From the SAI it follows that $V(x,y) \leq \gamma(\|x-y\|)$ and by taking $t = 0$ in the definition of $V$ we obtain $\|x-y\| \leq V(x,y)$. The first requirement on $V$ is thus satisfied with $\underline{\alpha}(r) = r$ and $\overline{\alpha}(r) = \gamma(r)$. The second requirement follows immediately from the definition of $V$ and the semi-group property of trajectories. □

It is well known that *continuous* Lyapunov functions mail fail to exist for uniformly globally stable differential equations [BR05]. This fact explains why condition (2) in the previous result cannot be improved to the more standard test $\dot{V} \leq 0$. However, this can be done for SAII since in this case $V$ is guaranteed to be differentiable:

**Proposition 2.7.** *A control system $\Sigma = (\mathbb{R}^n \times \mathbb{R}^n, U \subset \mathbb{R}^m, \mathcal{U}, f)$ satisfies SAII iff there exist a function $k : \mathbb{R}^n \times \mathbb{R}^n \times U \to U$ satisfying:*

1. *$k$ is continuously differentiable on $\mathbb{R}^{2n} \backslash \Delta$;*
2. *$k(y,x,u) = u$ for $(x,y) \in \Delta$,*
3. *$f \times_k f$ defined in (2.4) is forward complete,*

*a smooth function $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_0^+$ and class $\mathcal{K}_\infty$ functions $\underline{\alpha}, \overline{\alpha}, \alpha$ for which the following inequalities hold for all $x, y \in \mathbb{R}^n$ and $u \in U$:*

1. *$\underline{\alpha}(\|x-y\|) \leq V(x,y) \leq \overline{\alpha}(\|x-y\|)$;*

(2) $\frac{\partial V}{\partial x} f(x,u) + \frac{\partial V}{\partial y} f(y,k(y,x,u)) \leq -\alpha(\|x-y\|)$.

*Proof.* Note that $\Delta$ is a closed set which is also invariant since $k(y,x,u) = u$ for $(x,y) \in \Delta$. The result now follows from Theorem 2.8 in [LSW96]. □

For linear systems SAI is implied by stabilizability of the origin while SAII follows from asymptotic stabilizability of the origin. This was the context in which the results in [Tab06a] were presented since only the linear case was discussed.

One can go one step further, by using the concept of control Lyapunov function, and eliminate the need for the knowledge of $k$ in a characterization of SAI and SAII. Following the ideas initially presented in [Art83] and later extended by many authors, the existence of a control Lyapunov function allows one to recover the controller $k$. To simplify the presentation let us consider new coordinates given by:

$$z = x - y \qquad w = x + y \tag{2.8}$$

**Proposition 2.8.** *Let $\Sigma = (\mathbb{R}^n \times \mathbb{R}^n, U \subset \mathbb{R}^m, \mathcal{U}, f)$ be a control affine system with $U = \left\{u \in \mathbb{R}^m \mid u_1^2 + u_2^2 + \ldots + u_m^2 \leq 1\right\}$ and assume the existence of a continuously differentiable function $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_0^+$ and class $\mathcal{K}_\infty$ functions $\underline{\alpha}, \overline{\alpha}$ for which the following inequalities hold:*

(1) $\forall z, w \in \mathbb{R}^n \qquad \underline{\alpha}(\|z\|) \leq V(z,w) \leq \overline{\alpha}(\|z\|)$;
(2) $\forall z \in \mathbb{R}\ \forall u \in U\ \exists v \in U\ \forall w \in \mathbb{R}^n \qquad \frac{\partial V}{\partial z} f((z,w),u) + \frac{\partial V}{\partial w} f((z,w),v) \leq 0$.

*Then, control system $\Sigma$ satisfies SAI.*

*Proof.* The result follows, for example, from the formulas given in [LS95]. In this reference only stability towards a compact closed set is considered. However, condition (2) guarantees that the resulting controller is a function of $z$ and $u$ alone thus guaranteeing global uniform stability. This is not the case when instead of (2) we use the usual condition $\inf_{v \in V} \frac{\partial V}{\partial z} f((z,w),u) + \frac{\partial V}{\partial w} f((z,w),v) \leq 0$ which corresponds to (note the change in the quantification order):

$$\forall z \in \mathbb{R}\ \forall w \in \mathbb{R}^n\ \forall u \in U\ \exists v \in U \qquad \frac{\partial V}{\partial z} f((z,w),u) + \frac{\partial V}{\partial w} f((z,w),v) \leq 0$$

□

A similar result holds for SAII:

**Proposition 2.9.** *Let $\Sigma = (\mathbb{R}^n \times \mathbb{R}^n, U \subset \mathbb{R}^m, \mathcal{U}, f)$ be a control affine system with $U = \left\{u \in \mathbb{R}^m \mid u_1^2 + u_2^2 + \ldots + u_m^2 \leq 1\right\}$ and assume the existence of a continuously differentiable function $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_0^+$ and class $\mathcal{K}_\infty$ functions $\underline{\alpha}, \overline{\alpha}, \alpha$ for which the following inequalities hold:*

(1) $\forall z, w \in \mathbb{R}^n \qquad \underline{\alpha}(\|z\|) \leq V(z,w) \leq \overline{\alpha}(\|z\|)$;
(2) $\forall z \in \mathbb{R}\ \forall u \in U\ \exists v \in U\ \forall w \in \mathbb{R}^n \qquad \frac{\partial V}{\partial z} f((z,w),u) + \frac{\partial V}{\partial w} f((z,w),v) \leq -\alpha(\|z\|)$.

*Then, control system $\Sigma$ satisfies SAII.*

The previous two results provide a more efficient way to determine if SAI or SAII are satisfied by searching for a single scalar function $V$ instead of having to search for controller $k$.

## 3. Approximate simulations

In this section we introduce the notion of approximate simulation upon which all the results in this paper rely. Approximate simulations relate transition systems that will be used in this paper as abstract models for control systems.

**Definition 3.1.** A transition system $T$ is quintuple $(Q, L, \longrightarrow, O, H)$ consisting of:

- A set of states $Q$;
- A set of labels $L$;
- A transition relation $\longrightarrow \subseteq Q \times L \times Q$;
- An output set $O$;
- An output function $H : Q \to O$.

A metric transition system is a transition system $(Q, L, \longrightarrow, O, H)$ in which the output set $O$ is equipped with a metric $\mathbf{d} : O \times O \to \mathbb{R}_0^+$.

We will follow standard practice and denote an element $(p, l, q) \in \longrightarrow$ by $p \xrightarrow{l} q$. We will also use the notation $p \xrightarrow{l} q$ when $l = l_1 l_2 \dots l_n \in L^*$ is a string of elements in $L$. In this case $p \xrightarrow{l} q$ denotes the existence of a sequence of transitions $p \xrightarrow{l_1} p_1 \xrightarrow{l_2} p_2 \xrightarrow{l_3} \dots \xrightarrow{l_n} q$. We shall say that a transition system $T$ is finite when $Q$ is finite. Transition systems capture dynamics through the transition relation. For any states $p, q \in Q$, $p \xrightarrow{l} q$ simply means that it is possible to evolve or jump from state $p$ to state $q$ under the action labeled by $l$. Note that we cannot model $\longrightarrow$ as a function since, in general, there may be several states $q_1, q_2 \in Q$ such that $p \xrightarrow{l} q_1$ and $p \xrightarrow{l} q_2$.

We will use transition systems as an abstract representation of control systems. There are several different ways in which we can transform control systems into transition systems. We now describe one of these which has the property of capturing all the information contained in a control system $\Sigma$:

**Definition 3.2.** Let $\Sigma = (\mathbb{R}^n, U, \mathcal{U}, f)$ be a control system. The transition system $T(\Sigma) = (Q, L, \longrightarrow, O, H)$ associated with $\Sigma$ is defined by:

- $Q = \mathbb{R}^n$;
- $E = \mathcal{U}$;
- $p \xrightarrow{\mathbf{u}} q$ if there exists a trajectory $\mathbf{x} : [0, \tau] \to \mathbb{R}^n$ of $\Sigma$ satisfying $\mathbf{x}(\tau, p, \mathbf{u}) = q$ for some $\tau \in \mathbb{R}^+$;
- $O = \mathbb{R}^n$;
- $H = 1_{\mathbb{R}^n}$.

Note that $T(\Sigma)$ is a metric transition system when we regard $O = \mathbb{R}^n$ as being equipped with the metric $d(p, q) = \|p - q\|$.

**Definition 3.3.** A run of a transition system $T = (Q, L, \longrightarrow, O, H)$ is a string $r \in Q^*$ for which there exists $l \in L^*$ satisfying $r(i) \xrightarrow{l(i)} r(i+1)$ for $i = 1, \dots, |r| - 1$. A string $s \in O^*$ is said to be an output run of $T$ if there exists a run $r$ of $T$ such that $H(r) = s$. The language of $T$, denoted by $L(T)$, is the set of all output runs of $T$.

Simulation and bisimulation relations are standard mechanisms to relate the properties of transition systems [CGP99]. Intuitively, a simulation relation from a transition system $T_1$ to a transition system $T_2$ is a relation between the corresponding state sets explaining how a run $r$ of $T_1$ can be transformed into a run $s$ of $T_2$. While typical simulation relations require that runs $r$ and $s$ are observationally indistinguishable, that is, $H_1(r) = H_2(s)$, we shall relax this by requiring $H_1(r)$ to simply be close to $H_2(s)$ where closeness is measured with respect to the metric on the output set:

**Definition 3.4.** Let $T_1 = (Q_1, L_1, \underset{1}{\longrightarrow}, O, H_1)$ and $T_2 = (Q_2, L_2, \underset{2}{\longrightarrow}, O, H_2)$ be metric transition systems with the same output space and let $\varepsilon, \delta \in \mathbb{R}^+$. A relation $R \subseteq Q_1 \times Q_2$ is said to be a $(\varepsilon, \delta)$-approximate simulation relation from $T_1$ to $T_2$ if:

(1) $(q_1, q_2) \in R$ implies $\mathbf{d}(H(q_1), H(q_2)) \leq \varepsilon$;
(2) $\mathbf{d}(H(q_1), H(q_2)) \leq \delta$ implies $(q_1, q_2) \in R$;

(3) $(q_1, q_2) \in R$ and $q_1 \xrightarrow[1]{l_1} q_1'$ imply $q_2 \xrightarrow[2]{l_2} q_2'$ with $(q_1', q_2') \in R$.

