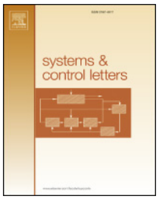
Systems & Control Letters 58 (2009) 94–101

Contents lists available at ScienceDirect

Systems & Control Letters

journal homepage: www.elsevier.com/locate/sysconle



Approximate equivalence and synchronization of metric transition systems

A. Agung Julius [a,*], Alessandro D'Innocenzo [a,b], Maria Domenica Di Benedetto [b], George J. Pappas [a]

[a] *Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia, PA 19104, USA*

[b] *Department of Electrical and Information Engineering, University of L'Aquila, L'Aquila 67040, Italy*

ARTICLE INFO

Article history:
Received 26 June 2006
Received in revised form
24 March 2008
Accepted 1 September 2008
Available online 1 October 2008

Keywords:
Metric transition systems
Approximate equivalence
Bisimulation
Approximate synchronization

ABSTRACT

In this paper, we consider metric transition systems which are transition systems equipped with metrics for observation and synchronization labels. The existence of metrics leads to the introduction of two new concepts, (i) (ϵ, δ)-approximate (bi)simulation of transition systems and (ii) approximate synchronization of transition systems.

We show that the notion of (ϵ, δ)-approximate (bi)simulation can be thought of as a generalization or relaxation of the earlier work on δ-approximate (bi)simulation by Girard and Pappas. We demonstrate the link between reachability verification and approximate (bi)simulation, and we also provide a characterization of (bi)simulation relations using a tool similar to the (bi)simulation function.

Approximate synchronization can be thought of as a generalization of synchronization of transition systems in the usual sense. In fact, the usual synchronization and interleaving synchronization are two special cases of the notion of approximate synchronization developed in this paper. Furthermore, we present a result on the compositional properties of the approximate (bi)simulation with respect to the approximate synchronization.

In addition to the theoretical presentation of approximate bisimulation and synchronization, we also discuss the application of this framework in analyzing control systems over digital communication networks.

1. Introduction

System abstraction is an important tool for analyzing complex systems. With abstraction, the complexity of the systems (typically associated with the size of the state space) can be decreased, resulting in lesser computational cost in the analysis [1].

System abstraction is traditionally associated with system equivalence, in the sense abstraction of a complex system amounts to constructing an equivalent system with lesser complexity. The equivalence guarantees that the results of analysis performed on the less complex system can be carried over into the complex system. Language equivalence and bisimulation (and its variants) are two of the most commonly used notions of system equivalence for systems abstraction [2–5].

Requiring the abstraction to be equivalent to the original system is sometimes too restrictive. Researchers have been working to develop more relaxed abstraction theories that enable further model simplification. One of the ideas is to relax the requirement that the abstraction is equivalent to the original system, and replace it with a requirement that the abstraction is only *approximately* equal to the original system (see, e.g. [6–8]). The key ingredient to these theories is a metric that can quantify the distance between the system and its abstraction, and hence the quality of the abstraction. In this paper, we start with the idea of approximate bisimulation of transition systems as developed recently in [8] and previous related papers by the authors.

Although we set our discussion in the framework of transition systems, the applicability of the results is not restricted to discrete event systems. In fact, many interesting classes of continuous and discrete time dynamical systems can be embedded as transition systems [3], and abstraction can be studied as abstraction of the transition system [9,2].

This paper presents some results that have been reported earlier in our conference paper [10]. Here, we extend the earlier work on approximate bisimulation [8] by introducing a pseudo-metric on set of labels of the transition systems. Having a notion of distance in the set of labels enables us to define a notion of *approximate synchronization*. Loosely speaking, by approximate synchronization we mean allowing systems to synchronize not only on the same label, but also with labels that are close. Approximate synchronization can be thought of as a relaxation of the notion of synchronization in the usual sense.

Contrary to *exact* notions of synchronization for traditional transition systems, *approximate* synchronization is a much more

[*] Corresponding author. Tel.: +1 215 7463161; fax: +1 215 5732048.
E-mail addresses: agung@seas.upenn.edu (A.A. Julius), adinnoce@ing.univaq.it (A. D'Innocenzo), dibenede@ing.univaq.it (M.D. Di Benedetto), pappasg@ee.upenn.edu (G.J. Pappas).

0167-6911/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.sysconle.2008.09.001

natural and robust concept especially when different systems need to synchronize over temporal or spatial variables where exact synchronization may be too restrictive or not robust. For example, random communication delays between geographically distant subsystems requires a notion of synchronization that does not require strict simultaneity. Thus, approximation in the synchronization can be related to tolerance in timing. Verification of systems with relaxed timing is an active research area. There has been some work in the direction of developing a new metric to quantify distance in the timing-relaxed way [11–13]. Similarly, in the area of multi-agent control, if spatial information about the agents is captured on the labels, then approximate synchronization can be used as a compact and natural way of representing communication (or cooperation) range. Here, labels that are close correspond to agents that are spatially close.

In this paper, we first extend the notion of approximate (bi)simulation of metric transition systems, by introducing a pseudometric on the set of labels. We elucidate the relation between our work and an earlier work by Girard and Pappas [8], and we also provide a way to characterize approximate (bi)simulation relations by using an extension of the (bi)simulation functions. We then introduce the notion of approximate synchronization and present a result that shows that approximate (bi)simulation is compositional with respect to approximate synchronization. Even further, we show that this result also extends to the case where clusters of transition systems (called composite transition systems) are synchronized. We then show that the notion of approximate synchronization is useful in analyzing systems with control over communication networks [14–16]. The transmission of uncertainty corresponding to measurement discretization can be naturally modeled as approximate synchronization.

2. Metric transition systems

In this section, we extend the idea of approximate simulation and bisimulation, by introducing a pseudometric on the set of labels of the transition systems.

We define a transition system as a six tuple $T = (Q, \Sigma, \rightarrow, Q^0, \Pi, \langle\cdot\rangle)$, where Q is the set of states, Σ is the set of labels, $\rightarrow \subset Q \times \Sigma \times Q$ is a set of transitions, Q^0 is the set of initial states, Π is the set of possible observations, $\langle\cdot\rangle : Q \rightarrow \Pi$ is the observation map. The transition system is called a *metric transition system* if the set of observations Π and labels Σ are equipped with pseudometrics d_Π and d_Σ respectively.[1] A pseudometric is a metric that allows zero distance between different points.

Notation 1. *In this paper we shall use the following notations.*

$$\forall \varepsilon \geq 0,\ \sigma \in \Sigma, \quad B_\varepsilon(\sigma) := \{\sigma' \in \Sigma \mid d_\Sigma(\sigma, \sigma') \leq \varepsilon\},$$

$$\forall \varepsilon \geq 0,\ z \in \Pi, \quad B_\varepsilon(z) := \{z' \in \Pi \mid d_\Pi(z, z') \leq \varepsilon\},$$

$$\forall q \in Q,\ S \subset \Sigma, \quad \Omega(q, S) := \{q' \in Q \mid \exists \sigma \in S, q \xrightarrow{\sigma} q'\}.$$

Definition 2. Given two transition systems $T_i = (Q_i, \Sigma, \rightarrow_i, Q_i^0, \Pi, \langle\cdot\rangle_i)$, $i = 1, 2$. A relation $\mathcal{R} \subset Q_1 \times Q_2$ is a (ε, δ)-**approximate simulation** of T_1 by T_2, $\delta, \varepsilon \geq 0$, if for any $(q_1, q_2) \in \mathcal{R}$,

(i) $d_\Pi(\langle q_1\rangle_1, \langle q_2\rangle_2) \leq \delta$,

(ii) For any $a \in \Sigma, q_1' \in Q_1$ such that $q_1 \xrightarrow{a} q_1'$, there exists an $a' \in \Sigma$ and $q_2' \in Q_2$ such that

$$d_\Sigma(a, a') \leq \varepsilon, \qquad q_2 \xrightarrow{a'} q_2', \quad (q_1', q_2') \in \mathcal{R}.$$

Notice that ε and δ represent the precision in the approximation in terms of the synchronization labels and the observations respectively. A $(0, \delta)$-approximate simulation relation is a δ-approximate simulation in the sense of [8], which requires exact synchronization. A $(0, 0)$-approximate simulation relation is a classical exact simulation relation with exact synchronization. Furthermore, the following proposition reveals the partial ordering of approximate simulation relations.

