Symbolic models for linear control systems with disturbances

Giordano Pola and Paulo Tabuada

Abstract— **A recent trend in the control systems community is the study of appropriate symbolic abstractions capturing the behavior of continuous and hybrid systems. This approach provides a common mathematical language to describe physical systems as well as software and hardware, and is therefore particularly appealing when dealing with the design of embedded systems. In this paper we address the construction of symbolic models for the class of linear control systems with politopically bounded states and disturbances. We show that under an asymptotic stabilizability assumption, it is always possible to construct a symbolic model that approximates the control system with a precision that is chosen a priori, as a design parameter. While in previous approaches in the existing literature, the construction of symbolic models relied on a (arbitrary) choice of a finite number of control signals, the symbolic model that we propose, captures any (control and disturbance) input. Therefore, the proposed model provides a finer description of the continuous model than the existing ones and this feature translates into a more efficient controller synthesis process. Furthermore, the computation of the symbolic model can be performed by resorting to linear matrix inequalities.**

keywords: symbolic models, quantized systems, approximate simulation, alternating simulation, linear control systems.

I. Introduction

Symbolic models have been recently proposed as a tool for the analysis and synthesis of complex control systems [1]. In particular, they enable a correct–by–design approach to the synthesis of embedded control software [2], [3]. The key idea in this approach is to regard the synthesis of software as a control problem to be solved *in conjunction* with the synthesis of the control algorithms. The heart of this approach is the definition of a symbolic model that approximates the continuous control system. Since these symbolic models are of the same nature of the models describing software and hardware, they provide a unified framework to study controller synthesis problems characterized by the interaction of the physical layer with software and hardware. Moreover, the use of symbolic models allows one to leverage standard techniques in the context of supervisory control [4] and of game theory [5], [6]. Previous work by the authors [3] addressed the construction of symbolic models by choosing a finite set of control signals. However, if the chosen control signals are "not enough", it may happen that a controller fails to exist for the finite abstraction. In this case, a finer choice of control signals is required and consequently the construction of a new finite abstraction is needed. In the context of quantized control systems [7], [8] similar approaches have been exploited for obtaining a lattice structure on the reachable sets of the finite abstractions; this lattice structure has been used to obtain efficient motion planning algorithms.

In this paper we focus on alternative ways of constructing symbolic models, where *all* (control and disturbance) inputs are captured. We consider the class of linear control systems with polytopically bounded states and disturbances. We show that if the linear control system is asymptotically stabilizable, there exists a symbolic model that approximates the system with a precision that is chosen a priori, as a design parameter. The proposed symbolic model captures any piecewise–constant control input and any measurable disturbance input. Furthermore, we show that this symbolic model can be constructed in a finite number of steps, by using standard techniques in the context of linear matrix inequalities [9]. At the technical level, we formalize a notion of simulation [10], [11] by merging the new notion of approximate simulation, introduced by Girard and Pappas in [12] with the classical one of alternating simulation, introduced by Alur and co–workers in [13]. Furthermore, the construction of the symbolic model relies on polytopic approximations of reachable sets (e.g. [14], [15]).

Notation. Given a set A, $card(A)$ denotes the cardinality of A. The identity map on a set A is denoted by 1_A. If A is a subset of B we denote by $\iota_A : A \hookrightarrow B$ or simply by ι the natural inclusion map taking any $a \in A$ to $\iota(a) = a \in B$. Given $a \in \mathbb{R}$, the symbol $|a|$ denotes the absolute value of a. Given a vector $x \in \mathbb{R}^n$ we denote by x_i the i–th element of x and by $\|x\|$ the infinity norm of x; we recall that $\|x\| = \max_{1\leq i\leq n} |x_i|$. Given a matrix M, the symbols M', $\mathrm{Im}(M)$ and $\|M\|$ denote respectively the transpose, the image and the infinity norm of M; if $M = \{m_{ij}\}_{i=1...n,j=1...m} \in \mathbb{R}^{n\times m}$, we recall that $\|M\| = \max_{1\leq i\leq m} \sum_{j=1}^{n} |m_{ij}|$. The closed ball centered at $x \in \mathbb{R}^n$ with radius ε is defined by $\mathcal{B}_\varepsilon(x) = \{y \in \mathbb{R}^n : \|x - y\| \leq \varepsilon\}$. For any $A \subseteq \mathbb{R}^n$ and $\mu \in \mathbb{R}$ set $[A]_\mu = \{a \in A \mid a_i = k_i\mu, k_i \in \mathbb{Z}, i = 1, ..., n\}$. Given two subsets A and B of $\mathbb{R}^n$, $A \oplus B$ denotes the Minkowski sum, i.e. $A \oplus B = \{a + b : a \in A, b \in B\}$. The symbol $conv(x_1, x_2, ..., x_m)$ denotes the convex hull of vectors $x_1, x_2, ..., x_m \in \mathbb{R}^n$. A bounded set of the form $conv(x_1, x_2, ..., x_m)$ is called a polytope. We identify a relation $R \subseteq A \times B$ with the map $R : A \to 2^B$ defined by $b \in R(a)$ iff $(a, b) \in R$; the relation R is said to be surjective if $R(A) = B$.

This work has been partially supported by the National Science Foundation CAREER award 0717188.