A different notion of approximate simulation appeared[2] in the work of Girard and Pappas [GP05a] where it was termed $\delta$-approximate simulation relation. Such notion is essentially the same as a $(\varepsilon, \delta)$-approximate simulation relation except for requirement (2) which is not present in [GP05a]. The need for this requirement and for two parameters, namely $\varepsilon$ and $\delta$, will become apparent in Section 4 where we provide a characterization in terms of the stabilizability concepts reviewed in Section 2.

While the existence of a simulation relation between two transition systems implies language containment, the existence of an approximate simulation only implies a weaker version of this containment:

**Proposition 3.5.** *If there exists a $(\varepsilon, \delta)$-approximate simulation relation from $T_1$ to $T_2$ satisfying $R(Q_1) = Q_2$, then $L(T_1) \subseteq \mathcal{B}_\varepsilon\big(L(T_2)\big)$ where $\mathcal{B}_\varepsilon\big(L(T_2)\big)$ denotes the language $\big\{s \in O^* \mid \mathbf{d}(s, r) \leq \varepsilon$ for some $r \in L(T_2)\big\}$.*

*Proof.* For any $s \in L(T_1)$ there exist strings $r \in Q^*$ and $l \in L^*$ such that:

$$r(1) \xrightarrow{l(1)} r(2) \xrightarrow{l(2)} \ldots \xrightarrow{l(|s|-1)} r(|s|)$$

and $H(r) = s$. Let now $q_2 \in Q_2$ satisfy $(r(1), q_2) \in R$ and note that $q_2$ exists since $R(Q_1) = Q_2$. By definition of approximate simulation relation we have $u(1) = q_2 \xrightarrow{m(1)} r(2)$ for some $m(1) \in L_2$ and $(r(2), u(2)) \in R$. Invoking (1) in the definition of approximate simulation we conclude that $\mathbf{d}(r(2), u(2)) \leq \varepsilon$. Extending this argument by induction on the length of $s$ we conclude the existence of $u \in Q_2^*$, $m \in L_2^*$ with $|u| = |r|$, $(r(i), u(i)) \in R$ for $i = 1, \ldots, |s|$ and thus $\mathbf{d}(H(r(i)), H(u(i))) \leq \varepsilon$ or $H(r) \in \mathcal{B}_\varepsilon(L(T_2))$. □

The notion of sub-transition system formalizes the idea of constructing a new transition system by isolating certain states and certain transitions of an existing transition system:

**Definition 3.6.** Transition system $T_1 = (Q_1, L_1, \xrightarrow[1]{}, O, H_1)$ is said to be a sub-transition system of $T_2 = (Q_2, L_2, \xrightarrow[2]{}, O, H_2)$ if $Q_1 \subseteq Q_2$, $H_1 = H_2|_{Q_1}$, and the graph $\Gamma(\imath)$ of the natural inclusion $\imath : Q_1 \hookrightarrow Q_2$ is a relation satisfying requirement (3) in Definition 3.4.

In the remaining paper we will work with sub-transition systems of $T(\Sigma)$ obtained by selecting those transitions from $T(\Sigma)$ describing trajectories of duration $\tau$ for some chosen $\tau \in \mathbb{R}^+$. This can be seen as a time discretization or sampling process.

**Definition 3.7.** Let $\Sigma$ be a control system and $T(\Sigma)$ its associated transition system. For any $\tau \in \mathbb{R}^+$, the sub-transition system $T_\tau(\Sigma) = (Q, L, \longrightarrow, O, H)$ of $T(\Sigma)$ is defined by:

(1) $Q = \mathbb{R}^n$;
(2) $L = \big\{\mathbf{u} \in \mathcal{U} \mid$ the domain of $\mathbf{u}$ is $[0, \tau]\big\}$;
(3) $p \xrightarrow{\mathbf{u}} q$ if there exists a trajectory $\mathbf{x}$ of $\Sigma$ satisfying $\mathbf{x}(\tau, p, \mathbf{u}) = q$;
(4) $O = \mathbb{R}^n$;
(5) $H = 1_{\mathbb{R}^n}$.

Note that $T_\tau(\Sigma)$ is a sub-transition system of $T(\Sigma)$. The notion of parallel composition, that we now introduce, models the effect of interconnecting and synchronizing transition systems on their common outputs. In the same way that transition systems provide an abstract description of control systems, parallel composition enables us to capture control by system interconnection.

**Definition 3.8.** Let $T_1 = (Q_1, L_1, \xrightarrow[1]{}, O, H_1)$ and $T_2 = (Q_2, L_2, \xrightarrow[2]{}, O, H_2)$ be transition systems with common output set. The parallel composition of $T_1$ and $T_2$, denoted by $T_1 \parallel T_2$, is the transition system $(Q_{12}, L_{12}, \xrightarrow[12]{}, O, H_{12})$ defined by:

[2]The authors of [GP05b] only discuss approximate bisimulations but one can easily derive the corresponding notion of approximate simulation.

- $Q_{12} = \{(q_1, q_2) \in Q_1 \times Q_2 \mid H_1(q_1) = H_2(q_2)\}$;
- $L_{12} = L_1 \times L_2$;
- $(q_1, q_2) \xrightarrow[12]{(l_1,l_2)} (q_3, q_4)$ if $q_1 \xrightarrow[1]{l_1} q_3$ and $q_2 \xrightarrow[1]{l_2} q_4$;
- $H_{12}(q_1, q_2) = H_1(q_1) = H(q_2)$.

The following result, describing how $L(T_1 \parallel T_2)$ can be obtained from $L(T_1)$ and $L(T_2)$, is an immediate consequence of the definition of parallel composition:

**Proposition 3.9.** *Let $T_1$ and $T_2$ be transition systems with common output set. Then, $L(T_1 \parallel T_2) = L(T_1) \cap L(T_2)$.*

## 4. Existence of approximate simulations

The adequacy of the notion of approximate simulation relation introduced in the previous section will be justified in this paper with two arguments: its characterization in terms of known stabilizability concepts and its essential role in the proposed symbolic control methodology. In this section we provide the first argument by proving one of the main results of the paper equating existence of approximate simulation relations with SAI:

**Theorem 4.1.** *Let $\Sigma$ be a control system satisfying SAI. Then, for any $\varepsilon \in \mathbb{R}^+$ there exists a $\delta \in \mathbb{R}^+$ such that for all $\tau \in \mathbb{R}^+$ there exists a $(\varepsilon, \delta)$-approximate simulation relation from $T_\tau(\Sigma)$ to $T(\Sigma)$. Conversely, if:*

1. *there exists a function $k : \mathbb{R}^n \times \mathbb{R}^n \times U \to U$ satisfying requirements (1) and (2) in Definition 2.4;*
2. *for any $\varepsilon \in \mathbb{R}^+$ there exists a $\delta \in \mathbb{R}^+$ such that for all $\tau > 0$ there exists a $(\varepsilon, \delta)$-approximate simulation relation from $T_\tau(\Sigma)$ to $T(\Sigma)$ satisfying requirement (3) in Definition 3.4 with $l_2 = k(q_2, q_1, l_1)$,*

*then $\Sigma$ satisfies SAI.*

*Remark* 4.2. Although this result appears to be asymmetric in the sense that the converse statement assumes the existence of $k$ instead of asserting it, this is the "best" converse result that can be proved. To see why this is the case assume that $f(0, 0) = 0$ and let $\mathbf{0}$ be the solution corresponding to initial condition 0 and input trajectory $\mathbf{u}(t) = 0$. Existence of a $(\varepsilon, \delta)$-simulation relation from $T_\tau(\Sigma)$ to $T(\Sigma)$ would imply for any initial condition $y \in \mathcal{B}_\delta(0)$ the existence of an input trajectory $\mathbf{v}$ such that for any $\tau \in \mathbb{R}^+$, $\mathbf{y}(\tau, y, \mathbf{v}) \in \mathcal{B}_\varepsilon(\mathbf{0}) = \mathcal{B}_\varepsilon(0)$. However, existence of such trajectories $\mathbf{y}$ does not imply the existence of a *continuous* feedback $k$ rendering $\dot{y} = f(y, k(y)) = f(y, k(y, 0, 0))$ stable (although discontinuous feedbacks may exist). Note that continuity of $k$ is essential to guarantee well defined trajectories.

