Abstraction by projection and application to multi-affine systems

Eugene Asarin[1] and Thao Dang[2]

[1] LIAFA,
Université Paris 7, Case 7014, 2 place Jussieu, 75251 Paris 5, France
Eugene.Asarin@liafa.jussieu.fr
[2] VERIMAG,
Centre Equation, 2 av de Vignate, 38610 Gières, France
Thao.Dang@imag.fr

Abstract. In this paper we present an abstraction method for nonlinear continuous systems. The main idea of our method is to project out some continuous variables, say z, and treat them in the dynamics of the remaining variables x as uncertain input. Therefore, the dynamics of x is then described by a differential inclusion. In addition, in order to avoid excessively conservative abstractions, the domains of the projected variables are divided into smaller regions corresponding to different differential inclusions. The final result of our abstraction procedure is a hybrid system of lower dimension with some important properties that guarantee convergence results. The applicability of this abstraction approach depends on the ability to deal with differential inclusions. We then focus on uncertain bilinear systems, a simple yet useful class of nonlinear differential inclusions, and develop a reachability technique using optimal control. The combination of the abstraction method and the reachability analysis technique for bilinear systems allows to treat multi-affine systems, which is illustrated with a biological system.

1 Introduction

Recent developments in embedded control systems have motivated much research on automated verification of continuous and hybrid systems. For systems involving non-trivial continuous dynamics (described by differential equations), exact and approximate reachability analysis methods have been developed [16, 22, 9, 3, 20, 24]. Even though these methods have been used to treat interesting case studies, the complexity of reachability computations currently limits the application to small size systems. In order to scale to larger systems, abstraction methods have been investigated (see [9, 32, 2, 31, 26]). Roughly speaking, abstraction is a general approach allowing to deduce properties of a system by analyzing a more abstract and, in general, smaller system (see [10, 8] and references therein). Some of the abstraction methods for hybrid systems, inspired by techniques from program analysis, aim at extracting (exactly or approximately) a finite-state model from a continuous/hybrid system while the other exploit the structure of the system in order to reduce it into a system of smaller dimension which preserves the properties of interest. In addition, the methods based on approximating continuous systems by hybrid systems with simpler continuous dynamics [28, 18, 4], that we call 'hybridization-based' methods, can also be viewed as an abstraction approach.

In this work, we propose an abstraction method for dimension reduction, which is along the lines of the hybridization-based approach. Our first observation is that in many practical systems, the properties to verify involve only a subset of variables, and the other variables may not need to be analyzed with great accuracy. The main idea of our method is to project out some continuous variables, say z, and treat them in the dynamics of the remaining variables x as uncertain input. Therefore, the dynamics of x is then described by a differential inclusion. In addition, in order to avoid excessively conservative abstractions, the domains of the projected variables are divided into smaller regions corresponding to different differential inclusions. The final result of our abstraction procedure is a hybrid system of lower dimension with some important properties that guarantee convergence results. However, this abstraction method does not solve the verification problem by itself. The success depends on the ability to deal with differential inclusions. We thus focus on the reachability problem for uncertain bilinear systems, a simple yet useful class of nonlinear differential inclusions. The combination of the abstraction method and the reachability analysis method for bilinear systems allows to treat multi-affine systems, which can be found in numerous applications in engineering, biology and economics.

The rest of the paper is organized as follows. In Section 2 we present our abstraction method and the convergence results. Section 3 is devoted to a reachability analysis method for uncertain bilinear systems, which is motivated by the application to multi-affine systems. This reachability technique uses results from optimal control. Section 4 contains an example of a biological system illustrating the theoretical results of the paper.

2 Abstraction by projection

2.1 Basic idea

We consider a continuous system

$$\begin{cases} \dot{x} = f(x, z) \\ \dot{z} = g(x, z) \end{cases} \tag{1}$$

where $x \in \mathcal{X} \subseteq \mathbb{R}^n$, $z \in \mathcal{Z} \subseteq \mathbb{R}^m$. We assume that the state space of the system is compact and the functions f, g are Lipschitz continuous. Given a vector x we use the notation x_i to denote the i^{th} component of x.

Suppose that we want to reduce the dimension of the system (1) from $n+m$ to n by projecting out the variables z. As in qualitative simulation, the first step of the abstraction is to partition the domain of z into disjoint regions, and in each region the dynamics of x is approximated by a *differential inclusion* which is obtained from $f(x,z)$ by letting z to take any value in the region. In other words, the effect of z in the dynamics of x is modeled as uncertain external input. Let us now formalize this idea.

We suppose that the domain of variable z_i is an interval $\mathcal{I}_i = [\underline{z}_i, \bar{z}_i]$, and the domain of z is thus a box $\mathcal{B} = \mathcal{I}_1 \times \mathcal{I}_2 \times \ldots \times \mathcal{I}_m$. We partition each interval $\mathcal{I}_i$ into k disjoint intervals[3] of the form $\{\mathcal{I}_i^1 = [\underline{z}_i^1, \bar{z}_i^1), \mathcal{I}_i^2 = [\underline{z}_i^2, \bar{z}_i^2), \ldots, \mathcal{I}_i^k = [\underline{z}_i^k, \bar{z}_i^k]\}$ such that $\underline{z}_i^1 = \underline{z}_i$, $\bar{z}_i^k = \bar{z}_i$ and for all $j \in \{1, \ldots, k-1\}$ $\bar{z}_i^j = \underline{z}_i^{j+1}$. Therefore, the box $\mathcal{B}$ is partitioned into k^m boxes, and we denote by $\mathcal{B}^{\mathbf{i}}$ with $\mathbf{i} \in \mathbb{N}^m$ the box $\mathcal{I}_1^{\mathbf{i}_1} \times \ldots \times \mathcal{I}_m^{\mathbf{i}_m}$. In the following we shall approximate the $(n+m)$-dimensional continuous system (1), referred to as the original system, by a *hybrid automaton* with n continuous variables.