The authors are with the Department of Electrical Engineering, University of California at Los Angeles, Los Angeles, CA 90095-1594, USA {pola,tabuada}@ee.ucla.edu.

II. Linear Control Systems

Consider the following linear control system:

$$\Sigma : \begin{cases} \dot{x} = Ax + Bu + Gd, \\ x \in X, u \in \mathbb{R}^m, d \in D, \end{cases} \quad (1)$$

where x is the state, u is the control input and d is the disturbance input. We suppose that $X \subseteq \mathbb{R}^n$ and $D \subseteq \mathbb{R}^l$ are polytopic sets with non–empty interior and that $0 \in X$; furthermore we suppose that the class of admissible control inputs $\mathcal{U}$ and of disturbances inputs $\mathcal{D}$ are, respectively, the class of measurable functions from any interval $[0, \tau] \subset \mathbb{R}$ to $\mathbb{R}^m$ and to D, for some $\tau \in \mathbb{R}^+$. The state reached at time $t \in \mathbb{R}_0^+$ with initial condition $x_0 \in X$, control input $\mathbf{u} \in \mathcal{U}$ and disturbance input $\mathbf{d} \in \mathcal{D}$ will be denoted by $\mathbf{x}(t, x_0, \mathbf{u}, \mathbf{d})$. The linear system (1) is said to be *asymptotically stabilizable* (resp. *controllable*) when Σ with $D = \{0\}$ is so. We suppose that the disturbance d is unknown and cannot be measured. Therefore the linear control system Σ can be thought of, as the arena of a 2–players polytopic game in the spirit of [16], where a *protagonist* chooses her/his action through the control input u and an *antagonist* chooses his/her action through the disturbance input d. We start by introducing the class of *alternating transition systems* that will be used in this paper, as abstract models for control systems. Alternating transition systems were introduced in [13] for modeling the arena of N–players discrete games. In the following definition we focus on a 2–players version of the general notion of [13].

Definition 1: A (alternating) transition system is a tuple:

$$T = (Q, L, W, \longrightarrow, O, H),$$

consisting of:

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

A transition system $(Q, L, W, \longrightarrow, O, H)$ is said to be *metric*, if the output set O is equipped with a metric $\delta : O \times O \to \mathbb{R}_0^+$ and *finite*, if Q is finite.

We will follow standard practice and denote a transition from q to p labeled by ℓ and w, by $q \xrightarrow{\ell,w} p$. Transition systems capture dynamics through the transition relation. For any states $q, p \in Q$, $q \xrightarrow{\ell,w} p$ simply means that it is possible to evolve or jump from state q to state p under the action labeled by ℓ and w. Analogously to the linear control systems that we consider in this paper, transition systems as in Definition 1 can be thought of as the arena of a 2–players game, where the protagonist acts through control labels and the antagonist acts through disturbance labels. 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. Given a linear control system Σ, define:

$$T(\Sigma) := (Q_1, L_1, W_1, \longrightarrow_1, O_1, H_1),$$

where:

- $Q_1 = X$;
- $L_1 = \mathcal{U}$;
- $W_1 = \mathcal{D}$;
- $q \xrightarrow{\mathbf{u},\mathbf{d}}_1 p$, if $\mathbf{x}(\tau, q, \mathbf{u}, \mathbf{d}) = p$ for some $\tau \in \mathbb{R}^+$;
- $O_1 = X$;
- $H_1 = 1_X$.

Transition system $T(\Sigma)$ is equivalent to linear control system Σ in that any sequence of transitions of $T(\Sigma)$ can be transformed into a trajectory of the linear system Σ and vice versa. In the following we will work with a subsystem of $T(\Sigma)$, obtained by selecting those transitions from $T(\Sigma)$ describing trajectories of duration τ for some chosen $\tau \in \mathbb{R}^+$. This can be thought of, as a sampling process or a time discretization.

Definition 2: Given a linear control system Σ and any $\tau \in \mathbb{R}^+$, define the following transition system:

$$T_\tau(\Sigma) := (Q_2, L_2, W_2, \longrightarrow_2, O_2, H_2),$$

where:

- $Q_2 = X$;
- $L_2 = \{\mathbf{u} \in \mathcal{U} : \text{the domain of } \mathbf{u} \text{ is } [0, \tau]\}$;
- $W_2 = \{\mathbf{d} \in \mathcal{D} : \text{the domain of } \mathbf{d} \text{ is } [0, \tau]\}$;
- $q \xrightarrow{\mathbf{u},\mathbf{d}}_2 p$, if $\mathbf{x}(\tau, q, \mathbf{u}, \mathbf{d}) = p$;
- $O_2 = X$;
- $H_2 = 1_X$.

In the subsequent developments we will construct a finite transition system that approximates the transition system $T_\tau(\Sigma)$ with a precision that is chosen a priori, as a design parameter.

