Trajectory Based Verification Using Local Finite-Time Invariance*

A. Agung Julius and George J. Pappas

Department of Electrical and Systems Engineering
University of Pennsylvania
200 South 33rd Street, Philadelphia PA-19104
United States of America
{agung,pappasg}@seas.upenn.edu

Abstract. In this paper we propose a trajectory based reachability analysis by using local finite-time invariance property. Trajectory based analysis are based on the execution traces of the system or the simulation thereof. This family of methods is very appealing because of the simplicity of its execution, the possibility of having a partial verification, and its highly parallel structure.

The key idea in this paper is the construction of local barrier functions with growth bound in local domains of validity. By using this idea, we can generalize our previous method that is based on the availability of global bisimulation functions. We also propose a computational scheme for constructing the local barrier functions and their domains of validity, which is based on the S-procedure. We demonstrate that our method subsumes some other existing methods as special cases, and that for polynomial systems the computation can be implemented using sum-of-squares programming.

1 Introduction

One of the main problems in the field of hybrid systems is reachability analysis/safety verification. This type of problems is related to verifying that the state of a hybrid system does not enter a declared unsafe set in its execution trajectory. The domain of application of the problem is very wide, ranging from engineering design [1,2], air traffic management systems [3,4], to systems biology [5,6]. Understanding the importance of the problem, the hybrid systems community has put a lot of efforts in the research of reachability analysis and verification. We refer the reader to [7,8,9,10,11,12,13,14,15,16] for some of the earlier references in this topic[1].

* This work is partially funded by National Science Foundations awards CSR-EHS 0720518 and CSR-EHS 0509327.

[1] Given the breadth of research in this topic, this list is by no means exhaustive. However, it does capture a broad spectrum of techniques that have been developed in the community to answer the safety/reachability problems.

R. Majumdar and P. Tabuada (Eds.): HSCC 2009, LNCS 5469, pp. 223–236, 2009.

Among the different approaches to reachability analysis, there is a family of methods that is based on simulation or trajectory analysis. In some literature, this type of approach is also called *testing based* [17], referring to the possibility of generating the trajectories through actual executions (tests). This type of approach is very appealing because of several reasons [18]. One of the reasons is its simplicity. Running or simulating a system is generally much simpler than performing symbolic analysis on it. This is particularly true for systems with complex dynamics. Another reason why trajectory based verification is attractive is that its algorithm is highly parallelizable. Since simulation runs of the system do not depend one on another, they can be easily assigned to different processors, resulting in a highly parallel system. Trajectory based verification is also close to some actual practice in the industry where verification is done through "exhaustive" testing and/or simulation. Of course, formal exhaustive testing for continuous/hybrid systems is not possible, unless they are coupled with some notion of robustness, which is the central issue in this paper.

Within the family of trajectory based reachability analysis techniques itself there are different approaches. Some methods, for example, conduct state space exploration through randomized testing [19] or by using Rapidly exploring Random Trees (RRT) or its adaptations [20,21]. Methods based on linearization of the system's nonlinear dynamics along the execution trajectory have also been proposed, for example in [22,23]. Other related methods incorporate the notions of sensitivity [24], local gain/contraction analysis [25,26] and bisimulation function [27,17,28] to measure the difference between neighboring trajectories. The method that we present in this paper belongs to this class. In a sense, these methods combine two of the most successful analysis techniques for nonlinear dynamics, simulation and stability analysis. The difference between our approach and other approaches that use, for example, sensitivity analysis [24] and local gain/contraction analysis [25,26] is in the fact that we are not restricted to use a prespecified metric in the state space. In fact, the bisimulation/barrier functions induce a pseudometric that can be (locally) customized to best fit the application [17].

In this paper, we extend the approach reported in [17] (and in [18] for stochastic systems). An illustration of the approach proposed in this paper is shown in Figure 1. Suppose that we have a test trajectory that satisfies the safety condition. In the above mentioned references, we rely on the assumption of the availability of a bisimulation function for each mode of dynamics, which is valid globally, to bound the divergence of the trajectories resulting from nearby initial conditions. The contribution of this paper lies in the relaxation of this global assumption, allowing for more flexibility in the computation. Effectively, we construct a guarantee on the divergence of execution trajectories by piecing together multiple local finite-time invariance arguments. The idea is to link the domains of validity of these local invariance to cover a neighborhood of the test trajectory. In Figure 1 these domains are shown as Domain-1, 2, and 3. The local invariance arguments that we construct are similar to the barrier certificate as proposed in [14], except for the fact that the validity of the invariance property is finite time. In each of these domains, the shape of the level sets of the barrier function