Each box $\mathcal{B}^{\mathbf{i}}$ corresponds to a location $loc^{\mathbf{i}}$ of the approximating hybrid automaton where the dynamics of x is approximated by the following differential inclusion: $\dot{x} \in F^{\mathbf{i}}(x) = \{f(x,z) \mid z \in \mathcal{B}^{\mathbf{i}}\}$. The transitions of this hybrid automaton correspond to the reachability relation between the boxes $\mathcal{B}^{\mathbf{i}}$ of the original system (1), which can be abstracted as follows. Note that since (1) is continuous, only transitions between adjacent boxes need to be considered. For our further developments, we need to introduce some additional notations. The boxes $\mathcal{B}^{\mathbf{i}}$ and $\mathcal{B}^{\mathbf{j}}$ are called *adjacent* if $|\mathbf{j}_i - \mathbf{i}_i| \leq 1$ for all i and $\mathbf{i} \neq \mathbf{j}$. We denote by $d(\mathbf{i},\mathbf{j}) = \{i \mid 1 \leq i \leq m \ \wedge \ \mathbf{j}_i \neq \mathbf{i}_i|\}$ the set of indices at which the components of $\mathbf{i}$ and $\mathbf{j}$ differ. We use $\partial(\mathcal{B}^{\mathbf{i}}, \mathcal{B}^{\mathbf{j}})$ to denote the common boundary of the boxes. Given two adjacent boxes $\mathcal{B}^{\mathbf{i}}$ and $\mathcal{B}^{\mathbf{j}}$, the condition for the transition from $\mathcal{B}^{\mathbf{i}}$ to $\mathcal{B}^{\mathbf{j}}$, denoted by $\mathcal{B}^{\mathbf{i}} \to \mathcal{B}^{\mathbf{j}}$, is:

$$\exists z \in \partial(\mathcal{B}^{\mathbf{i}}, \mathcal{B}^{\mathbf{j}}) \ \forall i \in d(\mathbf{i},\mathbf{j}) : (\mathbf{j}_i - \mathbf{i}_i) g_i(x,z) \geq 0 \tag{2}$$

where g_i denotes the i^{th} component of g. The above condition says that the transition from a box to one of its adjacent boxes is possible if there exists at least one point on the common boundary of the two boxes at which the derivative of z points into the arrival box. As an example, for two adjacent boxes $\mathcal{B}^{\mathbf{i}}$ and $\mathcal{B}^{\mathbf{j}}$ such that $\mathbf{j}_i = \mathbf{i}_i + 1$ and $\mathbf{j}_j = \mathbf{i}_j$ for all other $j \neq i$, the condition for the transition $\mathcal{B}^{\mathbf{i}} \to \mathcal{B}^{\mathbf{j}}$ is $g_i(x, \bar{z}^i) \geq 0$. Similarly, the condition for the transition $\mathcal{B}^{\mathbf{j}} \to \mathcal{B}^{\mathbf{i}}$ is $g_i(x, \bar{z}^i) \leq 0$. Obviously, the condition (2) is not sufficient since it only implies that there exists a trajectory of the original system that goes from one box to an adjacent box. Hence, the resulting hybrid system is an over-approximation of the original continuous system. The approximating system where z is scalar is shown in Figure 1.

2.2 Remedy discontinuities

It should be noted that the way we project out the variables z introduces discontinuities in the derivative of the remaining variables x. For the sake of well-posedness, as in the sliding mode[4] approaches, we shall "convexify" the dynamics

[3] For simplicity of notation, we choose the same number of intervals for all z_i.

[4] The literature of sliding mode control is vast, see for example [34, 1].

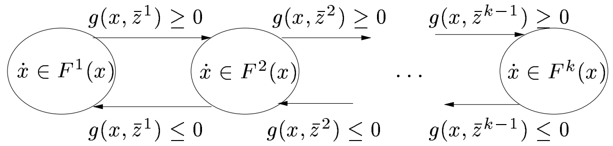

Fig. 1. Hybrid automaton obtained after projecting out the variables z.

of the abstract system in order to guarantee the existence of solutions [14] as well as an error bound of the approximation of the solution set.
Let $\mathcal{B}^{\mathbf{i}}$ and $\mathcal{B}^{\mathbf{j}}$ be two adjacent boxes. Between the locations $loc^{\mathbf{i}}$ and $loc^{\mathbf{j}}$, we add a location $loc^{\mathbf{ij}}$ whose continuous dynamics is defined as: $\dot{x} \in F^{\mathbf{ij}}(x) = co\{F^{\mathbf{i}}(x), F^{\mathbf{j}}(x)\}$ where co denotes the closed convex hull. The resulting system is illustrated in Figure 2. For brevity, we denote the approximating system of

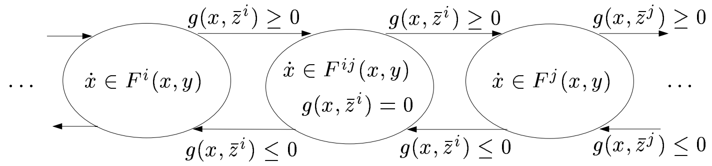

Fig. 2. Approximating hybrid system with upper semi-continuous dynamics.

Figure 2 by

$$\dot{x} \in \mathcal{F}(x). \tag{3}$$

The above "convexification" provides the system (3) with an important property stated in the following lemma.

Lemma 1. *The multifunction $\mathcal{F}$ in (3) is one-sided Lipschitz and upper semi-continuous.*

The concepts of one-sided Lipschitz and upper semi-continuity are recalled in the proof of the lemma, presented in Appendix.
To quantify the error between the original and approximating systems, we first define the size of the discretization of z. The diameter of the box $\mathcal{B}^{\mathbf{i}}$ is $diam(\mathcal{B}^{\mathbf{i}}) = \max\{|z - z'| : z \in \mathcal{B}^{\mathbf{i}} \wedge z' \in \mathcal{B}^{\mathbf{i}}\}$ where $|\cdot|$ is the Euclidean norm. Then, the size of the discretization of z is $\delta_z = \max_{\mathbf{i}}\{diam(\mathcal{B}^{\mathbf{i}})\}$.

Lemma 2. *Let δ_z be the size of the discretization of z and L_f be the Lipschitz constant of the function f in (1). Let $(x(\cdot), z(\cdot))$ be a solution of (1). Then, for all $t \geq 0$ $d_H(\dot{x}(t), \mathcal{F}(x(t))) \leq L_f \delta_z$ where d_H is the Haussdorf distance.*

The above lemma gives a bound on the distance between the derivatives of the original system and the approximating system. Using the one-sided Lipschitz and upper semi-continuity properties of the approximating system, we can establish the following convergence result.

Theorem 1. *Let $x(\cdot)$ and $z(\cdot)$ be absolutely continuous functions satisfying (1). Then, there exists a solution $\tilde{x}(\cdot)$ of (3) such that for all $t \geq 0$*

$$|x(t) - \tilde{x}(t)| \leq |x(0) - \tilde{x}(0)|e^{\mathcal{L}t} + \frac{\Delta}{\mathcal{L}}(e^{\mathcal{L}t} - 1)$$

where $\mathcal{L}$ is the Lipschitz constant of $\mathcal{F}$, and $\Delta = L_f \delta_z$ is the bound on the distance between the derivatives estimated in Lemma 2.

This theorem is proved in Appendix. The proof uses the assumption that $\mathcal{F}(x)$ is nonempty and takes closed convex values.