III. Approximate simulation

In this section we consider the simpler case of linear control systems where no disturbance inputs are acting, i.e. systems Σ as in (1) with $D = \{0\}$. The next section will be devoted to the more general case of linear systems Σ with disturbances. Since $D = \{0\}$ in Σ, then $W_2 = \{\mathbf{0}\}$ in $T_\tau(\Sigma)$. For notational simplicity, we denote any transition system $T = (Q, L, \{0\}, \longrightarrow, O, H)$ by $T = (Q, L, \longrightarrow, O, H)$, any transition $q \xrightarrow{\ell,0} p$ by means of $q \xrightarrow{\ell} p$ and we write $\mathbf{x}(t, x, \mathbf{u})$ instead of $\mathbf{x}(t, x, \mathbf{u}, \mathbf{0})$, where $\mathbf{0}$ is the null disturbance input. We start by introducing a notion of approximate relation that will be the basis upon which our results rely. The notion that we consider is the one of simulation relation [10], [11]. Simulation relations are standard mechanisms to relate the properties of transition systems. 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 sequence of transitions r_1 of T_1 can be transformed into a sequence of transitions r_2 of T_2. While typical simulation relations require r_1 and r_2 to be observationally indistinguishable, that is $H_1(r_1) = H_2(r_2)$, we shall relax this by requiring $H_1(r_1)$ to simply be close to $H_2(r_2)$, where closeness is measured with respect to the (common) metric δ on the (common) output set. The following notion has been introduced in [12] and in a slightly different formulation in [3].

Definition 3: Let $T_1 = (Q_1, L_1, \longrightarrow_1, O, H_1)$ and $T_2 = (Q_2, L_2, \longrightarrow_2, O, H_2)$ be metric transition systems with the same observation set O and metric δ and let be $\varepsilon \in \mathbb{R}^+$. A relation $R \subseteq Q_1 \times Q_2$ is said to be an *ε–approximate simulation relation* from T_1 to T_2 if for any $(q_1, q_2) \in R$:

(i) $\delta(H_1(q_1), H_2(q_2)) \leq \varepsilon$;

(ii) $q_1 \xrightarrow{\ell_1} p_1$ implies the existence of $q_2 \xrightarrow{\ell_2} p_2$ such that $(p_1, p_2) \in R$.

As argued in [3], the existence of surjective approximate simulation relations simplifies the controller synthesis for physical systems interfacing software and hardware. Indeed suppose that a finite model T can be found, so that a surjective approximate simulation from T to Σ exists. In this case one can synthesize a controller on T rather than on Σ. This approach is appealing since transition systems provide a common mathematical language to describe physical systems as well as software and hardware of microprocessors implementing controllers and therefore it is important in the design of embedded control software.

Let $\{a_1, a_2, ..., a_m\}$ be a basis for $\mathbb{R}^m$. In the following, given some $\tau \in \mathbb{R}^+$ we denote by u the constant control input $\mathbf{u}(t) = u$, $t \in [0, \tau]$. Given Σ, any $\tau \in \mathbb{R}^+$ and $\eta \in \mathbb{R}^+$, define the following transition system:

$$T_{\tau,\eta}(\Sigma) := (Q_1, L_1, \longrightarrow_1, O_1, H_1), \quad (2)$$

where:

- $Q_1 = [X]_\eta$;
- $L_1 = \mathbb{R}^m$;
- $q \xrightarrow{\ell}_1 p$ if there exist $\alpha_i \in \mathbb{R}$, $i = 1, 2, ..., m$ such that:

$$\begin{array}{l} \sum_{i=1}^{m} \alpha_i \mathbf{x}(\tau, q, a_i) \in \mathcal{B}_\eta(p), \\ \ell = \sum_{i=1}^{m} \alpha_i a_i; \end{array} \quad (3)$$

- $O_1 = X$;
- $H_1 = \imath : Q_1 \longrightarrow O_1$.

Parameters τ and η in the transition system $T_{\tau,\eta}(\Sigma)$ can be thought of respectively, as a sampling time and a state space quantization. Notice that, since the state space X of Σ is bounded, *the defined transition system $T_{\tau,\eta}(\Sigma)$ is finite*. Although the set of control labels is infinite, it is possible to explicitly construct $T_{\tau,\eta}(\Sigma)$. In fact, condition (3) can be reformulated as follows:

$$\{A_\tau q\} \oplus \mathrm{Im}(B_\tau) \cap \mathcal{B}_\eta(p) \neq \varnothing, \quad (4)$$

where:

$$A_\tau = e^{A\tau}; \qquad B_\tau = \int_0^\tau e^{A(\tau - t)} B dt. \quad (5)$$

Since the set defined in the left hand side of (4) is semi–linear (recall that $\mathcal{B}_\eta(p)$ is a closed ball, induced by the infinity norm), the construction of the transition relation of $T_{\tau,\eta}(\Sigma)$ can be performed by using standard techniques available in the literature on linear matrix inequalities [9]. We will provide more details of such construction in Section V. We point out that the control labels that are used in the construction of $T_{\tau,\eta}(\Sigma)$ are the m constant curves $\mathbf{u}(t) = a_i$ for $t \in [0, \tau]$, $i = 1, 2, ..., m$. The number of steps required for constructing $T_{\tau,\eta}(\Sigma)$ is bounded by $m\, card(Q_1)$, where $card(Q_1)$ depends on the state space quantization η. The finite model $T_{\tau,\eta}(\Sigma)$ differs from the one proposed in the context of quantized systems (e.g. [7], [8]) where a finite set of control signals is chosen a priori. In fact the label set L_1 of $T_{\tau,\eta}(\Sigma)$ is $\mathbb{R}^m$. We can now give the following result.