Proposition 3. *Given two transition systems $T_i = (Q_i, \Sigma, \rightarrow_i, Q_i^0, \Pi, \langle\cdot\rangle_i)$, $i = 1, 2$. Let $\mathcal{R} \subset Q_1 \times Q_2$. For any $\delta' \geq \delta \geq 0$ and $\varepsilon' \geq \varepsilon \geq 0$ the following statements hold.*

(i) *If $\mathcal{R}$ is a (ε, δ)-approximate simulation of T_1 by T_2 then it is also a (ε', δ)-approximate simulation of T_1 by T_2.*

(ii) *If $\mathcal{R}$ is a (ε, δ)-approximate simulation of T_1 by T_2 then it is also a (ε, δ')-approximate simulation of T_1 by T_2.*

A (ε, δ)-approximate bisimulation relation can be defined as a symmetric version of a (ε, δ)-approximate simulation, as follows.

Definition 4. Given two transition systems $T_i = (Q_i, \Sigma, \rightarrow_i, Q_i^0, \Pi, \langle\cdot\rangle_i)$, $i = 1, 2$. A relation $\mathcal{R} \subset Q_1 \times Q_2$ is a (ε, δ)-**approximate bisimulation** between T_1 and T_2, $\delta, \varepsilon \geq 0$, if $\mathcal{R}$ is both a (ε, δ)-**approximate simulation** of T_1 by T_2 and a (ε, δ)-**approximate simulation** of T_2 by T_1.

Corollary 5. *Given two transition systems $T_i = (Q_i, \Sigma, \rightarrow_i, Q_i^0, \Pi, \langle\cdot\rangle_i)$, $i = 1, 2$. Let $\mathcal{R} \subset Q_1 \times Q_2$. For any $\delta' \geq \delta \geq 0$ and $\varepsilon' \geq \varepsilon \geq 0$ the following statements hold.*

(i) *If $\mathcal{R}$ is a (ε, δ)-approximate bisimulation between T_1 and T_2 then it is also a $(\varepsilon', \delta)-$ approximate bisimulation between T_1 and T_2.*

(ii) *If $\mathcal{R}$ is a (ε, δ)-approximate bisimulation between T_1 and T_2 then it is also a (ε, δ')-approximate bisimulation between T_1 and T_2.*

Approximate simulation and bisimilarity between transition systems are characterized as follows.

Definition 6. Given two transition systems $T_i = (Q_i, \Sigma, \rightarrow_i, Q_i^0, \Pi, \langle\cdot\rangle_i)$, $i = 1, 2$. We say that T_2 **simulates** T_1 **with precision** (ε, δ) if there exists $\mathcal{R}$, a (ε, δ)-approximate simulation of T_1 by T_2, such that for every $q_1^0 \in Q_1^0$, there exists a $q_2^0 \in Q_2^0$ such that $(q_1^0, q_2^0) \in \mathcal{R}$. This relation is denoted by $T_1 \preceq_{\varepsilon,\delta} T_2$.

Definition 7. Given two transition systems $T_i = (Q_i, \Sigma, \rightarrow_i, Q_i^0, \Pi, \langle\cdot\rangle_i)$, $i = 1, 2$. We say that T_1 and T_2 **are approximately bisimilar with precision** (ε, δ) if there exists $\mathcal{R}$, a (ε, δ)-approximate bisimulation between T_1 and T_2, such that

(i) for every $q_1^0 \in Q_1^0$, there exists a $q_2^0 \in Q_2^0$ such that $(q_1^0, q_2^0) \in \mathcal{R}$,

(ii) for every $q_2^0 \in Q_2^0$, there exists a $q_1^0 \in Q_1^0$ such that $(q_1^0, q_2^0) \in \mathcal{R}$.

This relation is denoted by $T_1 \approx_{\varepsilon,\delta} T_2$.

The concept of (ε, δ)-approximate bisimulation is illustrated in Fig. 1. Based on Proposition 3 and Corollary 5, we can derive the following proposition.

Proposition 8. *Given two transition systems T_1 and T_2. For any $\delta' \geq \delta \geq 0$ and $\varepsilon' \geq \varepsilon \geq 0$. the following statements hold.*

(i) *If $T_1 \preceq_{\varepsilon,\delta} T_2$ then $T_1 \preceq_{\varepsilon',\delta} T_2$.*

(ii) *If $T_1 \preceq_{\varepsilon,\delta} T_2$ then $T_1 \preceq_{\varepsilon,\delta'} T_2$.*

(iii) *If $T_1 \approx_{\varepsilon,\delta} T_2$ then $T \approx_{\varepsilon',\delta} T_2$.*

(iv) *If $T_1 \approx_{\varepsilon,\delta} T_2$ then $T \approx_{\varepsilon,\delta'} T_2$.*

[1] From this point on we assume that all transition systems are metric transition systems, hence we do not distinguish between the two notions.

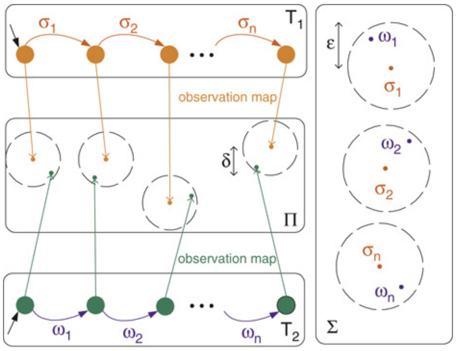


Fig. 1. An illustration of approximate (bi)simulation with metricized labels between two transition systems T_1 and T_2. The outputs of related states must be distanced by at most δ. The two transition systems does not have to synchronize with the same labels. Rather, the labels can be at most ε apart.

We can also show that the approximate bisimulation relations possess some kind of transitivity property, as stated in the following proposition.

Proposition 9. *Given three transition systems T_1, T_2 and T_3. For any $\delta, \delta' \geq 0$ and $\varepsilon, \varepsilon' \geq 0$. the following statements hold.*

(i) *If $T_1 \preceq_{\varepsilon,\delta} T_2$ and $T_2 \preceq_{\varepsilon',\delta'} T_3$, then $T_1 \preceq_{\varepsilon+\varepsilon',\delta+\delta'} T_3$.*
(ii) *If $T_1 \approx_{\varepsilon,\delta} T_2$ and $T_2 \approx_{\varepsilon',\delta'} T_3$, then $T_1 \approx_{\varepsilon+\varepsilon',\delta+\delta'} T_3$.*

The relation between the reachable sets (of observations) of the transition systems and the approximate (bi)simulation is summarized as follows.

Definition 10. Given a transition system $T = (Q, \Sigma, \rightarrow, Q^0, \Pi, \langle\cdot\rangle)$, an observation $y \in \Pi$ belongs to the reachable set of the transition system $\mathcal{R}(T)$ if there exists an initial state $x_0 \in Q^0$ and a trajectory starting from x_0,

$$x_0 \xrightarrow{a_1} x_1 \xrightarrow{a_2} \cdots \xrightarrow{a_n} x_n,$$

such that $\langle x_n\rangle = y$.