2.3 Abstraction with timing information

So far we have used only the sign of the derivative of z to determine the switching conditions of the hybrid system. However, the time for the system to move from one box to its adjacent boxes is omitted, in other words, in the approximating system this time can be anything between 0 and $+\infty$. To obtain a more precise abstraction, we can include information about the time the system can stay in a location, which we call *staying time*. In order to see how the information about staying time can improve the abstraction precision, we notice that in the original system a point (x, z) satisfying the condition for the transition from $\mathcal{B}^{\mathbf{i}}$ to $\mathcal{B}^{\mathbf{j}}$, such as $g(x, \bar{z}^i) \geq 0$, does not necessarily lie on the switching surface $\partial(\mathcal{B}^{\mathbf{i}}, \mathcal{B}^{\mathbf{j}})$ and thus from there the system can either continue with the dynamics of $\mathcal{B}^{\mathbf{i}}$ or switch to the dynamics of $\mathcal{B}^{\mathbf{j}}$. Consequently, for soundness, the transitions in the approximating hybrid automaton in Figures 1 and 2 are not urgent, and it is possible to stay at the same location indefinitely (i.e. no staying condition is imposed). It is clear that there may be boxes in which the original system can stay for only a finite time; hence, adding constraints on staying time at each location allows to reduce approximation error.

For a general nonlinear dynamics of z, it is not easy to estimate the staying time. A method to approximate the smallest time a linear systems with constant input can stay inside a convex polyhedron is developed in [15] and extended to uncertain linear systems in [11]. However, its generalization to nonlinear systems requires solving a nonlinear optimization problem. Here, we propose a simple method to exploit timing information by considering not only the sign but also the values of $\dot{z}$. More concretely, we additionally discretize the derivative of z into a finite number of disjoint boxes, as it is done for z. Each location of the approximating hybrid automaton now corresponds to a box $\mathcal{B}^{\mathbf{i}}$ of z and a box $\beta^{\mathbf{j}}$ of $\dot{z}$, and we label it with $loc^{\mathbf{ij}}$. Then, based on the intervals of the derivative of each component z_i, we can estimate the bounds on the staying time and then embed this information in the transition guards.

To facilitate the discussion, we introduce some definitions and notations. Location $loc^{\mathbf{ij}}$ is called a *neighbor* of location $loc^{\mathbf{pq}}$ if either the corresponding boxes $\mathcal{B}^{\mathbf{i}}$ and $\mathcal{B}^{\mathbf{p}}$ or the boxes $\beta^{\mathbf{j}}$ and $\beta^{\mathbf{q}}$ are adjacent. Location $loc^{\mathbf{ij}}$ is called the *left z_i-neighbor* of $loc^{\mathbf{pq}}$ if $\mathbf{p}_i - \mathbf{i}_i = 1$ and the *right z_i-neighbor* if $\mathbf{i}_i - \mathbf{p}_i = 1$. The *left* and *right $\dot{z}_i$-neighbors* are defined similarly.

We first specify the staying conditions of the approximating hybrid system. The staying condition of location $loc^{\mathbf{ij}}$ is simply $\dot{z} \in \beta^{\mathbf{j}}$, which can be rewritten as $G^{\mathbf{j}}(x) \cap \beta^{\mathbf{j}} \neq \emptyset$ where $G^{\mathbf{j}}(x) = \{g(x,z) \mid z \in \mathcal{B}^{\mathbf{i}}\}$. Since $g(x,z)$ is continuous[5], only transitions between neighbor locations are possible. However, we do not know the evolution of the derivative of g, therefore we let the guards of the transitions between $\dot{z}$-neighbors be *true*, meaning that the switchings between $\dot{z}$-neighbors are only restricted by the staying conditions of the locations. To define the guards of the transitions between z-neighbors, we shall use the bounds on $\dot{z}$ to estimate the time $t_{\mathbf{ij}}$ the system can stay within a location $loc^{\mathbf{ij}}$. Again, we illustrate the idea with the case where z is scalar, i.e. $m = 1$. Consider location $loc^{\mathbf{ij}}$ which corresponds to intervals $[\underline{z}^i, \bar{z}^i)$ of z and $[\underline{\xi}^j, \overline{\xi}^j)$ of $\dot{z}$. We distinghuish the following 3 cases: (1) If $\overline{\xi}^j < 0$, then a transition from $loc^{\mathbf{ij}}$ to its right z-neighbor is impossible. The staying time is $t_{\mathbf{ij}} \in [(\bar{z}^i - \underline{z}^i)/|\underline{\xi}^j|, (\bar{z}^i - \underline{z}^i)/|\overline{\xi}^j|)$ if $\underline{\xi}^j \neq -\infty$ and $t_{\mathbf{ij}} < (\bar{z}^i - \underline{z}^i)/|\overline{\xi}^j|$ otherwise; (2) If $\underline{\xi}^j > 0$, then a transition from $loc^{\mathbf{ij}}$ to its left z-neighbor is impossible and the bounds on $t_{\mathbf{ij}}$ are defined similarly; (3) If $\overline{\xi}^j \geq 0 \ \wedge \underline{\xi}^j \leq 0$, then the transitions from $loc^{\mathbf{ij}}$ to its both left and right z-neighbors are possible. However, unlike in the two previous cases, the staying time $t_{\mathbf{ij}}$ may range from 0 to $+\infty$.

2.4 Application to multi-affine systems

We have presented an abstraction method for nonlinear continuous systems. The resulting abstract system is simpler than the original system in terms of dimensionality, however it requires the ability to deal with nonlinear differential inclusions. In the remainder of the paper we focus on the reachability problem for a class of differential inclusions which are *uncertain bilinear control systems.* The study of such systems is motivated by our interest in applying the abstraction approach to a large class of biological systems which are modeled as multi-affine systems [19, 23]. Indeed, by projecting out some variables of a *multi-affine system*, one can obtain an uncertain bilinear system, as illustrated in Section 4 where we study a simplified model of a biological system.

Before proceeding with the reachability problem for bilinear systems, we mention that besides the interest of bilinear systems for effective applications of our abstraction approach, these systems have received much attention over the past decades since they could represent a variety of important physical processes in engineering. A number of results related to the control of such systems can

[5] In more general cases, the discontinuities in g can be modeled explicitly by discrete transitions with resets.

be found in [25]. On the other hand, it should be noted that the problem of approximating viability kernels of differential inclusions, which is closely related to the reachability problem, was studied in [29].

3 Reachability analysis of bilinear control systems

In this section, we present a method for solving the reachability problem for uncertain bilinear systems with both multiplicative and additive control input:

$$\dot{x}(t) = f(x(t), u(t)) = Ax(t) + \sum_{j=1}^{l} u_j(t) B_j x(t) + Cu(t) \tag{4}$$

where $x \in \mathbb{R}^n$ is the state variables; $u(\cdot) \in \mathcal{U}$, the set of admissible inputs consisting of piecewise continuous functions u of the form $u : \mathbb{R}^+ \to U$, U is a bounded convex polyhedron in $\mathbb{R}^l$. The matrices A, B_j and C are of appropriate dimension.