Theorem 1: Consider a linear control system Σ as in (1) with $D = \{0\}$, and any desired precision $\varepsilon \in \mathbb{R}^+$. If Σ is asymptotically stabilizable then, for any matrix K such that $A + BK$ is Hurwitz, any $\tau \in \mathbb{R}^+$ and any $\eta \in \mathbb{R}^+$ satisfying the following condition:

$$\eta + \|e^{(A+BK)\tau}\| \varepsilon \leq \varepsilon, \quad (6)$$

there exists a surjective ε–approximate simulation relation from $T_{\tau,\eta}(\Sigma)$ to $T_\tau(\Sigma)$.

Before giving the proof, we stress that the above result relates $T_\tau(\Sigma)$ to a finite model that captures the effect of *all* constant inputs $u \in \mathbb{R}^m$, while in previous work [3] the set of control inputs considered was finite. Furthermore, we point out that if Σ is asymptotically stabilizable, there always exist $\tau \in \mathbb{R}^+$ and $\eta \in \mathbb{R}^+$ satisfying condition (6). In fact, if $A + BK$ is Hurwitz then there always exists a sufficiently large $\tau \in \mathbb{R}^+$ so that $\left\|e^{(A+BK)\tau}\right\| < 1$; then, by choosing a sufficiently small value of η, condition (6) is fulfilled.

Proof: Consider the relation $R \subset Q_1 \times Q_2$ defined by $(q, x) \in R$ if and only if $||q - x|| \leq \varepsilon$. By geometrical considerations on the infinity norm, $Q_2 \subseteq \bigcup_{q_1 \in Q_1} \mathcal{B}_\eta(q_1)$ and therefore, since by (6), $\eta < \varepsilon$, we have that $R(Q_1) = Q_2$. We now show that R is an ε–approximate simulation relation from $T_{\tau,\eta}(\Sigma)$ to $T_\tau(\Sigma)$. Consider any matrix K such that $A + BK$ is Hurwitz and any $(q, x) \in R$. By definition of R, condition (i) in Definition 3 is satisfied. Let us now show that condition (ii) of Definition 3 also holds. Consider any $\ell_1 \in L_1$. This implies the existence of coefficients $\alpha_1, \alpha_2, ..., \alpha_m \in \mathbb{R}$ such that $\ell_1 = \sum_{i=1}^{m} \alpha_i a_i$. Since $Q_2 \subseteq \bigcup_{q_1 \in Q_1} \mathcal{B}_\eta(q_1)$, there exists $p \in Q_1$ such that:

$$z := \sum_{i=1}^{m} \alpha_i \mathbf{x}(\tau, q, a_i) \in \mathcal{B}_\eta(p), \quad (7)$$

and then $q \xrightarrow{\ell_1}_1 p$. Define the control feedback $\mathbf{u}_2 = \sum_{i=0}^{m} \alpha_i a_i - K(\mathbf{q} - \mathbf{x})$, where $\mathbf{x}$ and $\mathbf{q}$ are respectively, the trajectories of Σ with initial conditions x and q, and control inputs $\mathbf{u}_2$ and ℓ_1. Consider the transition $x \xrightarrow{\mathbf{u}_2}_2 y$. By conditions (7) and (6), the following chain of inequalities holds:

$$\begin{aligned} \|p - y\| &= \|p - z + z - y\| \leq \|p - z\| + \|z - y\| \\ &= \|p - z\| + \|\mathbf{x}(\tau, q, \ell_1) - \mathbf{x}(\tau, x, \mathbf{u}_2)\| \\ &\leq \|p - z\| + \|e^{(A+BK)\tau}(q - x)\| \\ &\leq \eta + \|e^{(A+BK)\tau}\| \varepsilon \leq \varepsilon. \end{aligned}$$

Thus $(p, y) \in R$, which completes the proof. ■

IV. Alternating approximate simulations

In this section we generalize the results of the previous section to the case of linear control systems with disturbances. In this context we first need to define a suitable notion of approximate simulation that appropriately distinguishes between the role of control inputs and the role of disturbance inputs. The following definition has been obtained by merging the notion of approximate simulation of [12], with the notion of alternating simulation of [13].

Definition 4: Let $T_1 = (Q_1, L_1, W_1, \longrightarrow_1, O, H_1)$ and $T_2 = (Q_2, L_2, W_2, \longrightarrow_2, O, H_2)$ be metric transition systems with the same observation set O and metric δ and let be $\varepsilon \in \mathbb{R}^+$. A relation $R \subseteq Q_1 \times Q_2$ is said to be an *alternating ε–approximate simulation relation* from T_1 to T_2 if for any $(q_1, q_2) \in R$:

(i) $\delta(H_1(q_1), H_2(q_2)) \leq \varepsilon$;

(ii) $\forall \ell_1 \in L_1\ \exists \ell_2 \in L_2\ \forall w_2 \in W_2\ \exists w_1 \in W_1$ such that $q_1 \overset{\ell_1,w_1}{\longrightarrow}_1 p_1$ and $q_2 \overset{\ell_2,w_2}{\longrightarrow}_2 p_2$ where $(p_1, p_2) \in R$.