Theorem 11. *Given two transition systems T_1 and T_2, the following relations hold.*

(i) *$T_1 \preceq_{\varepsilon,\delta} T_2$ for some $\varepsilon, \delta \geq 0$ implies*

$$\sup_{y_1\in\mathcal{R}(T_1)} \inf_{y_2\in\mathcal{R}(T_2)} d_\Pi(y_1, y_2) \leq \delta. \tag{1}$$

(ii) *$T_1 \approx_{\varepsilon,\delta} T_2$ for some $\varepsilon, \delta \geq 0$ implies*

$$\max\left(\sup_{y_1\in\mathcal{R}(T_1)} \inf_{y_2\in\mathcal{R}(T_2)} d_\Pi(y_1, y_2),\right.$$
$$\left.\sup_{y_2\in\mathcal{R}(T_2)} \inf_{y_1\in\mathcal{R}(T_1)} d_\Pi(y_1, y_2)\right) \leq \delta. \tag{2}$$

Proof. (i) We need to show that if $T_1 \preceq_{\varepsilon,\delta} T_2$ for some $\varepsilon, \delta \geq 0$, then for any $y_1 \in \mathcal{R}(T_1)$, there exists a $y_2 \in \mathcal{R}(T_2)$ such that $d_\Pi(y_1, y_2) \leq \delta$. There exists a trajectory of T_1 starting from $x_{1,0} \in Q_1^0$,

$$x_{1,0} \xrightarrow{a_1} x_{1,1} \xrightarrow{a_2} \cdots \xrightarrow{a_n} x_{1,n},$$

such that $\langle x_{1,n}\rangle_1 = y_1$. Suppose that $\mathcal{R} \subset Q_1 \times Q_2$ is a (ε, δ)-approximate simulation of T_1 by T_2. By the definition of approximate simulation, we can infer that there exists a trajectory of T_2 starting from a $x_{1,0} \in Q_1^0$,

$$x_{2,0} \xrightarrow{a'_1} x_{2,1} \xrightarrow{a'_2} \cdots \xrightarrow{a'_n} x_{2,n},$$
$$(x_{1,i}, x_{2,i}) \in \mathcal{R}.$$

Denote $\langle x_{2,n}\rangle_2 = y_2$. It follows from the definition of approximate simulation that $d_\Pi(y_1, y_2) \leq \delta$.

(ii) Analogous to part (i). □

The application of approximate (bi)simulation as an aid in safety verification of dynamical systems is presented in [8]. Given a dynamical system embedded as a transition system T_1, another dynamical system embedded as a transition system T_2 is constructed such that $T_1 \preceq_{0,\delta} T_2$. The system corresponding with T_2 is simpler, in the sense of smaller state space. The reachable set of T_1 can thus be approximated with that of T_2 with precision δ.

The introduction of a metric for the labels can be thought of as a relaxation that allows for tighter bound in the approximation of the reachable set. This is illustrated on the continuous time dynamical system

$$\frac{\mathrm{d}x}{\mathrm{d}t} = f(x, u), \qquad y = h(x), \tag{3}$$

$$x \in \mathcal{X}, \quad x(0) \in \mathcal{X}^0, \quad u \in \mathcal{U}, \quad y \in \mathcal{Y} \subset \mathbb{R}^m. \tag{4}$$

This system can be embedded into a transition system $T = (Q, \Sigma, \rightarrow, Q^0, \Pi, \langle\cdot\rangle)$, where $Q = \mathcal{X}$, $\Sigma = \mathbb{R}_+$, $Q^0 = \mathcal{X}^0$, $\Pi = \mathcal{Y}$, $\langle x\rangle = h(x)$.

$$\rightarrow \subset \mathbb{R}^n \times \mathbb{R}_+ \times \mathbb{R}^n,$$

such that $x \xrightarrow{\tau} x'$ if and only if there exist $x_0 \in \mathcal{X}^0$ and $u : [0, \tau] \rightarrow \mathcal{U}$ such that the continuous solution to the differential equation

$$\frac{\mathrm{d}x}{\mathrm{d}t} = f(x, u), \qquad x(0) = x_0 \tag{5}$$

satisfies $x(\tau) = x'$. Alternatively stated, $x \xrightarrow{\tau} x'$ if and only if there is an input that can drive the system starting at the initial state x to the state x' in τ time unit. The set of labels and observations, $\mathbb{R}_+$ and $\mathcal{Y} \subset \mathbb{R}^m$ are equipped with the Euclidian distance $\|\cdot\|$. With this interpretation of transition system, the distance between two labels corresponds to the difference in the timing, in which the terminal state is reached. Therefore, in this case, approximate synchronization corresponds to relaxation in the timing. The following implication can be proven.

Proposition 12. *Given two transition systems T_1 and T_2, the following relations hold.*

(i) *$T_1 \preceq_{\infty,\delta} T_2$ for some $\delta \geq 0$ if and only if*

$$\sup_{y_1\in\mathcal{R}(T_1)} \inf_{y_2\in\mathcal{R}(T_2)} d_\Pi(y_1, y_2) \leq \delta. \tag{6}$$

(ii) *$T_1 \approx_{\infty,\delta} T_2$ for some $\delta \geq 0$ if and only if*

$$\max\left(\sup_{y_1\in\mathcal{R}(T_1)} \inf_{y_2\in\mathcal{R}(T_2)} d_\Pi(y_1, y_2),\right.$$
$$\left.\sup_{y_2\in\mathcal{R}(T_2)} \inf_{y_1\in\mathcal{R}(T_1)} d_\Pi(y_1, y_2)\right) \leq \delta. \tag{7}$$

Therefore, by relaxing the requirement on the timing, we can get a result stronger than Theorem 11. A different treatment of a similar idea is presented in [12].

3. Extension of the (bi)simulation functions

In this section we discuss the extension of the concept of (bi)simulation functions [8], to deal with metrics on synchronization labels.

Definition 13. Given two transition systems $T_i = (Q_i, \Sigma, \rightarrow_i, Q_i^0, \Pi, \langle\cdot\rangle_i)$, $i = 1, 2$. A function $\phi : Q_1 \times Q_2 \rightarrow \mathbb{R}_+ \cup \{\infty\}$ is an ε- simulation function of T_1 by T_2 if for any $q_1 \in Q_1$ and $q_2 \in Q_2$,

$$\phi(q_1, q_2) \geq d_\Pi(\langle q_1\rangle_1, \langle q_2\rangle_2), \tag{8a}$$

$$\phi(q_1, q_2) \geq \sup_{q_1 \xrightarrow{\sigma} q_1'} \inf_{q_2 \xrightarrow{B_\varepsilon(\sigma)} q_2'} \phi(q_1', q_2'). \tag{8b}$$

Notice that an ε-simulation function can be thought of as a relaxed version of bisimulation function in the sense of [8]. In order the match a transition of T_1, T_2 does not necessarily perform a transition with the same label. Rather, T_2 can choose any move, as long as its label is at most ε apart from that of T_1. A bisimulation function in the sense of [8] is a 0- simulation function.