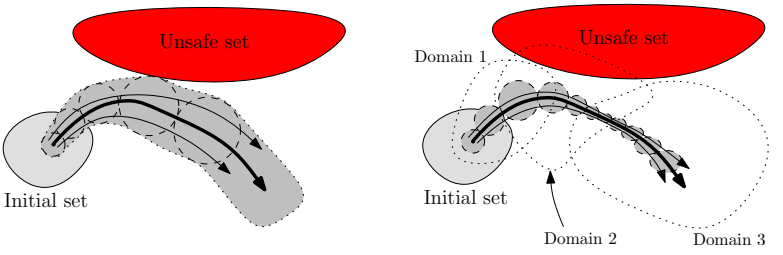

Fig. 1. The main idea presented in this paper. The test trajectory is shown as the thick curve. The use of global bisimulation function to bound the divergence of the trajectories is illustrated on the left side. Local finite-time invariance based analysis is illustrated on the right side.

and the stability property of the dynamics can be different. This is illustrated in Figure 1 by the changing of the shape and the size of the level sets.

The rest of the paper is organized as follows. In the next section, we present some basic results about local finite-time invariance of dynamical systems. The application of these results in safety verification is discussed in Section 3. In Section 4, we also propose a computational scheme to compute the barrier functions and their domains of validity based on the S-procedure [29]. We show that for affine systems, the method proposed in this paper coincides with that in [17]. We also show that our result captures, as a special case, the method based on local linearization of nonlinear systems. For polynomial systems we show that the computation can be implemented by using sum-of-squares (SOS) programming and demonstrate it with an example.

2 Local Finite-Time Invariance

We consider nonlinear dynamical system of the form

$$\dot{x} = f(x),\ x \in \mathcal{X}, \tag{1}$$

where $\mathcal{X} \subset \mathbb{R}^n$ is the state space of the system, and a differentiable function $\phi : \mathcal{X} \to \mathbb{R}_+$. We assume that the differential equation posed in (1) admits a unique solution for any initial condition in $\mathcal{X}$, during the time interval of interest, $\mathcal{T}$.

Notation. We denote the flow of the dynamical system at time t with initial condition $x(t)_{t=t_0} = x_0$ as $\xi(t; x_0, t_0)$. That is, $\xi(t; x_0, t_0)$ satisfies

$$\frac{d}{dt}\xi(t; x_0, t_0) = f(\xi(t; x_0, t_0)),$$
$$\xi(t_0; x_0, t_0) = x_0.$$

We have the natural semigroup property of the flow: $\xi(t; x_0, t_0) = \xi(t; x', t')$, where $x' := \xi(t'; x_0, t_0)$ for any $t' \in [t_0, t]$. We also have the time invariance property: $\xi(t; x_0, t_0) = \xi(t + \Delta; x_0, t_0 + \Delta)$ for any $\Delta \in \mathbb{R}$.

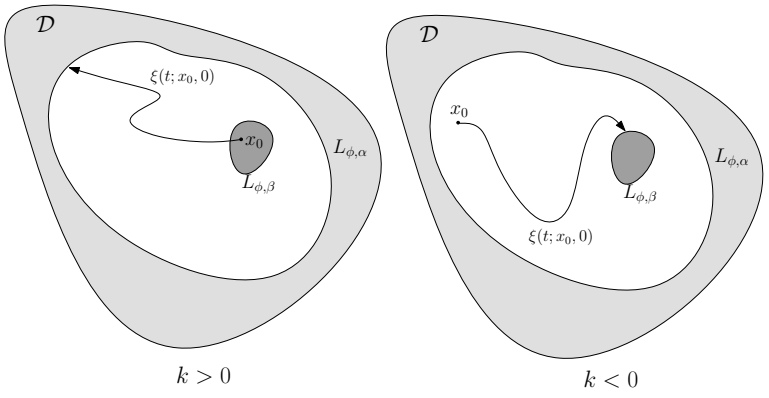

Fig. 2. Illustration for Propositions 1 and 2 for the case when $k > 0$ (left) and $k < 0$ (right)

Notation. We denote the level set of a function $\phi : \mathcal{X} \to \mathbb{R}$ as

$$L_{\phi,\alpha} := \{x \in \mathcal{X} \mid \phi(x) \leq \alpha\}. \tag{2}$$

In the subsequent discussion in this paper we need the following two results related to local finite-time invariance.