The reachability problem for a system with uncertain input can be formulated as an optimal control. The essential idea of our reachability method is to use the Pontryagin Maximum Principle to find the inputs allowing to derive a conservative approximation of the reachable set.

3.1 Approximating the reachable set using optimal control

Let $\varphi(t, x, u(\cdot))$ denote the trajectory of (4) starting from x under input $u(\cdot)$. For a set of initial points $X_0 \subseteq \mathbb{R}^n$ and $t > 0$, the reachable set at time t is defined as: $\mathcal{R}(t, X_0) = \{\, y \mid \exists u(\cdot) \in \mathcal{U}\ \exists x \in X_0 \ : \ y = \varphi(t, x, u(\cdot))\,\}$. Indeed, we can show that $\mathcal{R}(t, X_0) = \{x \in \mathbb{R}^n \mid V(t, x) \leq 0\}$ where $V(t, x)$ is the value function: $V(t, x) = \min_{u(\cdot) \in \mathcal{U}} \{d^2(x_0, X_0) \mid x = \varphi(t, x_0, u(\cdot))\}$ where $d(x_0, X_0)$ is the distance from x_0 to X_0. For nonlinear systems, the exact solution $V(t, x)$ can be determined by solving a rather complicated HJB equation [20, 21]. Reachability methods based on solving the partial differential equations have been developed (see e.g. [33, 24]). As mentioned earlier, our approach is to use the results from optimal control to overapproximate the reachable set. More concretely, the idea is to track the evolution of the supporting hyperplanes of the initial set under some (optimal) input. This idea has been explored in [35, 5] to compute polyhedral approximations of the reachable set of linear control systems.

Let $\mathcal{H}$ be a hyperplane with the normal vector v that supports the initial set X_0 at point p. Then, for all points $x \in X_0$ we have

$$\langle v, x \rangle - \langle v, p \rangle \leq 0 \tag{5}$$

where $\langle \cdot, \cdot \rangle$ is the scalar product. The following result is obtained by applying the Pontryagin Maximum Principle (see [27]).

Theorem 2. *Let $S(t)$ be the halfspace defined as $S(t) = \{x \in \mathbb{R}^n \mid \rho(t,x) \leq 0\}$ where $\rho(t,x) = \langle \tilde{q}(t), x\rangle - \langle \tilde{q}(t), \tilde{x}(t)\rangle$ such that $\tilde{q}(t)$ and $\tilde{x}(t)$ are solutions of the following Hamiltonian system with the maximality condition:*

$$\dot{\tilde{x}} = A\tilde{x} + \sum_{j=1}^{l} \tilde{u}_j B_j \tilde{x} + C\tilde{u} \tag{6}$$

$$\dot{\tilde{q}} = -\frac{\partial H}{\partial x}(\tilde{x}, \tilde{q}, \tilde{u}) \quad \textit{where } H(q,x,u) = \langle q, Ax + \sum_{j=1}^{l} u_j B_j x + Cu\rangle \tag{7}$$

$$\tilde{u}(t) \in argmax\{\langle \tilde{q}(t), \sum_{j=1}^{l} u_j B_j \tilde{x}(t) + Cu\rangle \mid u \in U\} \tag{8}$$

with initial conditions: $\tilde{q}(0) = v$, $\tilde{x}(0) = p$. Then, $\forall t > 0 : \mathcal{R}(t, X_0) \subseteq S(t)$, and $\mathcal{H}(t) = \{x \in \mathbb{R}^n \mid \rho(t,x) = 0\}$ is a supporting hyperplane of $\mathcal{R}(t, X_0)$.

The proof of the theorem can be found in Appendix. We note that the Hamiltonian H in (7) is affine with respect to u, therefore the input $\tilde{u}$ takes its values in the boundary of the polyhedron U. Furthermore, we assume the optimality of $\tilde{u}$, and for a bilinear system this assumption can be effectively verified using sufficient optimality conditions in [30].

Theorem 2 provides a method to overapproximate the reachable set of (4). Indeed, by the theorem, for every face of the initial polyhedron X_0 there exists an input such that tracking the evolution of the face under this input is sufficient to derive a polyhedral overapproximation of the reachable set. However, solving the optimal control problem (6)-(8) for a bilinear system under a general class of input functions is difficult, we therefore restrict to piecewise constant inputs. This allows more tractable solutions and, in addition, the error inherent to the restriction can be estimated and controled, as we shall show in the next section.

3.2 Reachability algorithm for uncertain bilinear control systems

Suppose that the initial polyhedron X_0 can be represented as intersection of a finite number n_f of halfspaces: $X_0 = \bigcap_{\nu=1}^{n_f} S^\nu$ where $S^\nu = \{x \mid \langle v^\nu, x\rangle \leq \langle v^\nu, p^\nu\rangle\}$, v^ν is the outward normal vector and p^ν is a point on the face of S^ν.

Let us recall that for tractability purposes, we shall solve the optimal problem (6)-(8) in Theorem 2 for a class of piecewise constant inputs. Given the set of admissible inputs $\mathcal{U}$ and a time step $h > 0$, we define a set $\mathcal{U}_h$ of piecewise constant inputs:

$$\mathcal{U}_h = \{u(\cdot) \in \mathcal{U} \mid u(\cdot) \text{ is constant on } (t^k, t^{k+1}),\ t^k = kh,\ k > 0\}. \tag{9}$$

We consider the following bilinear equations with $\nu = 1, \ldots, n_f$ which describe the evolution of the normal vectors v^ν and supporting points p^ν of the faces of the initial set X_0:

$$\begin{cases} \dot{q}^\nu(t) = -(A + \sum_{j=1}^{l} u_j^\nu(t) B_j)^T q^\nu(t), \\ \dot{x}^\nu(t) = A x^\nu(t) + \sum_{j=1}^{l} u_j^\nu(t) B_j x^\nu(t) + C u^\nu(t), \\ u^\nu(t) \in \arg\max \ \{\langle q^\nu(t), \sum_{j=1}^{l} u_j B_j x_i(t) + C u \rangle \mid u \in U\}, \\ q^\nu(0) = v^\nu; \quad x^\nu(0) = p^\nu \quad \text{(initial condition)}. \end{cases} \tag{10}$$

The superscript T denotes the transpose of a matrix. We denote by $\hat{\mathcal{P}}(\cdot)$ the polyhedron constructed from the solution $(x^\nu(\cdot), q^\nu(\cdot), u^\nu(\cdot))$ of (10) under the set $\mathcal{U}$ of admissible inputs: $\hat{\mathcal{P}}(t) = \bigcap_{\nu=1}^{nf} \ \{x \mid \langle q^\nu(t), x \rangle \leq \langle q^\nu(t), x^\nu(t) \rangle\}$. If the set of admissible inputs is $\mathcal{U}_h$ defined in (9), we denote the corresponding polyhedron by $\hat{\mathcal{P}}_h(t)$. Note that by Theorem 2, $\mathcal{R}(t, X_0) \subseteq \hat{\mathcal{P}}(t)$.