*Proof.* Assume that (1) and (2) in Theorem 4.1 hold and denote by $R$ the $(\varepsilon, \delta)$-approximate simulation relation. Let also $\varepsilon, \delta$ and $\tau$ be the scalars whose existence is asserted by (2). For any state $x \in \mathbb{R}^n$ of $T_\tau(\Sigma)$ and for any state $y \in \mathbb{R}^n$ of $T(\Sigma)$ such that $\|x - y\| \leq \delta$ we have $(x, y) \in R$. It then follows from (1) and (2) in Theorem 4.1 and the definition of $(\varepsilon, \delta)$-approximate simulation relation that for any $\mathbf{u} \in \mathcal{U}$, $(\mathbf{x}(\tau, x, \mathbf{u}), \mathbf{y}(\tau, y, k(\mathbf{y}, \mathbf{x}, \mathbf{u})) \in R$ which implies $\|\mathbf{x}(\tau, x, \mathbf{u}) - \mathbf{y}(\tau, y, k(\mathbf{y}, \mathbf{x}, \mathbf{u}))\| \leq \varepsilon$. We thus conclude that for any $\varepsilon > 0$ there exists a $\delta > 0$ such for all $\tau \in \mathbb{R}^+$ the solution of $f \times_k f$ satisfies:

$$\|x - y\| \leq \delta \qquad \Longrightarrow \qquad \|\mathbf{x}(\tau, x, \mathbf{u}) - \mathbf{y}(\tau, y, k(\mathbf{y}, \mathbf{x}, \mathbf{u}))\| \leq \varepsilon$$

Let now $\overline{\delta}(\varepsilon)$ be the supremum of all $\delta$ satisfying the above implication for a fixed $\varepsilon$. Note that according to Definition 3.4, $\overline{\delta}$ is a function of $\varepsilon$ but not of $\tau$. The function $\overline{\delta}$ is positive and strictly increasing and we can lower bound it by a class $\mathcal{K}_\infty$ function $\xi$, that is, $\xi(\varepsilon) \leq \overline{\delta}(\varepsilon)$. It then follows that if we take $\gamma = \xi^{-1}$ we obtain the desired estimate:

$$\|\mathbf{x}(\tau, x, \mathbf{u}) - \mathbf{y}(\tau, y, k(\mathbf{y}, \mathbf{x}, \mathbf{u}))\| \leq \gamma(\|x - y\|)$$

Assume now that $\Sigma$ satisfies SAI and let $Q$ be the set of states of $T_\tau(\Sigma)$. According to Proposition 2.6 there exists a function $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ satisfying $\underline{\alpha}(\|x - y\|) \leq V(x, y) \leq \overline{\alpha}(\|x - y\|)$. Let $\chi = \underline{\alpha}(\varepsilon)$ and define the relation $R \subseteq Q \times \mathbb{R}^n$ by $(q, x) \in R$ iff $V(q, x) \leq \chi$. Then, it follows that $(q, x) \in R$ implies $V(q, x) \leq \chi = \underline{\alpha}(\varepsilon)$

and thus $\|q-x\| \leq \underline{\alpha}^{-1}(V(q,x)) \leq \underline{\alpha}^{-1}(\underline{\alpha}(\varepsilon)) = \varepsilon$ which shows that condition (1) in Definition 3.4 is satisfied. Define now $\delta$ as $\overline{\alpha}^{-1}(\chi)$. Then, $\|q-x\| \leq \delta$ and $V(q,x) \leq \overline{\alpha}(\|q-x\|)$ imply $V(q,x) \leq \overline{\alpha}(\overline{\alpha}^{-1}(\chi)) = \chi$ leading to $(q,x) \in R$ and showing that condition (2) in Definition 3.4 holds. It remains to show that condition (3) also holds. Let $(q,x) \in R$, assume that $q \xrightarrow{l} q'$ in $T_\tau(\Sigma)$ and let $\mathbf{q}$ be the trajectory defined by initial condition $q$ and input trajectory $l \in \mathcal{U}$. From (2) in Proposition 2.6 we conclude that $V(q',x') \leq V(q,x) \leq \chi$ with $x' = \mathbf{x}(\tau, x, k(\mathbf{x}, \mathbf{q}, l))$ which implies $(q',x') \in R$. By definition of $T(\Sigma)$ we have $x \xrightarrow{k(\mathbf{x},\mathbf{q},l)} x'$ in $T(\Sigma)$ which shows that requirement (3) holds and concludes the proof. □

In concrete applications we shall not work with $T_\tau(\Sigma)$ but with a finite sub-transition system of $T_\tau(\Sigma)$. In this case we can still guarantee existence of a $(\varepsilon,\delta)$-approximate simulation relation:

**Corollary 4.3.** *Let $\Sigma$ be a control system satisfying SAI and let $T = (Q, L, \longrightarrow, O, H)$ be a finite sub-transition system of $T_\tau(\Sigma)$. Then there exists a contractible compact set $S \subset \mathbb{R}^n$ containing $Q$ and a $(\varepsilon,\delta)$-approximate simulation relation $R$ from $T$ to $T_\tau(\Sigma)$ satisfying $R(Q) = S$.*

*Proof.* The result follows from Theorem 4.1 by choosing $\chi$ large enough. Let $S'$ be a contractible compact set containing $Q$. Since $V$ is radially unbounded we can always chose $\chi$ large enough so that the sets $V_q^\chi = \{x \in \mathbb{R}^n \mid V(q,x) \leq \chi\}$ cover $S'$, that is, $S' \subseteq \bigcup_{q\in Q} V_q^\chi$. Define now $S$ as $S = \bigcup_{q\in Q} V_q^\chi$. Set $S$ clearly satisfies $R(Q) = S$, is compact since it is the union of compact sets and is contractible since we can contract each set $V_q^\chi$ to $q \in S'$ and $S'$ is also contractible. □

Existence of approximate simulations from arbitrary sub-transition systems of $T_\tau(\Sigma)$ to $T_\tau(\Sigma)$ is thus guaranteed by SAI which, according to Proposition 2.8, can be checked by resorting to a control Lyapunov function. The correct by design methodology that is being introduced in this paper thus leverages on the extensive work that has been done by the control community on stability, stabilization and its Lyapunov characterizations.

The equality $R(Q) = S$, provided by Corollary 4.3, is important since it guarantees that for any point $s \in S$ we can always find a state of $T$ which is approximately related to $s$. This implies, as we will see in the next section, that a controller designed for $T$ can be used to control $T(\Sigma)$ for any $s \in S$.

## 5. Approximate simulation based control

In this section we provide part of the second argument justifying the need for the concept of approximate simulation. We show how we can use approximate simulations to simplify controller synthesis. Further substantiation for this claim is provided by the examples in Section 7.

**Theorem 5.1.** *Let $\Sigma$ be a control system, let $T$ be a sub-transition system of $T(\Sigma)$ and let $\mathcal{S} \subseteq \mathcal{B}_\varepsilon\big(L(T(\Sigma))\big)$ be a language specification. If there exists a controller $C$ such that $L(C \parallel T) \subseteq \mathcal{S}$, then controller $C' = C \parallel T$ satisfies $L(C' \parallel T(\Sigma)) \subseteq \mathcal{S}$.*

*Proof.* Since there exists a $(\varepsilon,\delta)$-approximate simulation relation from $T$ to $T(\Sigma)$ we have, by Proposition 3.5, that $L(T) \subseteq \mathcal{B}_\varepsilon\big(L(T(\Sigma))\big)$. Therefore:

$$\begin{aligned} L(C' \parallel T(\Sigma)) &= L(C \parallel T \parallel T(\Sigma)) \\ &= L(C) \cap L(T) \cap L(T(\Sigma)) \\ &\subseteq L(C) \cap L(T) \cap \mathcal{B}_\varepsilon\big(L(T(\Sigma))\big) \\ &= L(C) \cap L(T) \\ &= L(C \parallel T) \\ &\subseteq \mathcal{S} \end{aligned}$$

□

Theorem 5.1 only acquires its true relevance when the synthesis of $C$ is much simpler than the synthesis of a controller for $T_\tau(\Sigma)$ or $\Sigma$. In particular, this is the case when $T$ is finite since controller design can then be seen as a purely algorithmic problem in the realm of supervisory control of discrete-event systems [KG95, CL99]. Since we are using approximate simulations we can only guarantee that controller $C'$ enforces specifications up to an accuracy measured by the parameter $\varepsilon$. However, reducing the value of this parameter will force the number of states in the abstraction $T$ to increase as we discuss in more detail in the next section where the actual computation of $T$ is addressed.

Supervisor $C'$ is a mathematical description of the control software necessary to enforce the specification as it prescribes the behavior of $\Sigma$. A more detailed model of the resulting control software, describing which input signals should be sent to $\Sigma$ and when, can be obtained from $C'$ as follows. We consider a hybrid controller $H(C')$ in which continuous flows take place on transitions and no time is spent on discrete locations. Although, this notion of hybrid system differs from the standard hybrid automata model [Hen96], it is equivalent and will lead to a simpler construction of $H(C')$ from $C'$. Moreover, as the hybrid control system $H(C')$ will not be used elsewhere in this paper, instead of a formal definition we will simply described its execution (semantics). Starting at a given state $x \in \mathbb{R}^n$ of $\Sigma$, which may be any state in $S$ or in a strict subset depending on the specific controller $C'$, there exists a state $p$ of $T$ such that $(p, x) \in R$ where $R$ is the $(\varepsilon, \delta)$-approximate simulation relation from $T$ to $T(\Sigma)$. Existence of $p$ follows from $R(Q) = S$ which is asserted by Corollary 4.3. We are implicitly assuming that $T$ is finite since when this is not the case $T$ cannot be physically implemented on a finite memory computing device. Let now $(p, x') \xrightarrow{\mathbf{u}} (q, y')$ be any transition in $C'$. This transition is "executed" on $\Sigma$ by using the controller $k$ during $\tau$ units of time, where $\tau$ is the duration of $\mathbf{u}$, to control $\Sigma$ from the current state $x$ to some state $y$. By definition of $(\varepsilon, \delta)$-approximate simulation relation we know that $\|y - y'\| \leq \varepsilon$. If we regard the transition $(p, x') \xrightarrow{\mathbf{u}} (q, y')$ as a symbolic command, the existence of a $(\varepsilon, \delta)$-approximate simulation relation guarantees that such command can be executed with guaranteed resolution $\varepsilon$. The process is now repeated by identifying a new state $q'$ (which may be $q$) such that $(q', y') \in R$ and by executing any transition $(q', y') \xrightarrow{\mathbf{u}'} (r, z)$ in $C'$ by using controller $k$. Controller $C$, relation $R$ and controller $k$ provide all the information necessary to automatically generate the control software of which $H(C')$ can be seen as a mathematical description.