Proposition 1. *Suppose that the following relation holds for a subset $\mathcal{D} \subset \mathcal{X}$ and for some $k \in \mathbb{R}$,*

$$\nabla_x \phi(x) f(x) \leq k, \forall x \in \mathcal{D}. \tag{3}$$

Take any $\alpha, \beta \in \mathbb{R}$ such that $\beta < \alpha$ and $L_{\phi,\alpha} \subset \mathcal{D}$. The following results hold.
(i) If $k > 0$, then any trajectory of the system (1) that starts in $L_{\phi,\beta}$ remains in $L_{\phi,\alpha}$ for at least $\frac{\alpha-\beta}{k}$ time units, or mathematically

$$\xi(t; x_0, 0) \in L_{\phi,\alpha},\ \forall x_0 \in L_{\phi,\beta}, \forall t \leq \frac{\alpha - \beta}{k}.$$

(ii) If $k < 0$, then any trajectory of the system (1) that starts in $L_{\phi,\alpha}$ enters $L_{\phi,\beta}$ after at most $\frac{\beta-\alpha}{k}$ time units, or

$$\xi(t; x_0, 0) \in L_{\phi,\beta},\ \forall x_0 \in L_{\phi,\alpha}, \forall t \geq \frac{\beta - \alpha}{k}.$$

Proposition 2. *Suppose that the following relation holds for a subset $\mathcal{D} \subset \mathcal{X}$ and for some $k \in \mathbb{R}$,*

$$\nabla_x \phi(x) f(x) \leq k\phi(x), \forall x \in \mathcal{D}. \tag{4}$$

Take any $\alpha, \beta \in \mathbb{R}$ such that $\beta < \alpha$ and $L_{\phi,\alpha} \subset \mathcal{D}$. The following results hold.
(i) If $k > 0$, then any trajectory of the system (1) that starts in $L_{\phi,\beta}$ remains in $L_{\phi,\alpha}$ for at least $\frac{\ln \alpha - \ln \beta}{k}$ time units, or mathematically

$$\xi(t; x_0, 0) \in L_{\phi,\alpha},\ \forall x_0 \in L_{\phi,\beta}, \forall t \leq \frac{\ln \alpha - \ln \beta}{k}.$$

(ii) If $k < 0$, then any trajectory of the system (1) that starts in $L_{\phi,\alpha}$ enters $L_{\phi,\beta}$ after at most $\frac{\ln \beta - \ln \alpha}{k}$ time units, or

$$\xi(t; x_0, 0) \in L_{\phi,\beta},\ \forall x_0 \in L_{\phi,\alpha}, \forall t \geq \frac{\ln \beta - \ln \alpha}{k}.$$

Definition 1. *Hereafter, we call a function $\phi : \mathcal{X} \to \mathbb{R}$ that satisfies (3) or (4) a barrier function with constant and linear growth bound, respectively. The corresponding domain $\mathcal{D}$ is called the domain of validity of the barrier functions.*

Propositions 1 and 2 can be proved by using an argument similar to Lyapunov stability theory, which is a standard result in nonlinear system analysis (see, for example [30]). Effectively, the results above can be used to establish a barrier certificate that is valid for a finite time. Notice that if $\frac{\partial \phi}{\partial x} f(x)$ is continuous and $\mathcal{D}$ is a compact set, we can always find a finite bound k in (3). In a sense, this property guarantees that for any continuous function $f(x)$ and a compact domain $\mathcal{D}$, we can always construct a smooth barrier function with a finite constant growth bound.

3 Safety Verification

In this section, we extend the results in the previous section to the product of a dynamical system with itself. The goal is to establish a method for computing the robustness of test trajectories for systems with nonlinear dynamics. We consider dynamical systems in the form of (1), and suppose that there is an unsafe subset of the state space $\mathcal{X}$, which we denote by `Unsafe`. We want to verify that the execution trajectories of the system are *safe*. That is, they do not enter the unsafe set. The object of robustness computation is to establish a neighborhood around a test trajectory that is guaranteed to have the same safety property.