Theorem 3. *For all $t > 0$ the Haussdorf distance between $\hat{\mathcal{P}}(t)$ and $\hat{\mathcal{P}}_h(t)$ satisfies: $d_H(\hat{\mathcal{P}}(t), \hat{\mathcal{P}}_h(t)) \leq \mathcal{C} h^2$, where $\mathcal{C}$ is a constant depending only on $|U|$ and the norm of the matrices A, B and C of (4).*

The above theorem shows that the error due to the restriction to piecewise constant inputs is quadratic in the discretization time step h. This bound is proved by using arguments similar to those in the paper [36], which investigated the problem of second order time-discretization of control systems. The proof (together with a formula describing the relation between the constant $\mathcal{C}$, $|U|$ and the norm of the matrices) is omitted due to space limitation and it can be found in [11]. In the remainder of this section, we assume that we are provided with a scheme to solve the bilinear system (4) under a fixed piecewise constant input $u(\cdot) \in \mathcal{U}_h$, which has the form:

$$\begin{cases} x^\nu(t^{k+1}) = \alpha^\nu(x^\nu(t^k), u(t^k)), \\ q^\nu(t^{k+1}) = \beta^\nu(q^\nu(t^k), u(t^k)), \\ t^k = kh, \quad \nu = 1, \ldots, n_f. \end{cases} \tag{11}$$

where $u(t^k)$ is the value of input $u(t)$ for all $t \in [t^k, t^{k+1})$. The development of such a scheme is defered to Section 3.3.

The procedure for overapproximating the reachable set of uncertain control bilinear systems is summarized in Algorithm 1. Each iteration k produces a polyhedral approximation $\hat{\mathcal{P}}_h(t^{k+1})$ of the reachable set at time $t^k = kh$. First, for each halfspace $S^\nu(t^k)$ represented by normal vector $\tilde{q}^\nu(t^k)$ and supporting point $\tilde{x}^\nu(t^k)$, the value $\tilde{u}^\nu(t^k)$ of the optimal piecewise constant input for the time interval $[t^k, t^{k+1})$ is computed using the maximality condition. Note that this can be done by solving a linear programming problem. Once $\tilde{u}^\nu(t^k)$ is determined, the new normal vector $\tilde{q}^\nu(t^{k+1})$ and supporting point $\tilde{x}^\nu(t^{k+1})$ are then computed using (11). Finally, the polyhedron $\hat{\mathcal{P}}_h(t^{k+1})$ is the intersection of the new halfspaces. Algorithm 1 produces indeed an overapproximation of the reachable set of the system (4) with the set $\mathcal{U}_h$ of admissible inputs. Using Theorem 3, we can enlarge the sets $\hat{\mathcal{P}}_h(t^{k+1})$ by the error bound to obtain an overapproximation of the reachable set of the original system.

Algorithm 1 Reachability algorithm for uncertain bilinear systems

for all $\nu \in \{1, \ldots, n_f\}$ $\tilde{x}^\nu(0) = v^\nu$, $\tilde{q}^\nu(0) = p^\nu$
$k = 0$ /* *(k_{max} is the maximal number of iterations)* */
while $k \leq k_{max}$ **do**
  $t^{k+1} = (k+1)h$
  for all $\nu \in \{1, \ldots, n_f\}$ **do**
    $\tilde{u}^\nu(t^k) \in \arg\max \ \{\langle \tilde{q}^\nu(t^k), \sum_{j=1}^{l} u_j B_j \tilde{x}^\nu(t^k) + Cu \rangle \mid u \in U\}$
    $\tilde{x}^\nu(t^{k+1}) = \alpha^\nu(\tilde{x}^\nu(t^k), \tilde{u}^\nu(t^k))$; $\tilde{q}^\nu(t^{k+1}) = \beta^\nu(\tilde{q}^\nu(t^k), \tilde{u}^\nu(t^k))$
    $S^\nu(t^{k+1}) = \{x \mid \langle \tilde{q}^\nu(t^{k+1}), x \rangle \leq \langle \tilde{q}^\nu(t^{k+1}), \tilde{x}^\nu(t^{k+1}) \rangle\}$
  end for
  $\hat{\mathcal{P}}_h(t^{k+1}) = \bigcap_{\nu=1}^{nf} S^\nu(t^{k+1})$, $k = k+1$
end while

3.3 Approximate solution of bilinear systems with piecewise constant input

In this section, we present a method to solve a bilinear system with piecewise constant input, which is used as the scheme (11) in Algorithm 1.

We assume a fixed input $u(\cdot) \in \mathcal{U}_h$ such that $\forall k \geq 0 \, \forall t \in [t^k, t^{k+1}) \ u(t) = u^k \in U$ where $t^k = kh$. For simplicity, we denote by $x^k = x(t^k)$ the reachable state at time t^k under such input $u(\cdot)$. The problem now is to determine the reachable state x^{k+1} from x^k. In all the formulas that follow, the superscript k of a term is used to indicate that its value depends on the interval k.

Since the input remains constant during $[kh, (k+1)h)$, given x^k one can compute x^{k+1} using the flow of affine vector field $A^k x + Cu^k$ where $A^k = A + \sum_{j=1}^{l} u_j^k B_j$, that is, $x^{k+1} = e^{hA^k}(x^k + \int_0^h e^{-\tau A^k} Cu^k d\tau)$. However, to do so, the transition matrix needs to be evaluated for each time interval since A^k depends on u^k. We present in the following an efficient computation scheme which requires matrix exponential computation only once.

The main idea is to consider the bilinear term in (4) during each time interval $[kh, (k+1)h)$ as independent input, in other words, the bilinear system is treated as a time invariant linear system with input $\sum_{j=1}^{l} u_j(t) B_j x(t) + C\,u(t)$. For brevity, we denote $W^k = \sum_{j=1}^{l} u_j^k B_j$. Then,

$$x^{k+1} = e^{Ah} x^k + \int_0^h e^{A(h-\tau)} W^k x(\tau)\, d\tau + \int_0^h e^{A(h-\tau)} C u^k \, d\tau. \tag{12}$$

The second integral has a closed form. As for the first integral, we shall approximate it by replacing the exact solution $x(\tau)$ for $\tau \in [0, h)$ with a polynomial $\pi^k(\tau) = p_3^k \tau^3 + p_2^k \tau^2 + p_1^k \tau + p_0^k$ where $p_i^k \in \mathbb{R}^n$ satisfying the following Hermite interpolation conditions: $\pi^k(0) = x^k$, $\dot{\pi}^k(0) = \dot{x}(t^k)$, $\pi^k(h) = x^{k+1}$, $\dot{\pi}^k(h) = \dot{x}(t^{k+1})$. It is well-known that the coefficients of Hermite interpolating polynomials are uniquely determined [17]. After some straightforward calculations, the coefficient p_i^k can be written in the following form:

$$p_i^k = (M_i u^k + N_i) x^k + (P_i u^k + Q_i) x^{k+1} + r_i^k, \ i \in \{0, 1, 2, 3\}. \tag{13}$$