Proposition 14. *Given two transition systems T_1 and T_2. If ϕ is an ε-simulation function of T_1 by T_2, for some $\varepsilon \geq 0$, then it is also an ε'-simulation function of T_1 by T_2, for any $\varepsilon' \geq \varepsilon \geq 0$.*

Definition 15. Given two transition systems $T_i = (Q_i, \Sigma, \rightarrow_i, Q_i^0, \Pi, \langle\cdot\rangle_i)$, $i = 1, 2$. A function $\phi : Q_1 \times Q_2 \rightarrow \mathbb{R}_+ \cup \{\infty\}$ is an ε-bisimulation function between T_1 and T_2 if it is both an ε- simulation function of T_1 by T_2 and an ε- simulation function of T_2 by T_1. That is, for any $q_1 \in Q_1$ and $q_2 \in Q_2$,

$$\phi(q_1, q_2) \geq d_\Pi(\langle q_1\rangle_1, \langle q_2\rangle_2), \tag{9}$$

$$\phi(q_1, q_2) \geq \sup_{q_1 \xrightarrow{\sigma} q_1'} \inf_{q_2 \xrightarrow{B_\varepsilon(\sigma)} q_2'} \phi(q_1', q_2'), \tag{10}$$

$$\phi(q_1, q_2) \geq \sup_{q_2 \xrightarrow{\sigma} q_2'} \inf_{q_1 \xrightarrow{B_\varepsilon(\sigma)} q_1'} \phi(q_1', q_2'). \tag{11}$$

The relation between (bi)simulation functions and approximate (bi)simulation can be summarized in the following theorems.

Theorem 16. *Given two transition systems T_1 and T_2. If ϕ is an ε-simulation function of T_1 by T_2, for some $\varepsilon \geq 0$, then for any $\delta \geq 0$, its δ-level set,*

$$\mathcal{R}_\delta(\phi) := \{(q_1, q_2) | \phi(q_1, q_2) \leq \delta\},$$

*is a (ε, δ)-**approximate simulation** of T_1 by T_2.*

Proof. Take any $(q_1, q_2) \in \mathcal{R}_\delta(\phi)$, by (8a) we have that,

$$d_\Pi(\langle q_1\rangle_1, \langle q_2\rangle_2) \leq \delta. \tag{12}$$

For any $\sigma \in \Sigma$ such that $q_1 \xrightarrow{\sigma} q_1'$, (8b) implies the existence of $q_2' \in Q_2$ and $\sigma' \in \Sigma$ such that

$$q_2 \xrightarrow{\sigma'} q_2', d_\Sigma(\sigma, \sigma') \leq \varepsilon,$$
$$\phi(q_1', q_2') \leq \delta.$$

Therefore $(q_1', q_2') \in \mathcal{R}_\delta(\phi)$. □

Theorem 17. *Given two transition systems T_1 and T_2. If ϕ is an ε-bisimulation function between T_1 and T_2, for some $\varepsilon \geq 0$, then for any $\delta \geq 0$, its δ-level set,*

$$\mathcal{R}_\delta(\phi) := \{(q_1, q_2) | \phi(q_1, q_2) \leq \delta\},$$

*is a (ε, δ)-**approximate bisimulation** between T_1 and T_2.*

Proof. Analogous to that of Theorem 16. □

Generally speaking, the characterization of an ε-simulation function is similar to that of a simulation function when there is nondeterminism in the system.

4. Approximate synchronization

Typically, synchronization of transition systems is formalized by (exact) synchronization of the labels. In this section, we introduce the idea of approximate synchronization. Loosely speaking, the idea is to let two transition systems synchronize using labels that are close, but not necessarily equal. Closeness is defined in the sense of the a pseudometric in the set of labels.

4.1. Approximate synchronization of transition systems

Definition 18. Given two transition systems $T_i = (Q_i, \Sigma, \rightarrow_i, Q_i^0, \Pi_i, \langle\cdot\rangle_i)$, $i = 1, 2$. The **approximate synchronization** operator $\|_\varepsilon$, $\varepsilon \geq 0$, acting on the two systems results in another transition system

$$T := T_1 \|_\varepsilon T_2, \tag{13}$$

where $T = (Q_1 \times Q_2, \Sigma \times \Sigma, \rightarrow, Q_1^0 \times Q_2^0, \Pi_1 \times \Pi_2, \langle\cdot\rangle)$. The transition relation $\rightarrow$ is such that $(q_1, q_2) \xrightarrow{\sigma,\sigma'} (q_1', q_2')$ iff $q_1 \xrightarrow{\sigma}_1 q_1'$, $q_2 \xrightarrow{\sigma'}_2 q_2'$, $d_\Sigma(\sigma, \sigma') \leq \varepsilon$. The observation map $\langle\cdot\rangle$ is defined as

$$\langle(q_1, q_2)\rangle := (\langle q_1\rangle_1, \langle q_2\rangle_2). \tag{14}$$

Notice that the composite transition system $T = T_1 \|_\varepsilon T_2$ is quite different from the transition systems T_1 and T_2, in the following sense:

- The observation space of T is a product of those of T_1 and T_2.
- The set of labels of T is also a product of those of T_1 and T_2.

We need to define a notion of pseudometric for an observation space that is a product of two observation spaces, and similarly for the set of labels.

Definition 19. The observation space $\Pi_1 \times \Pi_2$ is equipped with the following pseudometric.

$$d_\Pi\left((\pi_1, \pi_2), (\pi_1', \pi_2')\right) := d_{\Pi_1}(\pi_1, \pi_1') + d_{\Pi_2}(\pi_2, \pi_2'). \tag{15}$$

The set of labels $\Sigma \times \Sigma$ is equipped with the following pseudometric.

$$d_{\Sigma^2}\left((\sigma_1, \sigma_2), (\sigma_1', \sigma_2')\right) := \max_{i=1,2} \max_{j=1,2} d_\Sigma(\sigma_i, \sigma_j'). \tag{16}$$

Generally, we can define the pseudometric d_Π on $\Pi_1 \times \Pi_2$ differently. The only requirement that needs to be satisfied is that d_Π should coincide with d_{Π_1} and d_{Π_2} when used to measure distances in Π_1 and Π_2, respectively.

$$d_\Pi\left((\pi_1, \pi_2), (\pi_1', \pi_2)\right) = d_{\Pi_1}(\pi_1, \pi_1'), \quad \forall \pi_2 \in \Pi_2, \tag{17}$$

$$d_\Pi\left((\pi_1, \pi_2), (\pi_1, \pi_2')\right) = d_{\Pi_2}(\pi_2, \pi_2'), \quad \forall \pi_1 \in \Pi_1. \tag{18}$$

The pseudometric on $\Sigma \times \Sigma$ is the largest pairwise distance between a label in the first composite transition system and the second composite transition system. This can be interpreted as the worst synchrony between the components of the two systems. Approximate synchronization can be thought of as a relaxed version of the exact synchronization. Exact synchronization is a special case of approximate synchronization $\|_\varepsilon$, namely when $\varepsilon = 0$. Obviously, the larger the tolerance (ε) in the synchronization is, the more flexible the two systems can evolve with respect to each other. If we assume that the transition systems have stutter transition [17], the case when $\varepsilon = \infty$ can be thought of as the situation when the executions of the two transition systems are interleaving. The executions can interleave because one transition system can always synchronize with the stutter transition of the other.

The fact that defined notion of approximate synchronization is a relaxation of the traditional notion of synchronization is reflected in the following proposition.

Proposition 20. *Given two transition systems $T_i = (Q_i, \Sigma, \rightarrow_i, Q_i^0, \Pi, \langle\cdot\rangle_i)$, $i = 1, 2$. For any $\varepsilon, \varepsilon' \geq 0$, the following holds.*

$$T_1 \parallel_\varepsilon T_2 \preceq_{0,0} T_1 \parallel_{\varepsilon+\varepsilon'} T_2. \tag{19}$$

This proposition tells us that a synchronization with higher tolerance always simulates one with less tolerance.

It is already known that the notion of approximate (bi)simulation has a compositional property [8] with respect to exact synchronization. In the following we shall show that the extended notion of approximate (bi)simulation that we present in this paper also has a compositional property with respect to approximate synchronization.