Consider a trajectory of the system with initial condition $x_i \in \mathcal{X}$ in the time interval $[0, T]$, as illustrated in Figure 3. Suppose that there exists a set $\mathcal{D} \subset \mathcal{X} \times \mathcal{X}$ such that the trajectory $(\xi(t; x_i, 0), \xi(t; x_i, 0)) \in \mathcal{D}$, and that the trajectory is safe, i.e. $\xi(t; x_i, 0) \notin$ `Unsafe`, for all $t \in [0, T]$. Further, for any function $\phi : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$, we define a function

$$d(t) := \inf_{y \in \texttt{Avoid}(t)} \phi(\xi(t; x_i, 0), y), \forall t \in [0, T], \tag{5}$$

$$\texttt{Avoid}(t) := \{y \mid y \in \texttt{Unsafe}, (\xi(t; x_i, 0), y) \in \mathcal{D}\} \cup \{y \mid (\xi(t; x_i, 0), y) \notin \mathcal{D}\}, \tag{6}$$

and introduce the following notation.

Notation. We introduce the level set notation

$$L^x_{\phi,\alpha} := \{y \mid \phi(x, y) \leq \alpha\}. \tag{7}$$

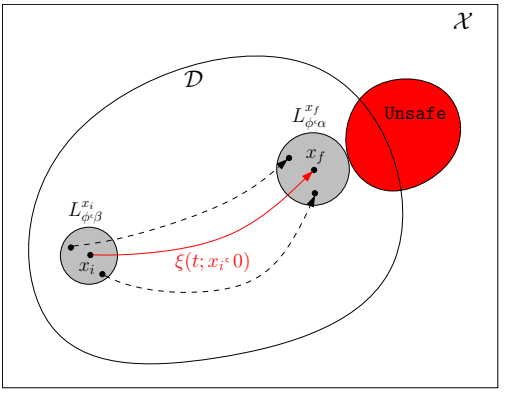

Fig. 3. Illustration for Proposition 3. The circles represent level sets of ϕ. For β that satisfies the condition in Proposition 3, any trajectory that starts in $L^{x_i}_{\phi,\beta}$ is guaranteed to possess the same safety property as $\xi(t; x_i, 0)$.

Proposition 3. *Suppose that for all $(x, y) \in \mathcal{D}$, there exists a $k \in \mathbb{R}$ such that*

$$\nabla_x \phi(x, y) f(x) + \nabla_y \phi(x, y) f(y) \leq k.$$

Let β and k' be such that

$$\beta + k't \leq d(t), \forall t \in [0, T], \tag{8}$$
$$k' \geq k. \tag{9}$$

For any initial condition $x_0 \in L^{x_i}_{\phi,\beta}$, we have that

$$\xi(t; x_0, 0) \notin \texttt{Unsafe}, \tag{10}$$
$$(\xi(t; x_i, 0), \xi(t; x_0, 0)) \in \mathcal{D}, \tag{11}$$

for all $t \in [0, T]$.

Proof. By applying Proposition 1, we can show that for all $t \in [0, T]$,

$$\phi(\xi(t; x_i, 0), \xi(t; x_0, 0)) \leq \beta + k't \leq d(t). \tag{12}$$

By definition, it implies that for all $t \in [0, T]$,

$$\phi(\xi(t; x_i, 0), \xi(t; x_0, 0)) \leq \inf_{y \in \texttt{Avoid}(t)} \phi(\xi(t; x_i, 0), y),$$

and therefore

$$\xi(t; x_0, 0) \notin \texttt{Avoid}(t).$$

By definition of $\texttt{Avoid}(t)$, this immediately implies the validity of (10 - 11).

A result similar to Proposition 3 for barrier functions with linear growth bound can be constructed as follows (the proof follows a similar construction).

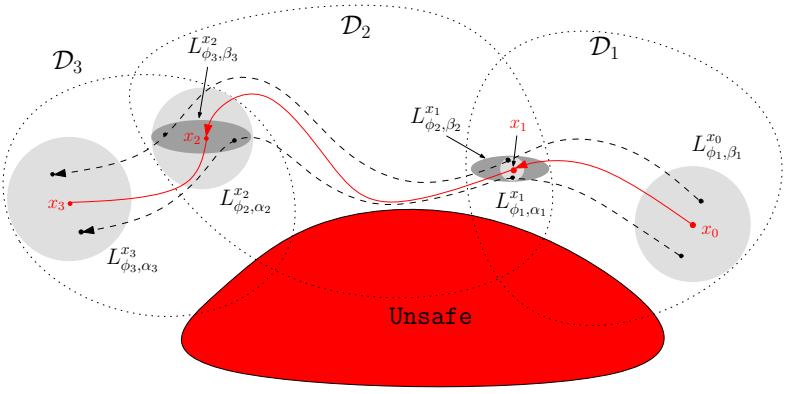

Fig. 4. Illustration of Theorem 1. The solid trajectory represents the test trajectory, while the dashed ones represent other trajectories with initial conditions in $L^{x_0}_{\phi_1,\beta_1}$.