Definition 4 differs from the original formulation of alternating simulations in [13], in that: firstly, the notion that we propose is given in an approximating sense (see condition (i)), while [13] requires the stronger condition of indistinguishability of observations; secondly, the notion that we propose considers only two players (the protagonist acting through control labels and the antagonist acting through disturbance labels), while [13] considers the more general case of N players. We now define an appropriate finite transition system that will be related to the control system Σ, by means of an alternating approximate simulation relation, as defined above. For any given $\tau \in \mathbb{R}^+$, consider the set:

$$\mathcal{R}_D^\tau = \left\{ x \in \mathbb{R}^n : x = \int_0^\tau e^{A(\tau-t)} G\mathbf{d}(t)dt, \mathbf{d} \in \mathcal{D} \right\}, \quad (8)$$

of all reachable states from the origin by means of any disturbance function $\mathbf{d}$ in $\mathcal{D}$ at time τ and with the null control function. The exact computation of the set $\mathcal{R}_D^\tau$ is in general hard. However there are many results available in the literature, that propose approximations of the reachable set $\mathcal{R}_D^\tau$ (e.g. [14], [15] and the references therein). In particular, some of those results provide polytopic external approximation of $\mathcal{R}_D^\tau$. From now on, we suppose that a polytope $P(\mathcal{R}_D^\tau)$ satisfying $\mathcal{R}_D^\tau \subseteq P(\mathcal{R}_D^\tau)$ is given and we set:

$$P(\mathcal{R}_D^\tau) = conv(b_1, b_2, ..., b_s).$$

Given Σ, any $\tau \in \mathbb{R}^+$ and $\eta \in \mathbb{R}^+$ define the following transition system:

$$T_{\tau,\eta}(\Sigma) := (Q_1, L_1, W_1, \longrightarrow_1, O_1, H_1), \quad (9)$$

where:

- $Q_1 = [X]_\eta$;
- $L_1 = \mathbb{R}^m$;
- $W_1 = P(\mathcal{R}_D^\tau)$;
- $q \overset{\ell,w}{\longrightarrow}_1 p$ if there exist $\alpha_i \in \mathbb{R}$, $i = 1, 2, ..., m$ and $\beta_i \in \mathbb{R}_0^+$, $i = 1, 2, ..., s$ with $\beta_1 + \beta_2 + ... + \beta_s = 1$, such that:

$$\begin{aligned} & z = \textstyle\sum_{i=1}^m \alpha_i \mathbf{x}(\tau, q, a_i, 0) + \sum_{j=1}^s \beta_j b_j, \\ & \ell = \textstyle\sum_{i=1}^m \alpha_i a_i, \\ & w = \textstyle\sum_{j=1}^s \beta_j b_j, \\ & \|z - p\| \leq \eta; \end{aligned} \quad (10)$$

- $O_1 = X$;
- $H_1 = \iota : Q_1 \to O_1$.

We point out that, analogously to the transition system in (2), even though control and disturbance labels sets L_2 and W_2 are infinite, it is still possible to explicitly construct $T_{\tau,\eta}(\Sigma)$ along the lines of the construction of the transition system in (2). In particular, condition (10) can be rewritten as:

$$\{A_\tau q\} \oplus \mathrm{Im}(B_\tau) \oplus W_1 \cap \mathcal{B}_\eta(p) \neq \varnothing, \quad (11)$$

where A_τ and B_τ are defined as in (5). Notice that the set in the left hand side of (11) is semi–linear and therefore also in this case, one can leverage standard techniques available in the literature [9] on linear matrix inequalities to construct the transition relation of $T_{\tau,\eta}(\Sigma)$. In Section V we will give more details about such construction. We point out that the control and disturbance labels that are used in the construction of $T_{\tau,\eta}(\Sigma)$ are the $m+s$ constant curves $\mathbf{u}(t) = a_i$ for $t \in [0,\tau]$, $i = 1, 2, ..., m$ and $\mathbf{d}(t) = b_j$ for $t \in [0,\tau]$, $j = 1, 2, ..., s$. The number of steps needed for constructing such transition system is bounded by $m\, s\, card(Q_1)$, where $card(Q_1)$ depends on the state space quantization η, provided that the set $P(\mathcal{R}_D^\tau)$ is available. The interested reader can refer to [14] for an analysis of the computational effort, required for computing polytopic external approximations of reachable sets.

We can now give the main result of this paper, that generalizes Theorem 1 to the context of alternating approximate simulations.

Theorem 2: Consider a linear control system Σ and any desired precision $\varepsilon \in \mathbb{R}^+$. If Σ is asymptotically stabilizable then for any matrix K such that $A + BK$ is Hurwitz, any $\tau \in \mathbb{R}^+$ and $\eta \in \mathbb{R}^+$ satisfying the following condition:

$$\eta + \|e^{(A+BK)\tau}\| \varepsilon \leq \varepsilon, \quad (12)$$

there exists a surjective alternating ε–approximate simulation relation R from $T_{\tau,\eta}(\Sigma)$ to $T_\tau(\Sigma)$.

Before giving the proof of this result we point out that, analogously to Theorem 1, if Σ is asymptotically stabilizable there always exist parameters $\tau \in \mathbb{R}^+$ and $\eta \in \mathbb{R}^+$ satisfying condition (12).