Theorem 21. *Consider transition systems T_1, T_2, T_1' and T_2'. Suppose that the transition systems T_1 and T_1' have observation space Π_1, while T_2 and T_2' have observation space Π_2. Moreover we assume that all of them share the same set of labels Σ. If $T_1 \preceq_{\varepsilon_1,\delta_1} T_1'$ and $T_2 \preceq_{\varepsilon_2,\delta_2} T_2'$, then for any $\varepsilon \geq 0$,*

$$T_1 \parallel_\varepsilon T_2 \preceq_{\varepsilon+\max(\varepsilon_1,\varepsilon_2),\delta_1+\delta_2} T_1' \parallel_{\varepsilon+\varepsilon_1+\varepsilon_2} T_2'. \tag{20}$$

Proof. Denote

$$T := T_1 \parallel_\varepsilon T_2, T' := T_1' \parallel_{\varepsilon+\varepsilon_1+\varepsilon_2} T_2'. \tag{21}$$

Since $T_1 \preceq_{\varepsilon_1,\delta_1} T_1'$ and $T_2 \preceq_{\varepsilon_2,\delta_2} T_2'$, there exist appropriate approximate simulation relations $\mathcal{R}_1 \subset Q_1 \times Q_1'$ and $\mathcal{R}_2 \subset Q_2 \times Q_2'$ (see Definition 6). We define $\mathcal{R} \subset (Q_1 \times Q_2) \times (Q_1' \times Q_2')$ as follows.

$$\left((q_1, q_2), (q_1', q_2')\right) \in \mathcal{R} :\Leftrightarrow$$
$$(q_1, q_1') \in \mathcal{R}_1 \text{and } (q_2, q_2') \in \mathcal{R}_2.$$

We are going to prove that $\mathcal{R}$ is a $(\varepsilon + \max(\varepsilon_1, \varepsilon_2), \delta_1 + \delta_2)$-approximate simulation of T by T'. Take any $\left((q_1, q_2), (q_1', q_2')\right) \in \mathcal{R}$.

$$d_\Pi\left(\left(\langle q_1\rangle_1, \langle q_2\rangle_2\right), \left(\langle q_1'\rangle_{1'}, \langle q_2'\rangle_{2'}\right)\right)$$
$$= d_{\Pi_1}(\langle q_1\rangle_1, \langle q_1'\rangle_{1'}) + d_{\Pi_2}(\langle q_1\rangle_2, \langle q_1'\rangle_{2'}) \quad \leq \delta_1 + \delta_2. \tag{22}$$

The inequality is due to the fact that $(q_i, q_i') \in \mathcal{R}_i$, $i = 1, 2$.

For any $\alpha, \beta \in \Sigma$ and $(\tilde{q}_1, \tilde{q}_2) \in Q_1 \times Q_2$ such that

$$d_\Sigma(\alpha, \beta) \leq \varepsilon, \quad (q_1, q_2) \overset{\alpha,\beta}{\rightarrow}_T (\tilde{q}_1, \tilde{q}_2),$$

we need to show that there exist $\alpha', \beta' \in \Sigma$ and $(\tilde{q}_1', \tilde{q}_2') \in Q_1' \times Q_2'$ such that

$$d_\Sigma(\alpha', \beta') \leq \varepsilon + \varepsilon_1 + \varepsilon_2, \quad (q_1', q_2') \overset{\alpha',\beta'}{\rightarrow}_{T'} (\tilde{q}_1', \tilde{q}_2'),$$
$$d_{\Sigma^2}\left((\alpha, \beta), (\alpha', \beta')\right) \leq \varepsilon + \max(\varepsilon_1, \varepsilon_2),$$
$$\left((\tilde{q}_1, \tilde{q}_2), (\tilde{q}_1', \tilde{q}_2')\right) \in \mathcal{R}.$$

Because $(q_i, q_i') \in \mathcal{R}_i$, $i = 1, 2$, we know that there exist $\alpha', \beta' \in \Sigma$ and $(\tilde{q}_1', \tilde{q}_2') \in Q_1' \times Q_2'$ such that

$$d_\Sigma(\alpha, \alpha') \leq \varepsilon_1, q_1' \overset{\alpha'}{\rightarrow}_{T_1'} \tilde{q}_1', (\tilde{q}_1, \tilde{q}_1') \in \mathcal{R}_1,$$

$$d_\Sigma(\beta, \beta') \leq \varepsilon_2, q_2' \overset{\beta'}{\rightarrow}_{T_2'} \tilde{q}_2', (\tilde{q}_2, \tilde{q}_2') \in \mathcal{R}_2.$$

It follows immediately that

$$\left((\tilde{q}_1, \tilde{q}_2), (\tilde{q}_1', \tilde{q}_2')\right) \in \mathcal{R}.$$

From the triangular inequality, we obtain

$$\begin{aligned} d_\Sigma(\alpha', \beta') &\leq d_\Sigma(\alpha, \beta) + d_\Sigma(\alpha, \alpha') + d_\Sigma(\beta, \beta'), \\ &\leq \varepsilon + \varepsilon_1 + \varepsilon_2, \end{aligned}$$

and therefore $(q_1', q_2') \overset{\alpha',\beta'}{\rightarrow}_{T'} (\tilde{q}_1', \tilde{q}_2')$. Furthermore,

$$\max_{i\in\{\alpha,\beta\}} \max_{j\in\{\alpha',\beta'\}} d_\Sigma(i, j) \leq \varepsilon + \max(\varepsilon_1, \varepsilon_2).$$

Hence

$$d_{\Sigma^2}\left((\alpha, \beta), (\alpha', \beta')\right) \leq \max(\varepsilon_1, \varepsilon_2).$$

Finally, we need to show that for any $(q_1^0, q_2^0) \in Q_1^0 \times Q_2^0$ there exists $(q_1'^0, q_2'^0) \in Q_1'^0 \times Q_2'^0$ such that $\left((q_1^0, q_2^0), (q_1'^0, q_2'^0)\right) \in \mathcal{R}$. This fact is a direct consequence of $\mathcal{R}_1$ and $\mathcal{R}_2$ being the approximate simulation relations that define $T_1 \preceq_{\varepsilon_1,\delta_1} T_1'$ and $T_2 \preceq_{\varepsilon_2,\delta_2} T_2'$. □

This result can be extended to approximate bisimulation, as follows.

Theorem 22. *Given transition systems T_1, T_2, T_1' and T_2'. Suppose that the transition systems T_1 and T_1' have observation space Π_1, while T_2 and T_2' have observation space Π_2. Moreover we assume that all of them share the same set of labels Σ. If $T_1 \approx_{\varepsilon_1,\delta_1} T_1'$ and $T_2 \approx_{\varepsilon_2,\delta_2} T_2'$, then for any $\varepsilon \geq 0$,*

$$T_1 \parallel_\varepsilon T_2 \approx_{\varepsilon+\max(\varepsilon_1,\varepsilon_2),\delta_1+\delta_2} T_1' \parallel_{\varepsilon+\varepsilon_1+\varepsilon_2} T_2'. \tag{23}$$

Proof. Analogous to that of Theorem 21. □

Notice that when $\varepsilon = \varepsilon_1 = \varepsilon_2 = 0$, Theorems 21 and 22 are reduced to the already known compositionality properties of the approximate (bi)simulation relation in [8].

4.2. Composite transition systems

As explained in the previous subsection, the result of approximately synchronizing two transition systems is a kind of composite transition systems, whose transitions are labeled by a pair of labels. It is quite straightforward to generalize this idea, for example if we want to have several transition systems synchronizing. In this subsection, we formalize this idea and make it possible to discuss approximate synchronization of two (or more) composite transition systems.