We have not made any determinism assumption on $C'$. This is intended since it allows for incremental design. The nondeterminism of $C'$ allows one to view $C' \parallel T_\tau(\Sigma) = T'$ as a control system in the sense that for any state there are different possibilities for future evolution. After designing $C$ we can consider additional requirements for $T'$ and synthesize a new supervisory controller $C''$ making $C'' \parallel T = C'' \parallel (C' \parallel T)$ satisfy the additional requirements. This incremental design possibility is very useful in practice since many of the specifications only become available after the design process has been initiated and many specifications are changed several times during the design phase.

## 6. Computation of finite sub-transition systems

We consider the computation of finite sub-transition systems in the framework of quantized control systems [BMP02, PLPB02, BMP06] where one restricts attention to a denumerable subset of $\mathcal{U}$ whose elements are termed control quanta. In this paper, control quanta are defined by constant input curves assuming values in a finite set $\mathtt{U} \subset U$. Although this restriction on the class of input curves may appear to be quite drastic, there are several reasons to consider it. In many man made systems, input signals are physically implemented as piece-wise constant signals. Our assumptions are then in consonance with real physical constraints. Moreover, input quantization can be seen as a very powerful complexity reduction mechanism simplifying several control synthesis problems [BMP02, PLPB02, BMP06].

From Corollary 4.3 we know that under SAI we can construct a $(\varepsilon, \delta)$-approximate simulation relation from any finite sub-transition system $T$ of $T_\tau(\Sigma)$ to $T_\tau(\Sigma)$. The question we address in this section is:

*How do we compute such finite sub-transition system?*

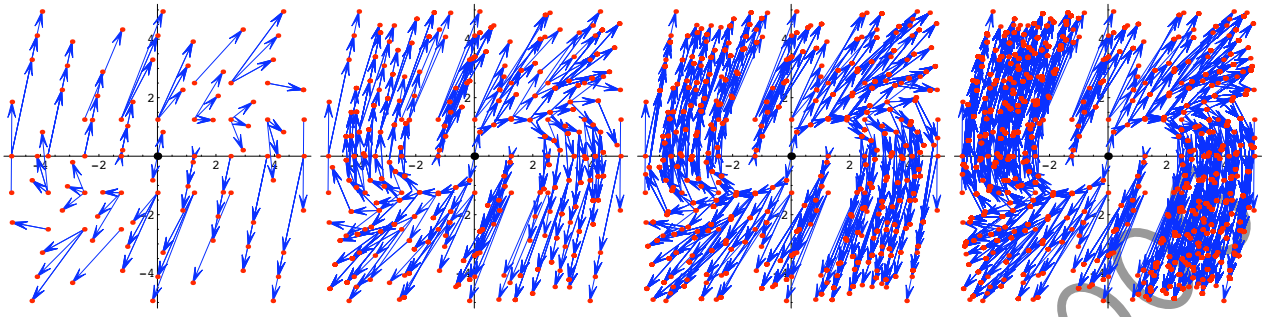

FIGURE 1. Finite sub-transition system of the linear system (6.1) obtained through the naive method. States are represented by red dots while black dots represent states for which there exists a self transition. Transitions are represented by blue arrows. From left to right we have the result of the first, third, fifth and tenth simulation rounds.

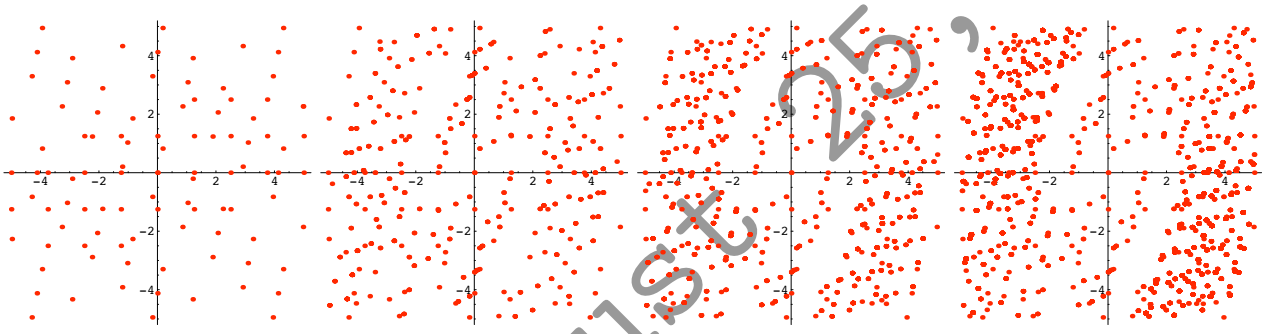

FIGURE 2. States of the finite sub-transition system of the linear system (6.1) obtained through the naive method. From left to right we have the result of the first, third, fifth and tenth simulation rounds.



We assume that parameters $\tau$ and $\varepsilon$, describing the desired sampling time and state accuracy, respectively, are given along with a finite set $\mathtt{U} \subset U$ of inputs and compact subset $S \subset \mathbb{R}^n$ of the state space. The finite set $\mathtt{U}$ describes the input quantization while the set $S$ represents the working region that is of interest and which will be compact (at least bounded) in concrete applications. The naive approach to obtain a sub-transition system based on the given data would be to construct the transition relation by rounds. The first round would compute all the transitions $p \xrightarrow{u} q$ with $u \in \mathtt{U}$, $p \in [S]_\eta$, (where $\eta \in \mathbb{R}^+$ is chosen so that any $x \in S$ belongs to $\mathcal{B}_\varepsilon(p')$ for some $p' \in [S]_\eta$) and for which there exists a trajectory $x : [0, \tau] \to \mathbb{R}^n$ of $\Sigma$ satisfying $\mathbf{x}(\tau, p, u) = q$. The second round would repeat the same construction, enlarging the transition relation with transitions starting at the states $q$ obtained in the first round. The sub-transition system $T$ could then be seen as the limit of this process. One immediate difficulty with this naive approach is to determine at which round to terminate the construction of $T$. But there are also other difficulties that we now illustrate through an academic example (more interesting examples will be given on Section 7).

Consider the following linear control system:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} 0 \\ u \end{bmatrix} \tag{6.1}$$

with states $(x_1, x_2) \in [-5, 5] \times [-5, 5] = S$ and input $u \in \{-1, 0, 1\} = \mathtt{U}$. The outcome of the naive approach to the construction of a finite sub-transition system of $T_{0.5}(\Sigma)$ is displayed in Figure 1 and Figure 2. The first observation is that terminating the process after some predetermined number $n$ of rounds may lead to a sub-transition system that is only guaranteed to be nonblocking during the first $n$ transitions. Since many

control tasks require the system to run for an arbitrarily long sequence of steps this is a serious drawback of the naive approach. Moreover, the states of the constructed sub-transition system are not evenly distributed across the state space thus implying that we have a better description of the dynamics in some areas than in others. These difficulties can be avoided when a *$\varepsilon$-regular* sub-transition system can be found:

**Definition 6.1.** Let $\Sigma$ be a control system and let $\tau, \varepsilon \in \mathbb{R}^+$ and a finite $\mathtt{U} \subset U$ be given. A sub-transition system $T$ of $T_\tau(\Sigma)$ is said to be $\varepsilon$-regular if:

(1) there exists a $(\varepsilon, \delta)$-approximate simulation relation from $T$ to $T_\tau(\Sigma)$;
(2) $Q \subseteq [\mathbb{R}^n]_\chi$ for some $\chi \in \mathbb{R}^+$;
(3) for every $p \in Q$ and $l \in \mathtt{U}$ there exists a $q \in Q$ such that $p \xrightarrow{l} q$ in $T$.

A regular sub-transition system $T$ is equipped with a $(\varepsilon, \delta)$-approximate simulation relation to $T_\tau(\Sigma)$ and solves the difficulties illustrated by the previous example by guaranteeing that its state set is a subset of a lattice. When working on a compact subset of the state space, usually the case in most applications, $T$ is in fact finite so the construction of $T$ is guaranteed to terminate. Furthermore, $T$ is nontrivial in the sense that for every state $p$ of $T$ all the transitions labeled by inputs in $\mathtt{U}$ are captured in $T$ and lead to states of $T$. Note that when one restricts attention to a compact subset $S$ of the state space, some states may fail to have transitions defined for every element of $\mathtt{U}$. However, this is the case only when these transitions would lead to states outside $S$. Existence of $\varepsilon$-regular sub-transition systems is guaranteed by SAII:

**Theorem 6.2.** *For any control system $\Sigma$ satisfying SAII, for any $\varepsilon \in \mathbb{R}^+$, for any finite $\mathtt{U} \subset U$ and for any $\tau \in \mathbb{R}^+$ such that $\beta(\varepsilon, \tau) < \varepsilon$ there exists a $\varepsilon$-regular sub-transition system $T$ of $T_\tau(\Sigma)$. Furthermore, $\chi$ can be chosen to be any positive real number integrally dividing $2\varepsilon/\sqrt{n}$ and satisfying:*

$$0 < \chi \leq \frac{2}{\sqrt{n}}\big(\varepsilon - \beta(\varepsilon, \tau)\big), \tag{6.2}$$

*and the $(\varepsilon, \delta)$-approximate simulation relation $R$ from $T$ to $T_\tau(\Sigma)$ satisfies $R(Q) = \mathbb{R}^n$ where $Q$ is the state set of $T$.*

*Proof.* We start by constructing $T$. Let $\xi = 2\varepsilon/\sqrt{n}$, assume that $\chi$ integrally divides $\xi$ and that it satisfies inequality (6.2). Let now $F : \mathbb{R}^n \to 2^{[\mathbb{R}^n]_\chi}$ be the function defined by $q \in F(x)$ if $x \in \mathcal{B}_{\varepsilon - \beta(\varepsilon,\tau)}(q)$. The set $Q$ of states of $T$ is the smallest set satisfying:

(1) $[\mathbb{R}^n]_\xi \subseteq Q$;
(2) $p \in Q$, $u \in \mathtt{U}$ and $q \in F\big(\mathbf{x}(\tau, p, \mathbf{u})\big)$ for some trajectory $\mathbf{x} : [0, \tau] \to \mathbb{R}^n$ of $\Sigma$ with $\mathbf{u}(t) = u$ for $0 \leq t \leq \tau$ imply $q \in Q$.