Proof: Consider the relation $R \subset Q_1 \times Q_2$ defined by $(q, x) \in R$ if and only if $||q - x|| \leq \varepsilon$. By geometrical considerations on the infinity norm, $Q_2 \subseteq \bigcup_{q_1 \in Q_1} \mathcal{B}_\eta(q_1)$ and therefore, since by (12), $\eta < \varepsilon$, we have that $R(Q_1) = Q_2$. We now show that R is an alternating ε–approximate simulation relation from $T_{\tau,\eta}(\Sigma)$ to $T_\tau(\Sigma)$. Consider any matrix K such that $A + BK$ is Hurwitz and any $(q, x) \in R$. By construction, condition (i) in Definition 4 is satisfied. Let us now show that condition (ii) of Definition 4 holds, as well. Consider any $\ell_1 \in L_1$. This implies the existence of coefficients $\alpha_1, \alpha_2, ..., \alpha_m \in \mathbb{R}$ such that $\ell_1 = \sum_{i=1}^{m} \alpha_i a_i$. Define the control feedback $\mathbf{u}_2 = \sum_{i=0}^{m} \alpha_i a_i - K(\mathbf{q} - \mathbf{x})$, where $\mathbf{x}$ and $\mathbf{q}$ are respectively the trajectories of Σ with initial conditions x and q, control inputs $\mathbf{u}_2$ and ℓ_1 and null disturbance input. For any given $\mathbf{w}_2 \in W_2$ consider $w_1 = \mathbf{x}(\tau, 0, \mathbf{0}, \mathbf{w}_2)$. By construction $w_1 \in \mathcal{R}_D^{\tau} \subseteq P(\mathcal{R}_D^{\tau}) = W_1$. This implies the existence of coefficients $\beta_1, \beta_2, ..., \beta_s \in \mathbb{R}_0^+$ with $\beta_1 + \beta_2 + ... + \beta_s = 1$, such that $w_1 = \sum_{i=1}^{s} \beta_i b_i$. Since $Q_2 \subseteq \bigcup_{q_1 \in Q_1} \mathcal{B}_\eta(q_1)$, there exists $p \in Q_1$ such that:

$$\|p - z\| \leq \eta, \tag{13}$$

where:

$$z = \mathbf{x}(\tau, q, \ell_1, \mathbf{w}_2) = \sum_{i=1}^{m} \alpha_i \mathbf{x}(\tau, q, a_i, \mathbf{0}) + \sum_{j=1}^{s} \beta_j b_i.$$

Thus $q \overset{\ell_1, w_1}{\longrightarrow}_1 p$. Consider now the transition $x \overset{\mathbf{u}_2, \mathbf{w}_2}{\longrightarrow}_2 y$. By (13) and (12), the following chain of inequalities holds:

$$\begin{aligned} \|p - y\| &= \|p - z + z - y\| \leq \|p - z\| + \|z - y\| \qquad (14) \\ &= \|p - z\| + \|\mathbf{x}(\tau, q, \ell_1, \mathbf{w}_2) - \mathbf{x}(\tau, x, \mathbf{u}_2, \mathbf{w}_2)\| \\ &= \|p - z\| + \|e^{(A+BK)\tau}(q - x)\| \\ &\leq \eta + \|e^{(A+BK)\tau}\|\varepsilon \leq \varepsilon. \end{aligned}$$

Thus $(p, y) \in R$, which completes the proof. ■

The choice of the asymptotically stabilizing matrix K in the statement of Theorem 2 is arbitrary. One can think to set up an optimization problem so that given τ an asymptotically stabilizing matrix can be found to minimize $\|e^{(A+BK)\tau}\|$. This choice of K would increase the value of η satisfying inequality (12) and consequently it would reduce the cardinality of the state space Q_1 of the symbolic model. We do not provide more details about such optimization process since it is out of the scope of the present paper.

We stress that under the asymptotic stabilizability assumption on the control system Σ, the symbolic model $T_{\tau,\eta}(\Sigma)$ ensures no error propagation in the sequence of transitions, as time proceeds. More formally, for any state x_k of the control system Σ reached at time $t = k\tau$ with $k \in \mathbb{N}$, there exists a state q_k of $T_{\tau,\eta}(\Sigma)$ so that $(q_k, x_k) \in R$ and hence $\|q_k - x_k\| \leq \varepsilon$. On the other hand, the proposed symbolic model $T_{\tau,\eta}(\Sigma)$ does not give information about the behavior of the control system at the intersampling times $t \in [0, \tau]$. One way to obtain a finer description of the original control system is to store information on the discrete states reached during the time interval $[0, \tau]$ in the transition relation $\longrightarrow_1$ of $T_{\tau,\eta}(\Sigma)$.

The above result is important for controller synthesis. Indeed suppose that the goal is to synthesize a controller C for a linear system Σ so that a given specification is fulfilled up to a given precision $\rho \in \mathbb{R}^+$. Then, by following [3] it is possible to derive from ρ a precision $\varepsilon \in \mathbb{R}^+$ so that if a controller exists for $T_{\tau,\eta}(\Sigma)$, that is related to $T_\tau(\Sigma)$ by a surjective alternating ε–approximate simulation, a controller exists for Σ, which satisfies the required specification with precision ρ. Once ε has been found, parameters τ and η can obtained by inequality (12).