Definition 23. Given a set of labels Σ, a **composite transition system** $T = (Q, \Sigma^n, \rightarrow, Q^0, \Pi, \langle\cdot\rangle)$ is a transition system with a set of labels Σ^n, $1 < n \in \mathbb{N}$. The number n is called the **multiplicity** of the composite transition systems.

Before we proceed to define approximate synchronization of composite transition systems (possibly with different multiplicities), we need to define a notion of distance between elements in Σ^n and Σ^m, where n and m are not necessarily equal.

Definition 24. Given $\sigma \in \Sigma^n$ and $\omega \in \Sigma^m$, we define the distance between σ and ω as

$$d_{\Sigma^*}(\sigma, \omega) = d_{\Sigma^*}(\omega, \sigma) := \max_{i=1,\ldots,n} \max_{j=1,\ldots,m} d_\Sigma(\sigma_i, \omega_j).$$

Definition 25. Given two composite transition systems $T_i = (Q_i, \Sigma^{n_i}, \rightarrow_i, Q_i^0, \Pi_i, \langle\cdot\rangle_i)$, $i = 1, 2$. The **approximate synchronization** operator $\parallel_\varepsilon$, $\varepsilon \geq 0$, acting on the two composite transition systems yield another composite transition system

$$T := T_1 \parallel_\varepsilon T_2, \tag{24}$$

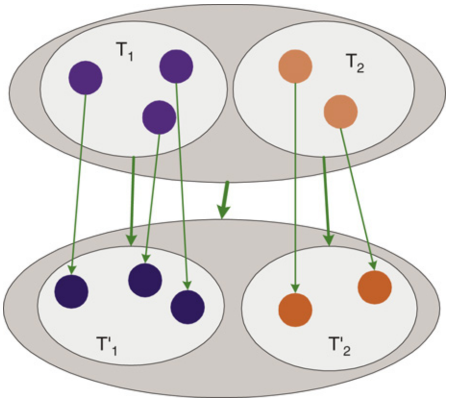


Fig. 2. Compositional properties of approximate (bi)simulation. Each ellipse symbolizes approximate synchronization. The arrows indicate approximate (bi)simulation. The relation between the precisions of the approximate (bi)simulations is given in Theorem 26 and not displayed here.

where $T = (Q_1 \times Q_2, \Sigma^{n_1+n_2}, \rightarrow, Q_1^0 \times Q_2^0, \Pi_1 \times \Pi_2, \langle\cdot\rangle)$. The transition relation $\rightarrow$ is such that $(q_1, q_2) \overset{\sigma,\sigma'}{\rightarrow} (q_1', q_2')$ iff $q_1 \overset{\sigma}{\rightarrow}_1 q_1'$, $q_2 \overset{\sigma'}{\rightarrow}_2 q_2'$, $d_{\Sigma^*}(\sigma, \sigma') \leq \varepsilon$. The observation map $\langle\cdot\rangle$ is defined as

$$\langle (q_1, q_2) \rangle := (\langle q_1 \rangle_1, \langle q_2 \rangle_2). \tag{25}$$

The new observation space $\Pi = \Pi_1 \times \Pi_2$ is equipped with the pseudometric

$$d_\Pi \left((\pi_1, \pi_2), (\pi_1', \pi_2') \right) = d_{\Pi_1}(\pi_1, \pi_1') + d_{\Pi_2}(\pi_2, \pi_2').$$

Notice that composite transition systems are intrinsically transition systems with an additional assumption in the structure of their sets of labels. Two composite transition systems with the same multiplicity share the same set of labels, and hence the concept of approximate (bi)simulation applies to them. The compositional properties of the approximate (bi)simulation in the previous subsection, which is defined for composite transition systems with multiplicity 2 can be extended easily to this more general case.

Theorem 26. *Given a set of labels Σ and composite transition systems T_1, T_2, T_1' and T_2'. Suppose that the transition systems T_1 and T_1' have observation space Π_1 and multiplicity n_1, while T_2 and T_2' have observation space Π_2 and multiplicity n_2.*

(i) *If $T_1 \preceq_{\varepsilon_1,\delta_1} T_1'$ and $T_2 \preceq_{\varepsilon_2,\delta_2} T_2'$, then for any $\varepsilon \geq 0$,*

$$T_1 \parallel_\varepsilon T_2 \preceq_{\varepsilon+\max(\varepsilon_1,\varepsilon_2),\delta_1+\delta_2} T_1' \parallel_{\varepsilon+\varepsilon_1+\varepsilon_2} T_2'. \tag{26}$$

(ii) *If $T_1 \approx_{\varepsilon_1,\delta_1} T_1'$ and $T_2 \approx_{\varepsilon_2,\delta_2} T_2'$, then for any $\varepsilon \geq 0$,*

$$T_1 \parallel_\varepsilon T_2 \approx_{\varepsilon+\max(\varepsilon_1,\varepsilon_2),\delta_1+\delta_2} T_1' \parallel_{\varepsilon+\varepsilon_1+\varepsilon_2} T_2'. \tag{27}$$

The compositional properties given in Theorem 26 is illustrated in Fig. 2.

5. Safety problem over a digital communication channel

In this section, we discuss the problem of safety verification of a control system over a digital communication channel, from the perspective of the theory presented in the previous sections. Problems with safety specifications arise in many application domains such as automotive control, manufacturing systems, and air-traffic management systems. Given a continuous time linear plant P_c and a set Ω of *good states* within which the plant should evolve, this problem deals with finding the set of all initial states (known in the literature as the *maximal safe set* [18]) for which there exists a controller such that the closed-loop system never leaves the set Ω. This control problem has been studied in the literature in the past few years both for continuous-time systems [19] and for discrete-time systems [20–22,18].

We address the issue of guaranteeing safety specifications for the control scheme shown in Fig. 3, where C and P_c share information via a communication link. Information coming from the controller is at first quantized and then sent via the communication link. Information coming from the plant is at first sampled, then quantized and finally sent via the link to the controller. The parameters that characterize the communication system are the sampling time T_s, the quantization threshold M and the quantization width δ, and the transmission power level p. Together, these variables define the communication cost, which is related to the bandwidth and the transmission power.

Let $x(k+1) = Ax + Bu$ and $u(k+1) = Fu + Gx$, with $x \in \mathbb{R}^n$, $u \in \mathbb{R}^m$, be the dynamics respectively of P (obtained by the discretization of the continuous time system P_c with sampling time T_s) and C. We assume that the communication channel is time-varying. The addressed controller synthesis problem can be stated as follows.

Problem 27. Given a plant P and a *safe set* $\Omega \subset \mathbb{R}^n$, find a (digital) controller C and the set of all initial states in Ω such that the closed-loop system satisfies the safety requirements for all possible transmission channel states, i.e.

$$x(k) \in \Omega, \quad \forall k \geq 0,$$

while keeping the communication cost as low as possible.