The transition relation is defined by $p \xrightarrow{u} q$ if $p, q \in Q$, $u \in \mathtt{U}$ and there exists a trajectory $\mathbf{x} : [0, \tau] \to \mathbb{R}^n$ of $\Sigma$ satisfying $q \in F\big(\mathbf{x}(\tau, p, \mathbf{u})\big)$ with $\mathbf{u}(t) = u$ for $0 \leq t \leq \tau$. Transition system $T$ is thus defined by $T = (Q, \mathtt{U}, \longrightarrow, \mathbb{R}^n, \imath : Q \hookrightarrow \mathbb{R}^n)$. The approximate simulation relation is given by $(q, x) \in R$ iff $\|q - x\| \leq \varepsilon$. Note that requirements (1) and (2) in Definition 3.4 are satisfied by construction if we take $\delta = \varepsilon$. By noting that any point $x \in \mathbb{R}^n$ belongs to $\mathcal{B}_\varepsilon(q)$ for some $q \in [\mathbb{R}^n]_\xi$ we conclude that $R(Q) = \mathbb{R}^n$. We now show that $R$ also satisfies requirement (3) in Definition 3.4. Let $(p, y) \in R$ and assume that $p \xrightarrow{\mathbf{u}} q$ with $\mathbf{u}(t) = u \in \mathtt{U}$ for $0 \leq t \leq \tau$. This implies the existence of a trajectory $\mathbf{x}$ of $\Sigma$ satisfying $q \in F\big(\mathbf{x}(\tau, x, \mathbf{u})\big)$ or equivalently $\|q - \mathbf{x}(\tau, x, \mathbf{u})\| \leq \varepsilon - \beta(\varepsilon, \tau)$. Since $(p, y) \in R$ implies $\|p - y\| \leq \varepsilon$ we have, by SAII, $\|\mathbf{x}(\tau, x, \mathbf{u}) - \mathbf{y}(\tau, y, k(\mathbf{y}, \mathbf{x}, \mathbf{u}))\| \leq \beta(\|p - y\|, \tau) = \beta(\varepsilon, \tau)$. It then follows:

$$\begin{aligned} \|q - \mathbf{y}(\tau, y, k(\mathbf{y}, \mathbf{x}, \mathbf{u}))\| &\leq \|q - \mathbf{x}(\tau, x, \mathbf{u}) + \mathbf{x}(\tau, x, \mathbf{u}) - \mathbf{y}(\tau, y, k(\mathbf{y}, \mathbf{x}, \mathbf{u}))\| \\ &\leq \|q - \mathbf{x}(\tau, x, \mathbf{u})\| + \|\mathbf{x}(\tau, x, \mathbf{u}) - \mathbf{y}(\tau, y, k(\mathbf{y}, \mathbf{x}, \mathbf{u}))\| \\ &\leq \varepsilon - \beta(\varepsilon, \tau) + \beta(\varepsilon, \tau) = \varepsilon \end{aligned}$$

thus showing $y \xrightarrow{k(\mathbf{y},\mathbf{x},\mathbf{u})} \mathbf{y}(\tau, y, k(\mathbf{y}, \mathbf{x}, \mathbf{u}))$ in $T_\tau(\Sigma)$ with $(q, \mathbf{y}(\tau, y, k(\mathbf{y}, \mathbf{x}, \mathbf{u}))) \in R$ which concludes the proof. □

The proof of Theorem 6.2 is constructive since it defines how to construct the sub-transition system $T$ and the $(\varepsilon,\delta)$-approximate simulation relation. Intuitively, the construction of $T$ proceeds as follows. We use $[\mathbb{R}^n]_{\frac{2\varepsilon}{\sqrt{n}}}$ as the initial state set $Q$ of $T$. This state set has the property that for every $x \in \mathbb{R}^n$ there exists a $q \in Q$ such that $x \in \mathcal{B}_\varepsilon(q)$. Starting from this initial state set we construct all the transitions $q \xrightarrow{u} p$ with $q \in Q$ and $u \in \mathcal{U}$. However, instead of declaring $q \xrightarrow{u} p$ to be a transition in $T$ we declare that all the transitions $q \xrightarrow{u} p'$, with $p' \in [\mathbb{R}^n]_\chi$ and $p \in \mathcal{B}_{\chi\frac{\sqrt{n}}{2}}(p')$, are transitions of $T$. It thus follows by construction that $Q \subset [\mathbb{R}^n]_\chi$ since $\chi$ integrally divides $\varepsilon$. Moreover, when working on a compact subset $S$ of $\mathbb{R}^n$, there are only finitely many points of the lattice $[\mathbb{R}^n]_\chi$ which are contained in $S$ and this guarantees termination of the construction of $T$ in a finite number of steps. Note also that the resulting transition system $T$ is nondeterministic since for every $p$ there exist, in general, several $p'$ satisfying the conditions $p' \in [\mathbb{R}^n]_\chi$ and $p \in \mathcal{B}_{\chi\frac{\sqrt{n}}{2}}(p')$. We thus see that the regularization process consists in approximating $p$ by several points $p' \in [\mathbb{R}^n]_\chi$. This is only possible since we only ask for the existence of a $(\varepsilon,\delta)$-approximate simulation relation from $T$ to $T_\tau(\Sigma)$ and since we can use the feedback controller $k$ to correct for the introduced errors when replacing $p$ with $p'$. It can also be seen from the construction of $T$ that if $S$ is of the form $S = [-s/2, s/2]^n$ for some $s \in \mathbb{R}$ then $T$ will have at most $\lceil s/\chi \rceil^n$ states and $\lceil s/\chi \rceil^n |\mathtt{U}|$ transitions. This exponential dependence on $n$ is unavoidable if we want to keep the resolution $\varepsilon$ constant when $n$ increases. We shall further comment on this fact in Section 9. The $(\varepsilon,\delta)$-approximate simulation relation $R$ from $T$ to $T_\tau(\Sigma)$ is simply given by $(q,x) \in R$ if $\|q - x\| \leq \varepsilon$ for any state $q \in Q$ of $T$ and $x \in \mathbb{R}^n$ of $T_\tau(\Sigma)$. Note that in this case we have $\delta = \varepsilon$.

We now return to the linear example to illustrate Theorem 6.2. Since the linear system (6.1) is controllable it is also asymptotically stabilizable which implies that SAII holds. One possible stabilizing controller is given by $u = Kx = -80x_1 - 20x_2$ which places the eigenvalues of the closed loop system at $-9$ and $-9$, respectively (the open loop eigenvalues are 1 and 1). Stability can also be shown by resorting to the Lyapunov function $V = x^T P x$ defined by the matrix:

$$P = \begin{bmatrix} \frac{43}{18} & \frac{1}{162} \\ \frac{1}{162} & \frac{41}{1458} \end{bmatrix}$$

and whose derivative along the closed loop system is $\dot{V} = -x^T x$. Since the dynamics of $x - y$ is given by:

$$\dot{x} - \dot{y} = Ax - Ay + Bu - Bv = A(x-y) + B(u-v)$$

we see that the controller $v = u + K(x-y)$ can be used to enforce SAII. In order to obtain a $\varepsilon$-regular sub-transition system for $\varepsilon = 1$ we solve for the flow of the closed loop system and obtain $\|\mathbf{x}(0.5) - \mathbf{y}(0.5)\| \leq 0.46$ for all initial conditions satisfying $\|x - y\| \leq 1$. Using 0.46 as our estimate for $\beta(1, 0.5)$ we pick $\chi = \frac{2}{\sqrt{2}}0.5$. The resulting 1-regular sub-transition system is displayed in Figure 3. It has 439 states while the naive approach produced a transition system with 4437 states after ten rounds. In the nonlinear case we cannot estimate $\beta$ by solving for the flow and we have to resort to estimates based on Lyapunov functions. This method produces much more conservative results as we now show. Using the above Lyapunov function $V$ we can use the following well known estimate [AM97]:

$$\|\mathbf{x}(\tau) - \mathbf{y}(\tau)\| \leq \sqrt{\frac{\lambda_M(P)}{\lambda_m(P)}}\, e^{\frac{1}{2}\frac{\lambda_M(Q)}{\lambda_M(P)}\tau} \|x - y\|$$

for $\beta(\|x-y\|, \tau)$ where $\lambda_M$ and $\lambda_m$ denote the largest and the smallest eigenvalues of a given matrix, respectively, and $Q$ is the matrix satisfying $\dot{V} = (x-y)^T Q (x-y)$. Using this estimate we obtain $\|\mathbf{x}(0.5) - \mathbf{y}(0.5)\| \leq 8.3$ and a value of 0.46 is only obtained for $\tau > 14.4s$. This is one of the difficulties faced when applying the proposed methodology to concrete examples. This difficulty can, however, be mitigated by defining the approximate simulation relation in terms of the level sets of a Lyapunov function. This and other extensions of Theorem 6.2 are now discussed in more detail.