V. A NUMERICAL EXAMPLE

Consider the linear control system (1), where:

$$\begin{aligned} &A = \begin{bmatrix} 2 & 0.5 \\ 0 & -0.5 \end{bmatrix}; B = \begin{bmatrix} 1 \\ 1 \end{bmatrix}; G = \begin{bmatrix} 0.1 \\ 0 \end{bmatrix}; \qquad (15) \\ &X = [-1, 1] \times [-1, 1]; \\ &D = [-0.25, 0.25]. \end{aligned}$$

We now illustrate the construction of a finite transition system $T_{\tau,\eta}(\Sigma)$, for which there exists a surjective alternating ε–approximate simulation relation from $T_{\tau,\eta}(\Sigma)$ to $T_\tau(\Sigma)$, where the required precision is set to be $\varepsilon = 1$. For doing so, we first need to choose a matrix K and parameters $\tau \in \mathbb{R}^+$ and $\eta \in \mathbb{R}^+$ so that condition (12) is fulfilled. Since the system Σ is controllable, we can choose a matrix K so that the eigenvalues of $A + BK$ are $-2, -2$:

$$K = \begin{bmatrix} -5.33 & -0.17 \end{bmatrix}.$$

By choosing $\tau = 2$, we obtain that $\left\|e^{(A+BK)\tau}\right\| = 0.26$ and therefore we can choose by condition (12):

$$\eta = \left(1 - \left\|e^{(A+BK)\tau}\right\|\right)\varepsilon = 0.74.$$

Theorem 2 guarantees that $T_{\tau,\eta}(\Sigma)$, as defined in (9), satisfies the required approximation of $T_\tau(\Sigma)$. We now construct $T_{2,0.74}(\Sigma)$. In this case we can explicitly compute $\mathcal{R}_D^2$, obtaining $\mathcal{R}_D^2 = [-0.67, 0.67] \times \{0\}$. Therefore the required transition system is:

$$T_{2,0.74}(\Sigma) = (Q_1, L_1, W_1, \longrightarrow_1, O_1, H_1),$$

where:

- $Q_1 = \{(i, j)' \in \mathbb{R}^2 : i, j = -\eta, 0, \eta\}$;
- $L_1 = \mathbb{R}$;
- $W_1 = conv\,((-0.67, 0)', (0.67, 0)')$;
- $\longrightarrow_1$ is illustrated in Figure 1;
- $O_1 = Q_1$;
- $H_1 = \iota : Q_1 \to O_1$.

Even though we do not show labels in Figure 1, we briefly discuss in the following how we can find the set of *all* labels $(\ell, w) \in L_1 \times W_1$ that ensure a transition $q \overset{\ell_1, w_1}{\longrightarrow}_1 p$ in $T_{2,0.74}(\Sigma)$, for any $q, p \in Q_1$. By setting:

$$\mathcal{B}_1(0) = \{x \in \mathbb{R}^2 : \bar{B}x \leq \bar{b}\},\ W_1 = \{x \in \mathbb{R}^2 : \bar{W}x \leq \bar{w}\},$$

for some appropriate matrices $\bar{B}$ and $\bar{W}$, and vectors $\bar{b}$ and $\bar{w}$, the set in the left hand side of (11), can be rewritten in terms of linear matrix inequalities, as follows:

$$\begin{bmatrix} \bar{B}B_\tau & \bar{B} \\ 0 & \bar{W} \end{bmatrix} \begin{bmatrix} \ell_1 \\ w_1 \end{bmatrix} \leq \begin{bmatrix} \eta\bar{b} + \bar{B}(p - A_\tau q) \\ \bar{w} \end{bmatrix}, \tag{16}$$

which is indeed, the required set of all labels ensuring the transition $q \overset{\ell_1, w_1}{\longrightarrow}_1 p$. Notice that such transition exists if and only if the set described by (16) is nonempty. This check can be performed by using standard results on linear matrix

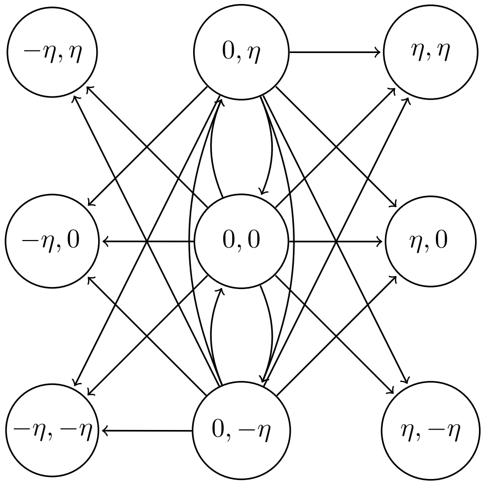

Fig. 1. Symbolic model of the linear control system (1) with dynamical matrices and constraints given in (15).

inequalities [9], as for example linear programming. As an illustrative example, the set of labels $(\ell_1, w_1) \in L_1 \times W_1$ that allow a transition from state $(0, -\eta)'$ to state $(-\eta, \eta)'$ is given by:

$$\begin{bmatrix} 31,91 & 1 & 0 \\ -31.91 & -1 & 0 \\ 1.26 & 0 & 1 \\ -1.26 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} \ell_1 \\ w_1^1 \\ w_1^2 \end{bmatrix} \leq \begin{bmatrix} 31.53 \\ -30.06 \\ 1.93 \\ -0.46 \\ 0.67 \\ 0.67 \\ 0 \\ 0 \end{bmatrix}$$

where we set $w_1 = (w_1^1, w_1^2)' \in \mathcal{R}_D^2$.