Our recent publication [23] proposes a method for solving Problem 27, that is based on the principles of PBD [24]. We formulate the control problem over the abstract scheme depicted in Fig. 3. Non-idealities coming from the communication system, such as quantization error and transmission noise, can be modeled as additive continuous disturbances d_1 and d_2. We assume that the disturbance on the signals is confined within compact sets $D_1 \subset \mathbb{R}^n, 0 \in D_1$ and $D_2 \subset \mathbb{R}^m, 0 \in D_2$. We also assume that τ_1 and τ_2 model the non-deterministic delay in data transmission in the two links: we assume that the delay belongs to a finite set of elements, namely a packet can non-deterministically be received within a finite number of steps. This happens when the communication protocol exploits error detection and admits a finite number of retransmissions. The above assumptions can be formalized as follows.

$$d_1 \in D_1, d_2 \in D_2, \tau_1 \in \{0, 1, \ldots, \bar{\tau}_1\}, \tau_2 \in \{0, 1, \ldots, \bar{\tau}_2\}. \tag{28}$$

The presence of continuous disturbances and delay has to be taken into account when designing the controller C to satisfy safety requirements. A controller solving the safety problem must be *robust* with respect to these disturbances. Our approach is based on an *assume-guarantee* reasoning, frequently used in the formal verification of reactive and timed systems. First we synthesize a controller that satisfies the safety requirements on the plant system P under the nominal condition, i.e. in the absence of disturbance [20,18], and in presence of the expected transmission delay:

$$d_1 = 0, \qquad d_2 = 0, \qquad \tau_1 = \tau_1^e, \qquad \tau_2 = \tau_2^e. \tag{29}$$

The approach reported in [23] considered the case with no delay ($\bar{\tau}_1 = \bar{\tau}_2 = 0$), and estimated by extensive Matlab simulations the *maximum disturbance* sets $\bar{D}_1, \bar{D}_2$, such that the safety constraint on the plant is satisfied. By relating the sets $\bar{D}_1, \bar{D}_2$ to the parameters of the communication systems, we were able to design a transmission power control strategy that minimizes a communication cost (e.g. power consumption) while guaranteeing that the disturbance

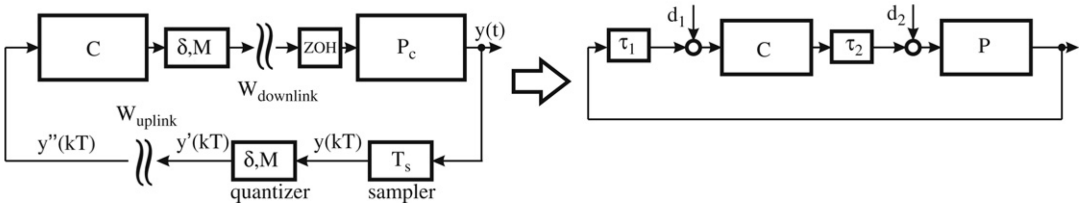


Fig. 3. Communication scheme.

remains bounded in $\bar{D}_1, \bar{D}_2$. More precisely, the disturbance sets $\bar{D}_1, \bar{D}_2$ were given as functions of the *signal-to-noise* ratio (SNR), and this information was used to design a switching strategy for the transmission power level.

However, the simulation-based method that we used to determine $\bar{D}_1, \bar{D}_2$ was qualitative and non conservative. One can exploit the approximation framework developed in this paper to compute tight upper bounds for $\bar{D}_1, \bar{D}_2$.

Given P and C, we use $C \parallel_\varepsilon P$ to model the real implementation of the control loop. That is, the synchronization between the plant and the controller is only *approximate*, because of the disturbance in the transmission. We assume without loss of generality that ε is the diameter of the sets $\bar{D}_1$ and $\bar{D}_2$. To take into account the delays, we can augment the state spaces $x_{\bar{\tau}_1}$ of P and $u_{\bar{\tau}_2}$ of C, as usually done in the analysis of time delay systems:

$$\begin{aligned} x_{\bar{\tau}_1}(k+1) &= \begin{bmatrix} A & 0 & \cdots & 0 & 0 \\ I & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & I & 0 \end{bmatrix} x_{\bar{\tau}_1}(k) + \begin{bmatrix} B \\ 0 \\ \vdots \\ 0 \end{bmatrix} u(k) \\ &= A_{\bar{\tau}_1} x_{\bar{\tau}_1}(k) + B_{\bar{\tau}_1} u(k), \end{aligned}$$

$$x_{\bar{\tau}_1} = (x, x_{(-1)}, \ldots, x_{(-\bar{\tau}_1)})^{\mathrm{T}} \in \mathbb{R}^{n(\bar{\tau}_1+1)}$$

$$x(0) \in X_0, x_{(-1)}(0) = x(0), \ldots, x_{(-\bar{\tau}_1)}(0) = x(0).$$

The variable x denotes the current value of the state, while the variables $x_{(-i)}$ denote the value of the state i steps before. The same can be done to define the augmented state space $u_{\bar{\tau}_2}$ of C. We can embed these two systems respectively into transition systems $\mathcal{T}_P$ and $\mathcal{T}_C$. We will illustrate the procedure in the case $\bar{\tau}_1 = \bar{\tau}_2 = 2$, since all other cases can be dealt with analogously.

Definition 28 (*Transition System Model of P*). Given a system P, we define a transition system $\mathcal{T}_P$ as follows:

- $Q_P = \mathbb{R}^{3n}$ is the state space;
- Q_P^0 is the set of initial states of the plant P;
- $\Sigma_P = \mathbb{R}^n \times \mathbb{R}^m$;
- $\rightarrow_P$ is the transition relation defined as follows:

$$(x, x_{(-1)}, x_{(-2)}) \xrightarrow{(x,\tilde{u})} (x', x, x) \Leftrightarrow x' = A_{\bar{\tau}_1} x + B_{\bar{\tau}_1} \tilde{u}; \tag{30}$$

$$(x, x_{(-1)}, x_{(-2)}) \xrightarrow{(x_{(-1)},\tilde{u})} (x', x, x_{(-1)}) \Leftrightarrow x' = A_{\bar{\tau}_1} x + B_{\bar{\tau}_1} \tilde{u}; \tag{31}$$

$$(x, x_{(-1)}, x_{(-2)}) \xrightarrow{(x_{(-2)},\tilde{u})} (x', x, x_{(-1)}) \Leftrightarrow x' = A_{\bar{\tau}_1} x + B_{\bar{\tau}_1} \tilde{u}; \tag{32}$$

- $\Pi_P = \mathbb{R}^n$ is the set of observations;
- $\langle x \rangle_P = x$ is the observation map.

The intuition of the transition relation is as follows: the augmented state space models the memory of the state in the previous $\bar{\tau}_1$ time slots, and the label indicates which one of these states triggers the synchronization with the other system. For the transition relation defined above, we assume that when the system synchronizes with the most recent state x (30), then it cannot synchronize in the future with the previous values $x_{(-1)}, x_{(-2)}$: this means that the received packets cannot swap (e.g. if we are using a packet reordering protocol, such as TCP).[2] When $\bar{\tau}_1 > 2$, one can iterate the reasoning above to define the transition relation rules. Similarly, we can define $\mathcal{T}_C$, the transition system model of C. We define a metric on $\Sigma = \Sigma_P \times \Sigma_C = \mathbb{R}^n \times \mathbb{R}^m$ as follows:

$$d\left((x, \tilde{u}), (\tilde{x}, u)\right) = \max\left\{|x - \tilde{x}|, |u - \tilde{u}|\right\}. \tag{33}$$

For a given disturbance set with diameter ε, the idea is to compute a finite abstraction of the approximate synchronization $C \parallel_\varepsilon P$, and verify its safety. We can achieve this by first computing finite approximate abstractions of the plant and the controller, and then computing the approximate synchronization of the abstract systems. Let $\mathcal{T}_P'$ and $\mathcal{T}_C'$ be abstractions of P and C such that $\mathcal{T}_P' \approx_{\varepsilon_P,\delta_P} \mathcal{T}_P$ and $\mathcal{T}_C' \approx_{\varepsilon_C,\delta_C} \mathcal{T}_C$. When the systems P and C are stable, it is possible to compute finite abstractions $\mathcal{T}_P'$ and $\mathcal{T}_C'$ with any desired precision [25]. By Theorem 22, the following holds:

$$(\mathcal{T}_C \parallel_\varepsilon \mathcal{T}_P) \approx_{\varepsilon+\max(\varepsilon_C,\varepsilon_P),\delta_C+\delta_P} (\mathcal{T}_C' \parallel_{\varepsilon+\varepsilon_C+\varepsilon_P,\delta_C+\delta_P} \mathcal{T}_P').$$

Our abstraction allows to verify in finite time the safety specifications: we can use the precision of our abstraction to compute an enlarged safe set, for which the abstract system is required to be safe [26]. It is reasonable that if ε (that is the diameter of the disturbance set) is greater than the diameter of the safe set, then the confidence on the precision of our abstraction will be too coarse to be able to verify safety.