(1) Instead of working with the Euclidean norm we could have constructed $T$ and defined the $(\varepsilon,\delta)$-simulation relation by directly using the level sets of the Lyapunov function whose existence is implied by SAII (see Proposition 2.7). Since given an equation of the form $\dot{V} \leq -\alpha(V)$ we can always transform

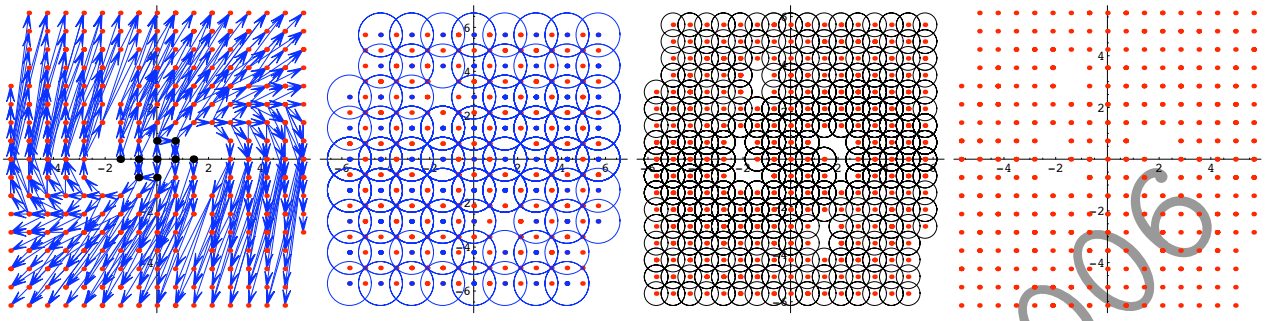

FIGURE 3. $\varepsilon$-regular sub-transition system associated with the linear system (6.1) for $\varepsilon = 1$ and $\chi = 0.5(2/\sqrt{2})$. From left to right we have: the 1-regular sub-transition system; the states of the sub-transition system belonging to $[S]_{1\frac{2}{\sqrt{2}}}$ represented in blue and enclosed in a circle of radius 1 while the remaining states are represented in red; all the states of the sub-transition system, enclosed in a circle of radius $0.5 = \chi\frac{\sqrt{2}}{2}$; all the states of the sub-transition system. The sates belonging to $[S]_\chi$ which are not displayed are states whose transitions lead to points outside $S$ and which have no incoming transitions.

$V$ into another Lyapunov function $U$ satisfying $\dot{U} \leq -U$, we can sidestep the need to estimate $\beta$. However, working directly with level sets of $U$ increases the complexity of the computations since $U$ is a general nonlinear function.

(2) The global nature of SAII upon which Theorem 6.2 relies was assumed for simplicity of presentation and can be relaxed. Since we have a $(\varepsilon, \delta)$-approximate simulation relation from $T$ to $T_\tau(\Sigma)$, states $x \in \mathbb{R}^n$ of $T(\Sigma)$ related to states $q \in Q$ of $T$ will necessarily satisfy $\|q - x\| \leq \varepsilon$. We can thus relax SAII by requiring that it holds only for initial conditions $(x, y) \in \mathbb{R}^n \times \mathbb{R}^n$ satisfying $\|x - y\| \leq \varepsilon$.

(3) SAII was defined in terms of the existence of a single controller $k$. In many situations, however, we have not only but but several controllers $\{k_i\}_{i\in I}$, each designed to track a familly of trajectories. It is clear that the conclusions of Theorem 6.2 still hold in this case provided that we use for $\beta$ a $\mathcal{KL}$ function satisfying $\beta_i(r, s) \leq \beta(r, s)$ for all $i \in I$ and where $\beta_i$ is the $\mathcal{KL}$ function associated with controller $k_i$.

(4) Although for linear systems we can explicitly compute the flow for each of the inputs in `U` the same is no longer true in the nonlinear case. We are thus forced to resort to numerical simulation methods in order to construct $T$. Theorem 6.2 is still of value in this case since given a bound $\eta > 0$ on the simulation error, that is, $\|\mathbf{x}(\tau) - \tilde{\mathbf{x}}(\tau)\| \leq \eta$ where $\tilde{\mathbf{x}}$ is the simulated value, the conclusions of Theorem 6.2 still hold provided that we choose $\tau$ such that $\beta(\varepsilon, \tau) < \varepsilon + \eta$. Note that such $\tau$ always exists since $\beta(r, s)$ is a decreasing function of $s$. In this case, $\chi$ can be any positive real number integrally dividing $2\varepsilon/\sqrt{n}$ and satisfying:

$$0 < \chi \leq \frac{2}{\sqrt{n}}\big(\varepsilon + \eta - \beta(\varepsilon, \tau)\big)$$

## 7. EXAMPLES

One of the simplest nonlinear control systems, representative of the large class of nonholomic control systems, is the unicycle. It is described by the following equations:

$$\begin{aligned} \dot{x}_1 &= u_1 \cos x_3 \\ \dot{x}_2 &= u_1 \sin x_3 \\ \dot{x}_3 &= u_2 \end{aligned} \tag{7.1}$$

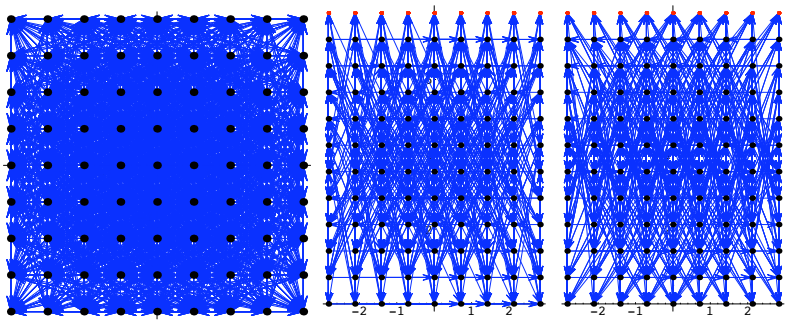


FIGURE 4. $\varepsilon$-regular sub-transition system of the unicycle (7.1) for $\tau = 3$, $\varepsilon = 1$, $\chi = 0.5$, $S = [-2, 2] \times [-2, 2] \times [0, 2\pi]$ and $\mathtt{U} = \{0, 1\} \times \{-1.1, -1, 1, 1.1\}$. States are represented by red dots while black dots represent states with self transitions. From left to right we have: the projection of $T$ on the $x_1$ and $x_2$ coordinates; the projection of $T$ on the $x_1$ and $x_3$ coordinates; and the projection of $T$ on the $x_2$ and $x_3$ coordinates.

where $(x_1, x_2) \in \mathbb{R}^n$ represents the Euclidean position of the unicycle, $x_3 \in [0, 2\pi]$ represents the unicycle's heading, parameterized by an angle between 0 and $2\pi$ measured with respect to the horizontal axis, and $u_1, u_2$ are the inputs describing translational and angular velocities, respectively. The input set is $U = [0, 1] \times [-1, 1]$ and we work on the compact $S = [-2, 2] \times [-2, 2] \times [0, 2\pi]$. Note that by definition of $U$, $u_1$ is always nonnegative in order to guarantee that the unicycle will not move backwards. We take $\mathcal{U}$ to be the set of constant functions defined on intervals $[0, \tau]$ for $\tau = 3$, with values on $\mathtt{U} = \{0, 1\} \times \{-1.1, -1, 1, 1.1\}$ and we are interested in building a $\varepsilon$-regular sub-transition system $T$ for $\varepsilon = 1$. In order to introduce a feedback enforcing SAII in this scenario we consider the error coordinates $z = (z_1, z_2, z_3)$ defined by:

$$\begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} = \begin{bmatrix} \cos y_3 & \sin y_3 & 0 \\ -\sin y_3 & \cos y_3 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 - y_1 \\ x_2 - y_2 \\ x_3 - y_3 \end{bmatrix} \tag{7.2}$$

Note that this transformation mapping $x - y$ to $z$ is invertible, maps the origin to the origin and has unitary norm. The error dynamics is now given by:

$$\begin{aligned} \dot{z}_1 &= v_2 z_2 - v_1 + u_1 \cos(z_3) \\ \dot{z}_2 &= -v_2 z_1 + u_1 \sin(z_3) \\ \dot{z}_3 &= u_2 - v_2 \end{aligned}$$

and using the following feedback inspired on [PLLN98]:

$$\begin{aligned} v_1 &= u_1 \cos(z_3) + \big(u_2 + z_3 - 2\,\mathrm{sign}(u_2)\big) z_2 + 2 z_1 \\ v_2 &= u_2 + z_3 \end{aligned}$$

which is at least $C^1$ since $u_2$ is constant, we obtain:

$$\dot{z}_1 = -2 z_1 + 2\,\mathrm{sign}(u_2) z_2 \tag{7.3}$$

$$\dot{z}_2 = -(u_2 + z_3) z_1 + u_1 \sin(z_3) \tag{7.4}$$

$$\dot{z}_3 = -z_3 \tag{7.5}$$

Since uniform global asymptotic stability of (7.3) through (7.5) can be proved by using the techniques introduced in [PLLN98] we conclude that SAII holds. The resulting $\varepsilon$-regular sub-transition system $T$ for $\chi = 0.5$ is shown in Figure 4. As exemplified with the linear system (6.1), obtaining an estimate of $\beta$ from a Lyapunov function results in a very conservative choice for $\chi$. The value of 0.5 chosen for $\chi$ was obtained based on extensive numerical simulations. An alternative approach would consist in working directly with the level sets of a Lyapunov equation as discussed before.

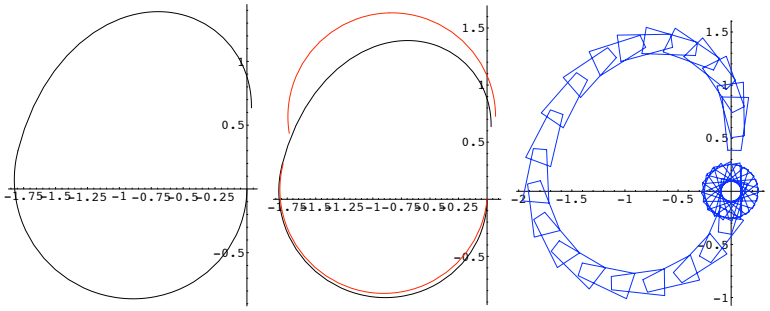

FIGURE 5. Evolution of the unicycle according to the sequence of transitions (7.6) implementing a specification requiring motion from position $(0,0)$ and heading $\pi/2$ to position $(0,1)$ and heading $3\pi/4$. The real position trajectory is represented in black, the reference position trajectories are represented in red and snapshots of the unicycle motion are represented in blue.