Then, developing the first integral with $x(\tau)$ replaced by $\pi(\tau)$ gives:

$$x^{k+1} = e^{Ah}x^k + \sum_{i=0}^{3} \Gamma_i W^k p_i^k + \Gamma_0 C\, u^k. \tag{14}$$

where $\Gamma_i = \int_0^h e^{A(h-\tau)}\tau^i \, d\tau$, which can also be written in a closed form. Combining (13) and (14), we obtain an affine relation between x^k and x^{k+1} of the form:

$$R^k x^{k+1} = D^k x^k + d^k, \tag{15}$$

One can see from (14) and (13) that all the terms dependent of u^k (i.e. W^k and p_i^k) do not involve matrix exponentials. Therefore, using (15) to compute reachable states x^{k+1}, we only need to compute the matrix exponential e^{Ah}.

Lemma 3. *Let $x(\cdot)$ be a solution of (4) under a fixed input $u(\cdot) \in \mathcal{U}_h$ and $\bar{x}^k$ be the approximate solution obtained by the scheme (15) with the same input $u(\cdot)$ such that $x(0) = \bar{x}^0$. If the derivative $x^{(4)}(t)$ is bounded by $\mathcal{M}$, then for all $k > 0$ $|x^k - \bar{x}^k| \leq \mathcal{M}h^4/(4!)$.*

The proof of the lemma uses standard results on the remainder term of Hermite interpolating polynomials [17], and it is omitted here. The lemma shows that the error of the scheme (15) is of order $O(h^4)$. As shown earlier, the error due to the restriction to piecewise constant inputs is quadratic; hence, this additional error does not change the order of the method.

4 Application to a biological system

In this section, we illustrate our approach with a multi-affine system, used to model the gene transcription control in the *Vibrio fischeri* bacteria. The results are obtained using an experimental implementation of the abstraction method and the reachability technique for bilinear systems presented in the previous sections. This bioregulatory network problem has been studied in [7]. The following brief description of the model is borrowed from [7]. The differential equations describing the dynamics of a mode of the system are as follows:

$$\begin{cases} \dot{x_1} = k_2 x_2 - k_1 x_1 x_3 + u_1 \\ \dot{x_2} = k_1 x_1 x_3 - k_2 x_2 \\ \dot{x_3} = k_2 x_2 - k_1 x_1 x_3 - n x_3 + n u_2 \end{cases} \tag{16}$$

The state variables x_1, x_2, x_3 represent cellular concentration of different species, and the parameters k_1, k_2, n are binding, dissociation and diffusion constants. The variables u_1 and u_2 are control variables (plasmid and external source of autoinducer). We abstract away the variable x_1 by discretizing its range and construct a hybrid automaton using the abstraction method of Section 2. The influence of x_1 in the dynamics of the variables x_2 and x_3 is modeled as an uncertain input u_x, and the resulting system is a hybrid system with uncertain bilinear dynamics. As an example, the dynamics of x_2 and x_3 of the location corresponding to the interval I^i of the values of x_1 are:

$$\begin{cases} \dot{x_2} = k_1 u_x x_3 - k_2 x_2 \\ \dot{x_3} = k_2 x_2 - k_1 u_x x_3 - n x_3 + n u_2 \\ u_x \in I^i \end{cases} \tag{17}$$

The reachability analysis results for this system are shown in Figure 3. The left figure is the reachable set of the approximate hybrid system when the control in unactivated ($u = 0$). The initial set is the rectangle X_0 where $x_2 \in [1.05, 1.55]$ and $x_3 \in [1.25, 1.95]$. We can see that the uncontrolled system can exit the rectangle $R = [1, 2] \times [1, 2]$ via the face $x_3 = 1$ while the control objective is to steer the system through the face $x_2 = 2$. In [7] the following feedback control law for this objective is designed: $u_2 = 6$ and u_1 is a multi-affine function of the state variables x. The reachability computation result for the system under this control law from the same initial set X_0 is shown in Figure 3 where on the left we can see the reachable set of the location corresponding to the interval $x_1 \in [1.0, 1.5]$ and on the right the reachable set of the location corresponding to $x_1 \in [1.5, 2]$. This result shows that indeed the controlled system is driven to the face $x_2 = 2$, as desired.

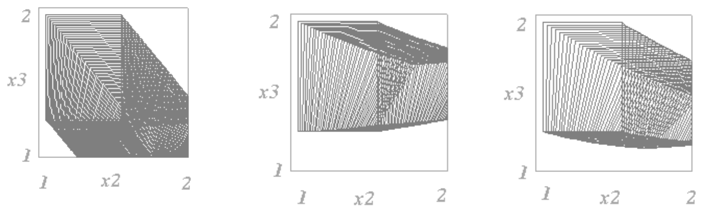

Fig. 3. Left: Reachable set of the uncontrolled system, i.e. when $u = 0$. Middle and right: Reachable set of the controlled system: location $u_x \in [1.0, 1.5]$ (middle); location $u_x \in [1.5, 2.0]$ (right), the input u_x represents the variable x_1 that is projected out.

5 Concluding remarks

In this paper, we proposed a framework for abstraction of continuous nonlinear systems by means of hybridization. We also developed a reachability algorithm for uncertain bilinear systems, necessary for an effective application of the approach to multi-affine systems. Experimental results are encouraging and various interesting research directions need to be explored. One important issue is the choice of variables to project out which still allows to prove the properties of interest. In addition, the assume-guarantee ideas from model-checking could be useful in this framework. Indeed, one can assume a reachable set for some variables z which is used as a set of input values in the computation for the remaining variables x. The reachable set of x is in turn used as the set of input values for the computation on z, which allows to verify the initial assumption. On the other hand, we intend to apply our approach to more problems in biological systems.