6. Conclusions

The notion of approximate (bi)simulation proposed by Girard and Pappas [8] has developed as a useful tool of abstraction of dynamical systems. The theory stems from the idea of relaxing the requirement that an abstraction is exactly equal to the original system. In this paper, we follow the same path by imposing even more relaxed conditions on the approximate (bi)simulation. Namely, we introduce a pseudometric on the set of labels and allow some tolerance in the labels, when one system simulates another. We show that this new notion of approximate (bi)simulation is a generalization of the other one, in the sense that if we set the tolerance in the label to zero, we recover all the existing results.

Another notion that we introduce in this paper is that of approximate synchronization. Approximate synchronization is based on the idea of relaxing the requirements that when two transition systems synchronize, they synchronize on the same label. Instead, we allow them to synchronize on labels that are close. We show that approximate (bi)simulation is compositional with respect to approximate synchronization. In addition to the theoretical presentation of approximate bisimulation and synchronization, we also discuss the application of this framework in analyzing control systems over digital communication network.

Having set up a theoretical framework, we set our next goal at providing a computational framework for the ideas that we discuss here. Approximate (bi)simulation of Girard and Pappas has a nice

[2] A model that does not perform packet reordering (e.g. UDP) can be modeled in this framework by appropriately redefining the transition relation.

computational framework, in the form of bisimulation functions, to facilitate the construction of approximate (bi)simulation relations [8,27]. We have generalized the notion of bisimulation function. We now need to extend the computation machinery to cope with the new notion.

Acknowledgments

The authors would like to thank Antoine Girard for valuable discussion during the preparation of this paper. This work is partially funded by the NSF Presidential Early CAREER (PECASE) Grant 0132716, and by European Commission under Project IST NoE HYCON contract n. 511368 and STREP project n. TREN/07/FP6AE/S07.71574/037180 iFLY.

References

[1] P. Tabuada, G.J. Pappas, P. Lima, Compositional abstractions of hybrid control systems, Discrete Event Dynamic Systems 14 (2) (2005) 203–238.
[2] R. Alur, T.A. Henzinger, G. Lafferriere, G.J. Pappas, Discrete abstraction of hybrid systems, Proceedings of the IEEE 88 (2000) 971–984.
[3] G.J. Pappas, Bisimilar linear systems, Automatica 39 (2003) 2035–2047.
[4] A.J. van der Schaft, Equivalence of dynamical systems by bisimulation, IEEE Transactions on Automatic Control 49 (12) (2004) 2160–2172.
[5] G. Pola, A.J. van der Schaft, M. Di Benedetto, Achievable bisimilar behaviour of abstract systems, in: Proc. 44th IEEE Conf. Decision and Control, IEEE, Seville, 2005.
[6] M. Ying, Topology in Process Calculus, Springer-Verlag, New York, 2001.
[7] L. de Alfaro, M. Faella, M. Stoelinga, Linear and branching system metrics, UCSC-CRL-05-01, School of Engineering, University of California at Santa Cruz (2005).
[8] A. Girard, G.J. Pappas, Approximation metrics for discrete and continuous systems, IEEE Transactions on Automatic Control 52 (5) (2007) 782–798.
[9] C.G. Cassandras, S. Lafortune, Introduction to Discrete Event Systems, Kluwer, 1999.
[10] A.A. Julius, G.J. Pappas, Approximate equivalence and approximate synchronization of metric transition systems, in: Proc. 45th IEEE Conf. Decision and Control, IEEE, San Diego, 2006.
[11] P. Caspi, R. Salem, Threshold and bounded-delay voting in critical control systems, in: M. Joseph (Ed.), Formal Techniques in Real-Time and Fault-Tolerant Systems, in: LNCS, vol. 1926, Springer Verlag, 2000.
[12] P. Caspi, A. Benveniste, Toward an approximation theory for computerised control, in: Proc. 2nd International Workshop on Embedded Software, Springer, Grenoble, 2002.
[13] C. Kossentini, P. Caspi, Approximation, sampling and voting in hybrid computing systems, in: Hybrid Systems: Computation and Control, in: LNCS, vol. 3927, Springer Verlag, 2006, pp. 363–376.
[14] G. Baliga, S. Graham, L. Sha, P.R. Kumar, Service continuity in networked control using etherware, IEEE Distributed Systems Online 5 (8) (2004) (online publication).
[15] S. Tatikonda, S. Mitter, Control under communication constraints, IEEE Transactions on Automatic Control 49 (7) (2004) 1056–1068.
[16] N.C. Martins, M.A. Dahleh, Fundamental limitations of performance in the presence of finite capacity feedback, in: Proc. American Control Conference, IEEE, 2005, pp. 79–86.
[17] R. Alur, C. Courcoubetis, N. Halbwachs, T.A. Henzinger, P.H. Ho, X. Nicollin, A. Olivero, J. Sifakis, S. Yovine, The algorithmic analysis of hybrid systems, Theoretical Computer Science 138 (1995) 3–34.
[18] E. De Santis, M.D. Di Benedetto, L. Berardi, Computation of maximal safe sets for switching systems, IEEE Transactions on Automatic Control 40 (2) (2004) 184–195.
[19] J. Lygeros, C. Tomlin, S. Sastry, Controllers for reachability specifications for hybrid systems, Automatica 35 (3) (1999) 349–370.
[20] F. Blanchini, Set invariance in control - a survey, Automatica 35 (11) (1999) 1747–1768.
[21] A. Bemporad, G. Ferrari-Trecate, M. Morari, Observability and controllability of piecewise affine and hybrid systems, IEEE Transactions on Automatic Control 45 (10) (2000) 1864–1876.
[22] R. Vidal, S. Schaffert, J. Lygeros, S. Sastry, Controlled invariance of discrete time systems, in: Hybrid Systems: Computation and Control, in: LNCS, vol. 1790, Springer Verlag, 2000, pp. 437–450.
[23] M. Di Benedetto, A. D'Innocenzo, C. Rinaldi, F. Santucci, E. Serra, Modelling and design of control algorithms over wireless networks, in: Proc. IEEE Multi-conference on Systems and Control (MSC)., Singapore, 2007.
[24] M. Sgroi, A. Wolisz, A. Sangiovanni-Vincentelli, J. Rabaey, A service-based universal application interface for ad-hoc wireless sensor networks, White Paper, Berkeley Wireless Research Center. Berkeley, California, USA, UC Berkeley, EECS (November 2003).
[25] A. Girard, Approximately bisimilar finite abstractions of stable linear systems, in: Hybrid Systems: Computation and Control, in: LNCS, vol. 4416, Springer Verlag, 2007, pp. 231–244.
[26] A. Girard, G. Pappas, Approximation metrics for discrete and continuous systems, IEEE Transactions on Automatic Control 52 (5) (2007) 782–798.
[27] A.A. Julius, Approximate abstraction of stochastic hybrid automata, in: Hybrid Systems: Computation and Control, in: LNCS, vol. 3927, Springer Verlag, 2006, pp. 318–332.