7.1. **Reachability specifications.** Reachability specifications can easily be addressed in the proposed framework. Assume, for example, that one is interested in driving the unicycle from the position $(0,0)$ with heading $\pi/2$ to the position $(0,1)$ with heading $3\pi/4$. A control strategy for this specification can be obtained by finding a path in $T$ from a state $p$ such that $(0,0,\pi/2) \in \mathcal{B}_1(p)$ to a state $q$ satisfying $(0,1,3\pi/4) \in \mathcal{B}_1(q)$. We have thus transformed the complicated problem of planning trajectories for nonholonomic systems into a search in a graph. One possible solution is given by:

$$(0,0,0.55\pi) \xrightarrow{(0,-1.1)} (0,0,1.47\pi) \xrightarrow{(1,-1)} (-1.73,1.15,0.55\pi) \xrightarrow{(1,-1.1)} (0,1.15,1.65\pi) \tag{7.6}$$

where we have labeled the transitions by the constant inputs used to implement the motion between the indicated states. Note that the first step corresponds to a pure rotation which does not alter the unicycle's position displayed in Figure 5. In this figure we can see that the reference trajectories are discontinuous although the discontinuities are within the resolution $\varepsilon = 1$. Moreover, these discontinuities are correctly compensated by the feedback controller $k$ as predicted by Theorem 6.2.

A different example of reachability specifications is the construction of periodic orbits. The design of periodic orbits is a frequent but difficult specification for certain kinds of control systems such as multi-legged robots, in which different periodic orbits represent different gaits, or industrial robots that need to perform repetitive tasks. Periodic orbits can easily be obtained by resorting to $T$. Assume that we want to identify a periodic orbit passing through the origin. We can, for example, search for a path from position $(0,0)$ and heading $\pi/2$ to position $(1.8,0)$ and heading $3\pi/4$. Then, we search for another path from position $(1.8,0)$ and heading $3\pi/4$ to position $(0,0)$ and heading $\pi/2$. A solution to this reachability problem is given by:

$$(0,0,0.55\pi) \xrightarrow{(1,-1.1)} (1.73,0,1.47\pi) \xrightarrow{(1,-1)} (0,0,0.55\pi) \tag{7.7}$$

and the corresponding trajectory is represented in Figure 6. Note that the initial and final positions match up to resolution $\varepsilon = 1$ and this error between the reference trajectories is correctly handled by the controller.

7.2. **Language specifications.** We now consider specifications described by regular languages. This is the kind of specifications that naturally leads to hybrid behavior of purely continuous systems. There are several examples where control objectives involve a sequence of smaller tasks that needs to be performed according to a given order. They arise in manufacturing systems where different sequences of processing steps are required to produce the final product, in autopilot control systems for landing and take-off maneuvers, and in mobile robotics among many other examples.

Let us consider a specification language $\mathcal{S} \subseteq O^*$ where $O$ is the output set of $T_\tau(\Sigma)$. As we discussed in Section 5, we can synthesize a controller enforcing $\mathcal{S}$ by working directly on $T$. The construction of such

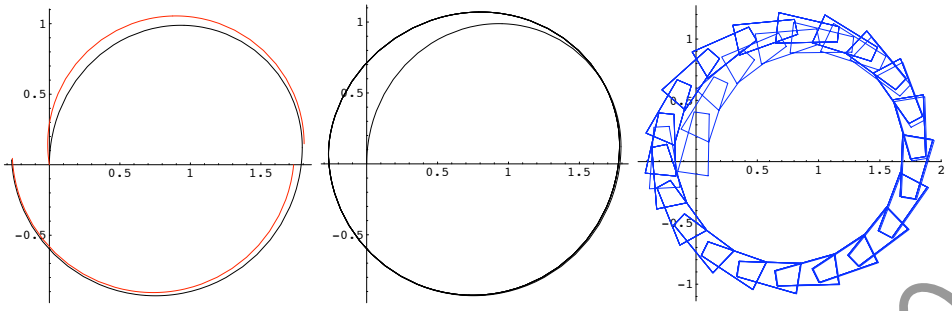

FIGURE 6. Periodic orbit passing through the origin and corresponding to the sequence of transitions (7.7). Reference position trajectory is represented in red and actual position trajectory in black. From left to right we have: reference and actual position trajectory for one orbit; actual position trajectory for 6 orbits; and snapshots of the unicycle motion for 6 orbits.

controller falls under the domain of supervisory control of discrete event systems [KG95, CL99] and it is well known that such controllers, being representable by finite-state machines, require discrete memory. Any such controller acting on the continuous system $\Sigma$ will naturally result in a hybrid system combining the discrete memory encoded in the finite-state machine supervisor with the feedback control laws enforcing the symbolic commands issued by the supervisor. To simplify the presentation we use a `Rotate-Right` task that can be enforced on $T$ by supervisor (7.7) and a `Rotate-Left` task that can be enforced on $T$ by supervisor:

$$(0,0,0.55\pi) \xrightarrow{(1,-1)} (-1.73,0,1.47\pi) \xrightarrow{(1,1.1)} (0,0,0.55\pi) \tag{7.8}$$

Let us now assume that specification $\mathcal{S}$ requires the following sequence of tasks:

$$\begin{array}{l} \texttt{RotateRight},\texttt{RotateRight},\texttt{RotateLeft},\texttt{RotateLeft},\texttt{RotateLeft} \\ \texttt{RotateRight},\texttt{RotateRight},\texttt{RotateLeft},\texttt{RotateLeft},\texttt{RotateLeft} \end{array} \tag{7.9}$$

This would mean that language $\mathcal{S}$ would consist of the single string:

$$\begin{array}{c} (0,0,0.55\pi)(1.73,0,1.47\pi)(0,0,0.55\pi)(1.73,0,1.47\pi)(0,0,0.55\pi)(-1.73,0,1.47\pi) \\ (0,0,0.55\pi)(-1.73,0,1.47\pi)(0,0,0.55\pi)(-1.73,0,1.47\pi)(0,0,0.55\pi)(0,0,0.55\pi) \\ (1.73,0,1.47\pi)(0,0,0.55\pi)(1.73,0,1.47\pi)(0,0,0.55\pi)(-1.73,0,1.47\pi)(0,0,0.55\pi) \\ (-1.73,0,1.47\pi)(0,0,0.55\pi)(-1.73,0,1.47\pi)(0,0,0.55\pi) \end{array}$$

A supervisor enforcing this specification on $T$ can be obtained by simply concatenating the supervisors for the `RotateRight` and `RotateLeft` tasks according to the sequence defined by (7.9). As we mentioned before, the resulting controller is intrinsically hybrid as can also be seen in Figure 7 since the controller needs to count the number of left and right turns in order to determine if the next turn will be a left or a right turn. This counting capability requires discrete memory thereby making the controller hybrid.

This example is a simple metaphor for the more complex behavior that can be synthesized by resorting to the proposed methodology. We emphasize once again that it is the concept of $(\varepsilon,\delta)$-approximate simulation relation that provides this link between supervisory control of finite abstractions and the hybrid controllers acting on the continuous plant.

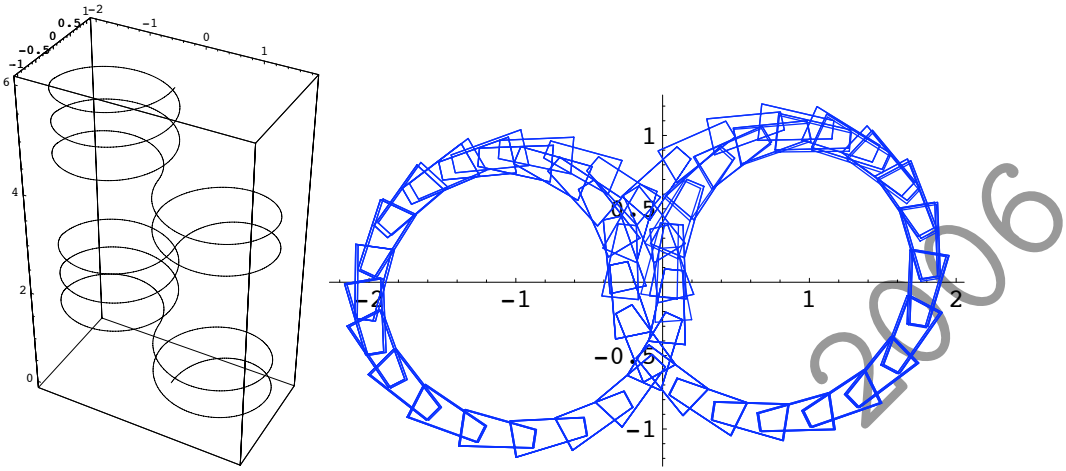

FIGURE 7. Motion of the unicycle when executing a task cosisting of several sub-tasks involving clockwise and counter clockwise rotations described by (7.9). Space is represented horizontally and time vertically on the left figure.

## 8. State-based switching specifications

We conclude this section with another typical example of a specification requiring a hybrid controller. We consider the scenario where it is necessary to employ different control strategies in different regions of the state space. State-based switching is natural in a variety of contexts one such example being fault-recovery procedures triggered when certain state variables exceed predefined thresholds.