References

1. J.C. Alexander and T.I. Seidman. Sliding modes in intersecting switching surfaces, *Houston J. Math.*, 24:545-569, 1994.
2. R. Alur, T. Dang, and F. Ivancic. Reachability Analysis Via Predicate Abstraction. In *HSCC*, LNCS 2289, Springer, 2002.
3. E. Asarin, O. Bournez, T. Dang, and O. Maler. Approximate Reachability Analysis of Piecewise-Linear Dynamical Systems. In *HSCC*, LNCS 1790, Springer, 2000.
4. E. Asarin, T. Dang, and A. Girard. Reachability Analysis of Nonlinear Systems Using Conservative Approximation. In *HSCC*, LNCS 2623, Springer, 2003.
5. E. Asarin, T. Dang, and O. Maler. d/dt: A tool for Verification of Hybrid Systems. *Computer Aided Verification*, Springer, LNCS, 2002.
6. J.P. Aubin and A. Cellina. Differential Inclusions: Set-valued Maps and Viability Theory, Springer, 1984.
7. C. Belta, L. C. G. J. M. Habets, and V. Kumar. Control of multi-affine systems on rectangles with an application to gene transcription control. *Proc. of CDC*, 2003.
8. S. Bensalem, Y. Lakhnech,and S. Owre. Computing Abstractions of Infinite State Systems Compositionally and Automatically. In *Computer Aided Verification*, LNCS 1427, Springer, 1998.
9. A. Chutinan and B.H. Krogh. Verification of Polyhedral Invariant Hybrid Automata Using Polygonal F low Pipe Approximations. In *HSCC*, LNCS 1569, Springer, 1999.
10. P. Cousot and R. Cousot. Abstract Interpretation and Application to Logic Programs. *Journal of Logic Programming*, 103-179, 1992.
11. T. Dang. Reachability Analysis of Bilinear Systems. Tech. report IMAG, 2003.
12. K. Deimling. Multivalued Differential Equations. De Gruyter, 1992.
13. T. Donchev and E. Farkhi. Stability and Euler approximation of one-sided Lipschitz differential inclusions. *SIAM Journal of Control and Optimization*, 36(2):780-796, 2000.
14. A.F. Filippov. Diff. Equations with Discontinuous Righthand Sides. Kluwer, 1988.
15. A. Girard. Detection of Event Occurence in Piecewise Linear Hybrid Systems, *Proc. RASC'02*, December 2002, Nottingham, UK.
16. M.R. Greenstreet and I. Mitchell. Reachability Analysis Using Polygonal Projections. In *HSCC*, LNCS 1569 Springer, 1999.
17. G. Hämmerlin and K. Hoffmann. Numerical Mathematics, Springer, 1991.
18. T.A. Henzinger, P.-H. Ho, and H. Wong-Toi. Analysis of Nonlinear Hybrid Systems. *IEEE Transactions on Automatic Control* 43, 540-554, 1998.
19. D. Kirschner, S. Lenhart, and S. Serbin. Optimal control of the chemotherapy of HIV. *Journal of Mathematival Biology*, 35:775-792, 1997.
20. A. Kurzhanski and P. Varaiya. Ellipsoidal Techniques for Reachability Analysis. In *HSCC*, LNCS 1790, Springer, 2000.
21. A. Kurzhanski and P. Varaiya. Dynamic optimization for reachability problems. *JOTA*, 108(2):227-251, 2001.

22. G. Lafferriere, G. Pappas, and S. Yovine. Reachability computation for linear systems. *Proc. of the 14th IFAC World Congress*, 7-12 E, 1999.
23. U. Ledzewicz and H. Schättler. Optimal control for 3-compartment model for cancer chemotherapy with quadratic objective. *Proc. of the 4th Int Conf on Dynamical Systems and Differential Equations*, Wilmington, NC, 2002.
24. I. Mitchell and C. Tomlin. Level Set Method for Computation in Hybrid Systems. In *HSCC*, LNCS 1790, Spinger-Verlag, 2000.
25. R.R. Mohler. Nonlinear Systems, 2, Prentice-Hall, Inc., Englewood Cliffs, 1991.
26. George J. Pappas. Bisimilar linear systems, in *Automatica*, 2003.
27. L. S. Pontryagin, V. G. Boltyanskii, R. V. Gamkrelidze, and E. F. Mischenko. The Mathematical Theory of Optimal Processes. *Pergamon Press*, Oxford, 1964.
28. A. Puri and P. Varaiya. Verification of Hybrid Systems using Abstraction. In *Hybrid Systems II*, LNCS 999, Springer, 1995.
29. P. Saint-Pierre. Approximation of Viability Kernels and Capture Basin for Hybrid Systems. *Proc. of European Control Conf. ECC'01*, 2776-2783, 2001.
30. A. Sarychev. Time-optimality of bang-bang controls for chained systems. *Proc. of 2nd IFAC Workshop on Lagrangian and Hamiltonian Methods for Nonlinear Control*, 2003.
31. P. Tabuada and G. Pappas, Model-Checking LTL over controllable linear systems is decidable. In *HSCC*, LNCS 2623, Springer, 2003.
32. A. Tiwari and G. Khanna. Series of Abstractions for Hybrid Automata. In *HSCC*, LNCS 2289, Springer, 2002.
33. C. Tomlin, J. Lygeros, and S. Sastry. A Game-Theoretic Approach to Controller Design for Hybrid Systems. *Proc. of the IEEE*, 88:940-970, 2000.
34. V.I. Utkin. Sliding Modes and their Application in Variable Structure Systems. *Mir, Moscow*, 1978.
35. P. Varaiya. Reach Set Computation using Optimal Control. *Proc. KIT Workshop*, Grenoble, 1998.
36. V. Veliov. On the time-discretization of control systems. *SIAM journal on Control and Optimization*, 35(5):1470-1468, 1997.

Appendix

Proof of Lemma 1 We first recall some basic definitions and notations (see [6, 13] for more details). We denote by B the open unit ball centered at the origin. Let $\mathcal{F} : \mathbb{R}^n \to \mathcal{X}$ be a multifunction where $\mathcal{X}$ is the set of all nonempty compact subsets of $\mathbb{R}^n$. $\mathcal{F}$ is called *upper semi-continuous* (respectively *lower semi-continuous*) at $x \in \mathbb{R}^n$ if for every $\varepsilon > 0$ there exists $\delta > 0$ such that $\forall x' \in x + \delta B$ $\mathcal{F}(x') \subseteq \mathcal{F}(x) + \varepsilon B$ (respectively $\mathcal{F}(x) \subseteq \mathcal{F}(x') + \varepsilon B$). $\mathcal{F}$ is called *one-sided Lipschitz* (OSL) with a constant $\mathcal{L}$ if and only if for all $x, x' \in \mathbb{R}^n$, $f \in \mathcal{F}(x)$ there exists $f' \in \mathcal{F}(x')$ such that $\langle x - x', f - f' \rangle \leq \mathcal{L}|x - x'|^2$.