VI. Discussion

In this paper we showed that if a linear control system with disturbances is asymptotically stabilizable there always exists a surjective alternating ε–approximate simulation from the symbolic model to the control system, with a precision that can be rendered as small as desired.

While previous approaches make use of a finite number of control signals in the construction of the finite abstraction, the proposed symbolic model captures the effect of any piecewise–constant control input and any measurable disturbance input acting on the system. This approach therefore, provides a finer description of the linear control systems considered, than the ones appearing in the previous literature. Furthermore, the proposed model can be constructed in a finite number of steps, by using standard techniques in the context of linear matrix inequalities.

In the companion paper [17], existence of approximately bisimilar[1] symbolic models of nonlinear control systems is studied. While important from the conceptual point of view, further work is required towards computational efficient algorithms for constructing the symbolic models of [17].

In many cases the constructed symbolic model contains more information than what is needed for synthesizing controllers. This can be avoided by integrating the construction of the symbolic model with the synthesis of the controller. We are currently exploiting these ideas, by adapting techniques from on–the–fly verification [18] of transition systems to find efficient algorithms for the controller design.

[1]Two transition systems are approximate bisimilar if they admit a symmetric surjective approximate simulation relation. We refer to [12], [3] for a formal notion of approximate bisimulation.

References

[1] M. Egerstedt, E. Frazzoli, and G. J. Pappas, *IEEE Transactions of Automatic Control*, vol. 51, no. 6, June 2006, special Issue on Symbolic Methods for Complex Control Systems.

[2] P. Tabuada and G. Pappas, "Linear Time Logic control of discrete-time linear systems," *IEEE Transactions on Automatic Control*, vol. 51, no. 12, pp. 1862–1877, 2006.

[3] P. Tabuada, "Approximate simulation relations and finite abstractions of quantized control systems," in *Hybrid Systems: Computation and Control*, ser. Lecture Notes in Computer Science, A. Bemporad, A. Bicchi, and G. Buttazzo, Eds. Berlin: Springer Verlag, 2007, vol. 4416, pp. 529–542.

[4] P. Ramadge and W. Wonham, "Supervisory control of a class of discrete event systems," *SIAM Journal on Control and Optimization*, vol. 25, no. 1, pp. 206–230, 1987.

[5] A. Arnold, A. Vincent, and I. Walukiewicz, "Games for synthesis of controllers with partial observation," *Theoretical Computer Science*, vol. 28, no. 1, pp. 7–34, 2003.

[6] W. Zielonka, "Infinite games on finitely coloured graphs with applications to automata on infinite trees," *Theoretical Computer Science*, vol. 200, pp. 135–183, 1998.

[7] A. Bicchi, A. Marigo, and B. Piccoli, "On the rechability of quantized control systems," *IEEE Transaction on Automatic Control*, April 2002.

[8] ——, "Feedback encoding for efficient symbolic control of dynamical systems," *IEEE Transaction on Automatic Control*, vol. 51, no. 6, pp. 987– 1002, June 2006.

[9] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*, ser. Studies in Applied Mathematics. Philadelphia, PA: SIAM, June 1994, vol. 15.

[10] R. Milner, *Communication and Concurrency*. Prentice Hall, 1989.

[11] D. Park, "Concurrency and automata on infinite sequences," ser. Lecture Notes in Computer Science, Springer-Verlag, Ed., vol. 104, 1981, pp. 167–183.

[12] A. Girard and G. Pappas, "Approximation metrics for discrete and continuous systems," *IEEE Transactions on Automatic Control*, vol. 52, no. 5, pp. 782–798, 2007.

[13] R. Alur, T. Henzinger, O. Kupferman, and M. Vardi, "Alternating refinement relations," in *Proceedings of the 8th International Conference on Concurrence Theory*, ser. Lecture Notes in Computer Science, no. 1466. Springer, 1998, pp. 163–178.

[14] P. Varaiya, "Reach set computation using optimal control," in *Proceedings of the KIT Workshop on Verification of Hybrid Systems*, Grenoble, France, 1998, pp. 377–383.

[15] I. Hwang, D. Stipanovic, and C. Tomlin, "Polytopic approximations of reachable sets applied to linear dynamic games and to a class of nonlinear systems," in *Advances in Control, Communication Networks, and Transportation Systems: In Honor of Pravin Varaiya*, ser. Systems and Control: Foundations and Applications, E. Abed, Ed. Boston, MA: Birkhuser, 2005.

[16] P. Caravani and E. D. Santis, "A polytopic game," *Automatica*, vol. 36, no. 7, pp. 973–981, July 2000.

[17] G. Pola, A. Girard, and P. Tabuada, "Approximately bisimilar symbolic models for nonlinear control systems," in *46th IEEE Conference on Decision and Control*, New Orleans, LA, December 2007.

[18] S. Tripakis and K. Altisen, "On-the-fly controller synthesis for discrete and dense-time systems," in *World Congress on Formal Methods in the Development of Computing Systems*, ser. Lecture Notes in Computer Science. Berlin: Springer Verlag, September 20th-24th 1999, vol. 1708.