Once again we shall use the `RotateRight` and `RotateLeft` tasks as a metaphor for more complex behavior. As a switching rule we shall require `RotateLeft` to be executed when the unicycle is below the horizontal axis and `RotateRight` when it is above. When the unicycle is *on* the horizontal axis both `RotateLeft` and `RotateRight` can be executed. Controllers enforcing state based switching are usually very difficult to analyze since it is difficult to predict which guards will be satisfied and which transitions will be taken as these depend on the continuous state evolution. Such problems do not arise in the proposed methodology since the hybrid controller will make sure that only transitions defined by the discrete supervisor will be executed by the closed loop system. In our particular example a supervisor enforcing the desired specification simply consists of the sub-transition system of $T_\tau(\Sigma)$ defined by the transitions $(p_1, p_2, p_3) \xrightarrow{u} (q_1, q_2, q_3)$ satisfying:

$$\begin{aligned} p_2 \geq 0 \quad &\Longrightarrow \quad u \in \{(1, 1.1), (1, 1)\} \\ p_2 \leq 0 \quad &\Longrightarrow \quad u \in \{(1, -1.1), (1, -1)\} \end{aligned}$$

Three different evolutions are presented in Figure 8. The first was obtained by starting at the initial condition consisting of position $(0, 0.5)$ and orientation $\pi/2$. Although states corresponding to `RotateLeft` are visited during the execution of the symbolic commands issued by the supervisor, the decision on which symbolic command should be executed is always taken above the horizontal axis. The second and third evolutions presented in Figure 8 correspond to an initial condition on the horizontal axis. The different behaviors obtained are a consequence of the switching rule allowing both `RotateLeft` and `RotateRight` tasks to be executed. Although, the closed loop trajectories are not unique, they are completely described by $C \parallel T$.

## 9. Discussion

The proposed methodology for the construction of hybrid controllers relies on two ingredients: the notion of $(\varepsilon, \delta)$-approximate simulation relation; and the possibility of constructing finite sub-transition systems of

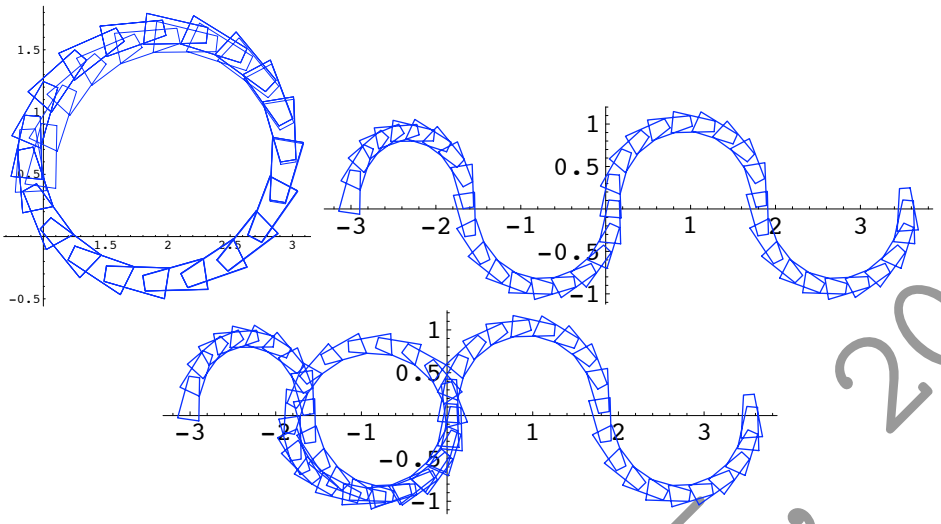


FIGURE 8. Motion of the unicycle when executing a state-switching based specification.

$T_\tau(\Sigma)$. Although we have tried to justify the merit of the presented results by illustrating them on several typical control designs requiring hybrid controllers, the presented results are only sufficient. If we fail to find a controller enforcing the desired specification on a finite sub-transition system $T$ of $T_\tau(\Sigma)$, we cannot conclude anything from Theorem 5.1 regarding the existence of a controller for $T_\tau(\Sigma)$. In order to obtain such converse guarantee one would have to strengthen the $(\varepsilon, \delta)$-approximate simulation $R$ from $T$ to $T_\tau(\Sigma)$ to an approximate bisimulation. The existence of such approximation bisimulation seems the be quite unlikely since the construction of $T$ is done by considering quantized inputs. However, one can still expect, under certain conditions, that some completeness results might hold. In the case of reachability, it is shown in [BMP02] that the reachable set of $T_\tau(\Sigma)$ is described by $T$ up to a certain accuracy that can be made arbitrarily small by using more quantized inputs, when $\Sigma$ belongs to the so called class of chained-form systems. Further research is still needed in oder to understand which other properties of $T_\tau(\Sigma)$ can be reflected on $T$ and how to select the input quanta in order to reflect these properties.

The proposed methodology enforces a constant accuracy $\varepsilon$ on the state set of a $\varepsilon$-regular sub-transition system $T$ by guaranteeing that it is a subset of a lattice $[\mathbb{R}^n]_\chi$ with $\chi$ integrally dividing $\varepsilon$. Although this guarantees a spatially uniform description of the dynamics of $\Sigma$, it also forces the size of $T$ to grow exponentially with $n$. Since the specification may not require a spatially uniform resolution, we can instead construct specification dependent multi-resolution finite abstractions. This kind of finite abstractions are currently being investigated by the author as a lower complexity alternative to the $\varepsilon$-regular sub-transition systems introduced in this paper.



## REFERENCES

[AM97] Panos J. Antsaklis and Anthony N. Michel. *Linear Systems*. McGraw-Hill, 1997.

[Art83] Z. Artstein. Stabilization with relaxed controls. *Nonlinear Analysis, Theory, Methods, and Applications*, 7:1163–1173, 1983.

[BMP02] A. Bicchi, A. Marigo, and B. Piccoli. On the reachability of quantized control systems. *IEEE Transaction on Automatic Control*, 47(4):546–563, April 2002.

[BMP06] A. Bicchi, A. Marigo, and B. Piccoli. Feedback encoding for efficient symbolic control of dynamical systems. *IEEE Transaction on Automatic Control*, 51(6):987– 1002, June 2006.

[BR05] A. Bacciotti and L. Rosier. *Liapunov functions and stability in control theory*. Communications and Control Engineering. Springer-Verlag, 2005.

[CGP99] E. M. Clarke, O. Grumberg, and D. Peled. *Model Checking*. MIT Press, 1999.

[CL99] C. Cassandras and S. Lafortune. *Introduction to discrete event systems*. Kluwer Academic Publishers, Boston, MA, 1999.

[EFP06] M. Egerstedt, E. Frazzoli, and G. J. Pappas, editors. *Special issue on symbolic methods for complex control systems*, volume 51. IEEE Transactions on Automatic Control, July 2006.

[FDF05] E. Frazzoli, M. A. Dahleh, and E. Feron. Maneuver-based motion planning for nonlinear systems with symmetries. *IEEE Transactions on Robotics*, 21(6):1077–1091, 2005.

[GNRR93] Robert L. Grossman, Anil Nerode, Anders P. Ravn, and Hans Rischel, editors. *Hybrid Systems*, volume 736 of *Lecture Notes in Computer Science*. Springer-Verlag, 1993.

[GP05a] A. Girard and G. Pappas. Approximate bisimulations for constrained linear systems. In *Proceedings of the 44th IEEE Conference on Decision and Control*, Seville, Spain, 2005.

[GP05b] A. Girard and G. J. Pappas. Approximate bisimulations for nonlinear dynamical systems. In *Proceedings of the 44th IEEE Conference on Decision and Control*, Seville, Spain, 2005.

[Hen96] T.A. Henzinger. The theory of hybrid automata. In *Proceedings of the 11th Annual IEEE Symposium on Logic in Computer Science*, pages 278–292. IEEE Computer Society Press, 1996.

[KG95] R. Kumar and V.K. Garg. *Modeling and Control of Logical Discrete Event Systems*. Kluwer Academic Publishers, 1995.

[KPS01] T. J. Koo, G. J. Pappas, and S. Sastry. Mode switching synthesis for reachability specifications. In M. D. Di Benedetto and A. Sangiovanni-Vincentelli, editors, *Hybrid Systems: Computation and Control*, volume 2034 of *Lecture Notes in Computer Science*, pages 333–346. Springer-Verlag, 2001.

[LS95] Y. Lin and E.D. Sontag. Control-lyapunov universal formulae for restricted inputs. *Control: Theory and Advanced Technology*, 10:1981–2004, 1995.

[LSW96] Y. Lin, E. Sontag, and Y. Wang. A smooth converse Lyapunov theorem for robust stability. *SIAM Journal on Control and Optimization*, 34:124–160, 1996.

[MRO02] T. Moor, J. Raisch, and S. O'Young. Discrete supervisory control of hybrid systems based on $l$-complete approximations. *Discrete Event Dynamic Systems*, 12(1):83–107, 2002.

[PLLN98] E. Panteley, E. Lefeber, A. Loria, and H. Nijmeijer. Exponential tracking control of a mobile car using a cascaded approach. In *Proceedings of the IFAC Workshop on Motion Control*, pages 221–226, Grenoble, France, September 1998.

[PLPB02] Stefania Pancanti, Laura Leonardi, Lucia Pallottino, and Antonio Bicchi. Optimal control of quantized linear systems. In Claire Tomlin and Mark R. Greenstreet, editors, *Hybrid Systems: Computation and Control*, Lecture Notes in Computer Sience, pages 351–363. Springer-Verlag, 2002.

[Tab06a] Paulo Tabuada. Symbolic control of linear systems based on symbolic subsystems. *IEEE Transactions on Automatic Control, Special issue on symbolic methods for complex control systems*, 51(6):1003–1013, June 2006.

[Tab06b] Paulo Tabuada. Symbolic models for control systems. 2006. Submitted for publication. Available at `http://www.nd.edu/∼ptabuada`.

[TP06] Paulo Tabuada and George J. Pappas. Linear Time Logic control of discrete-time linear systems. *IEEE Transactions on Automatic Control*, 2006. In press, available at `http://www.nd.edu/∼ptabuada`.

Department of Electrical Engineering, 66-147F Engineering IV Building, University of California at Los Angeles, Los Angeles, CA 90095-1594, `http://www.ee.ucla.edu/∼tabuada`

*E-mail address*: `tabuada@ee.ucla.edu`