We proceed to prove Lemma 1. The condition that $\mathcal{F}$ is one-sided Lipschitz is easy to verify. To prove that $\mathcal{F}$ is upper semi-continuous, it suffices to prove that it is upper semi-continuous at the switching surfaces. Let x be a point on the switching surface $S^{\mathbf{ij}}$, hence $\mathcal{F}(x) = F^{\mathbf{ij}}(x)$. For a point $x' \in (x+\delta B) \setminus S^{\mathbf{ij}}$ (in the δ-neighborhood of x but not on the switching surface), either $\mathcal{F}(x') = F^{\mathbf{i}}(x')$ or $\mathcal{F}(x') = F^{\mathbf{j}}(x')$. Since all $F^{\mathbf{i}}$ are Lipschitz continuous, there exists $\varepsilon > 0$ $F^{\mathbf{i}}(x') \subseteq F^{\mathbf{i}}(x) + \varepsilon B$. Therefore, $\mathcal{F}(x') \subseteq \mathcal{F}(x) + \varepsilon B$. Obviously, this also holds for a point $x' \in (x + \delta B) \cap S^{\mathbf{ij}}$; hence, $\mathcal{F}$ is upper semi-continuous at x. □

Proof of Theorem 1. To prove the theorem we suppose that the multifunction $\mathcal{F}$ in (3) is one-sided Lipschitz with a constant $\mathcal{L}$ and bounded on bounded sets. We also assume that $\mathcal{F}$ is upper semi-continuous and takes closed convex values. By Lemma 2, $x(\cdot)$ is absolutely continuous and satisfies $d_H(\dot{x}(t), \mathcal{F}(x(t))) \leq \Delta$ for all $t > 0$. We shall prove that there exists a solution $\tilde{x}(\cdot)$ of $\frac{d\tilde{x}(t)}{dt} \in \mathcal{F}(\tilde{x}(t))$; $\tilde{x}(0) = \tilde{x}_0$ such that for all $t > 0$

$$|\tilde{x}(t) - x(t)| \leq |\tilde{x}(0) - x(0)|e^{\mathcal{L}t} + \frac{\Delta}{\mathcal{L}}(e^{\mathcal{L}t} - 1). \tag{18}$$

To do so, we consider the differential inclusion

$$\frac{\tilde{x}(t)}{dt} \in \mathcal{G}(\tilde{x}(t)); \quad \tilde{x}(0) = \tilde{x}_0 \tag{19}$$

where $\mathcal{G}(\tilde{x}) = \{v \in \mathcal{F}(\tilde{x}) \mid \langle x(t) - \tilde{x}, \dot{x}(t) - v\rangle \leq \mathcal{L}|x(t) - \tilde{x}|^2 + \Delta|x(t) - \tilde{x}|\}$. We shall use a well-known existence theorem for upper semi-continuous differential inclusions from [12] to prove that (19) has a solution that satisfies (18). To do so, we need to verify that $\mathcal{G}(\tilde{x})$ is nonempty, convex, closed-valued and satisfies the condition of boundedness of the solution set. We first prove that $\mathcal{G}(\tilde{x})$ is nonempty for each $\tilde{x}$. Let $w \in \mathcal{F}(x)$ be such that $|\dot{x}(t) - w| = d_H(\dot{x}(t), \mathcal{F}(x(t))) \leq \Delta$. By the OSL condition, given $\tilde{x}$, we can choose $v \in \mathcal{F}(\tilde{x})$ such that $\langle x(t) - \tilde{x}, w - v\rangle \leq \mathcal{L}|x(t) - \tilde{x}|^2$. Hence,

$$\begin{aligned}\langle x(t) - \tilde{x}, \dot{x}(t) - v\rangle &= \langle x(t) - \tilde{x}, \dot{x}(t) - w\rangle + \langle x(t) - \tilde{x}, w - v\rangle \\ &\leq |x(t) - \tilde{x}|\Delta + \mathcal{L}|x(t) - \tilde{x}|^2 \end{aligned}\tag{20}$$

The above implies that $v \in \mathcal{G}(\tilde{x})$. It is not hard to see that $\mathcal{G}(\tilde{x})$ is convex, closed-valued and satisfies the condition of boundedness of the solution set since $\mathcal{F}$ does. From Theorem 5.2 of [12] we conclude that there exists a solution $\tilde{x}(\cdot)$ of (19). Denoting $\sigma(t) = |x(t) - \tilde{x}(t)|$, σ is an absolutely continuous function. Furthermore, if $\dot{\sigma}(t)$ exists, then $\sigma(t)\dot{\sigma}(t) = \frac{1}{2}\frac{d}{dt}\sigma^2(t) = \langle x(t) - \tilde{x}(t), \dot{x}(t) - \dot{\tilde{x}}(t)\rangle \leq \mathcal{L}\sigma^2(t) + \Delta\sigma(t)$, by (20). From this, it can be shown that $\dot{\sigma}(t) \leq \mathcal{L}\sigma(t) + \Delta$ for all $t > 0$, and combining with $\sigma(0) = |x(0) - \tilde{x}(0)|$ we obtain the inequality (18). □

Proof of Theorem 2. The equation (7) can be rewritten as $\dot{\tilde{q}} = -\frac{\partial H}{\partial x}(\tilde{q}, \tilde{x}, \tilde{u}) = -(A + \sum_{j=1}^{l} \tilde{u}_j B_j)^T \tilde{q}$. For brevity, we use $x(t)$ to denote a trajectory $\varphi(t, x_0, u(\cdot))$ of (4) starting from some point $x_0 \in X_0$ under an arbitrary admissible input $u(\cdot)$. Then, $\frac{d\langle \tilde{q}(t), x(t)\rangle}{dt} = \langle \dot{\tilde{q}}(t), x(t)\rangle + \langle \tilde{q}(t), \dot{x}(t)\rangle = \langle \tilde{q}(t), -(A + \sum_{j=1}^{l} \tilde{u}_j B_j)x(t)\rangle + \langle \tilde{q}, Ax(t) + \sum_{j=1}^{l} u_j B_j x(t) + Cu(t)\rangle = \langle \tilde{q}(t), -\sum_{j=1}^{l} \tilde{u}_j B_j x(t) + \sum_{j=1}^{l} u_j B_j x(t) + Cu(t)\rangle$. By the maximality condition (8), for all admissible inputs $u(\cdot)$ and all $t > 0$, $\langle \tilde{q}(t), \sum_{j=1}^{l} u_j(t) B_j \tilde{x}(t) + Cu(t)\rangle \leq \langle \tilde{q}(t), \sum_{j=1}^{l} \tilde{u}_j(t) B_j \tilde{x}(t) + C\tilde{u}(t)\rangle$. Therefore, $\frac{d\langle \tilde{q}(t), x(t)\rangle}{dt} \leq \frac{d\langle \tilde{q}(t), \tilde{x}(t)\rangle}{dt}$. In addition, from the initial condition and (5), $\langle \tilde{q}(0), x(0)\rangle \leq \langle \tilde{q}(0), \tilde{x}(0)\rangle$. Thus, we have $\forall t > 0$ $\langle \tilde{q}(t), x(t)\rangle \leq \langle \tilde{q}(t), \tilde{x}(t)\rangle$. It then follows that every point x reachable by (4) from X_0 at time $t > 0$ satisfies $\rho(t, x) \leq 0$. □