Proposition 4. *Suppose that for all $(x, y) \in \mathcal{D}$, there exists a $k \in \mathbb{R}$ such that*

$$\nabla_x \phi(x, y) f(x) + \nabla_y \phi(x, y) f(y) \leq k\phi(x, y).$$

Let β and k' be such that

$$\ln \beta + k't \leq \ln d(t), \forall t \in [0, T], \tag{13}$$

$$k' \geq k. \tag{14}$$

For any initial condition $x_0 \in L^{x_i}_{\phi,\beta}$, we have that

$$\xi(t; x_0, 0) \notin \texttt{Unsafe}, \tag{15}$$

$$(\xi(t; x_i, 0), \xi(t; x_0, 0)) \in \mathcal{D}, \tag{16}$$

for all $t \in [0, T]$.

The results above establish a way to perform a local testing-based safety verification using a local bisimulation function/ Lyapunov function type argument, which is similar to [17]. Namely, we can guarantee the safety of all trajectories starting from a neighborhood $L^{x_i}_{\phi,\beta}$ of the nominal initial state x_i. The new contribution in this paper lies in the fact that the domain of validity of the function can be local. The locality of this analysis can be extended by linking multiple local analysis to cover a test trajectory. This idea is elucidated in the following theorem, and illustrated in Figure 4.

Theorem 1. *Consider a test trajectory $\xi(t; x_0, 0)$, $t \in [0, T]$. Suppose that for $i = 1, \ldots, N$, there exists a family of sets $\mathcal{D}_i \subset \mathcal{X} \times \mathcal{X}$, functions $\phi_i : \mathcal{X} \times \mathcal{X} \to \mathbb{R}_+$, positive constants α_i and β_i, and time intervals $0 = t_0 < t_1 < \cdots < t_N = T$ such that*
(i) $(\xi(t; x_0, 0), \xi(t; x_0, 0)) \in \mathcal{D}_i$ for all $t \in [t_{i-1}, t_i]$,
(ii) for all $(x, y) \in \mathcal{D}_i$, there exists a $k_i \in \mathbb{R}$ such that

$$\nabla_x \phi_i(x, y) f(x) + \nabla_y \phi_i(x, y) f(y) \leq k_i, \tag{17}$$

(iii) there exists a $k_i' \geq k_i$ *such that*

$$\beta_i + k_i' t \leq d_i(t), \forall t \in [0, t_i - t_{i-1}],$$
$$\beta_i + k_i' (t_i - t_{i-1}) \leq \alpha_i,$$

where

$$d_i(t) := \inf_{y \in \texttt{Avoid}_i(t)} \phi_i(\xi(t; x_{i-1}, 0), y), \forall t \in [0, t_i - t_{i-1}],$$
$$\texttt{Avoid}_i(t) := \{y \mid y \in \texttt{Unsafe}, (\xi(t; x_{i-1}, 0), y) \in \mathcal{D}_i\} \cup \{y \mid (\xi(t; x_{i-1}, 0), y) \notin \mathcal{D}_i\},$$
$$x_{i-1} := x(t_{i-1}),$$

(iv) for $i = 1, \ldots, N-1$,

$$\alpha_i \leq \sup \left\{ \alpha \mid L^{x_i}_{\phi_i, \alpha} \subset L^{x_i}_{\phi_{i+1}, \beta_{i+1}} \right\}.$$

For any initial condition $\tilde{x}_0 \in L^{x_0}_{\phi_1, \beta_1}$, *we have that*

$$\xi(t; \tilde{x}_0, 0) \notin \texttt{Unsafe}, \tag{18}$$
$$(\xi(t; x_0, 0), \xi(t; \tilde{x}_0, 0)) \in \cup_{i=1}^N \mathcal{D}_i, \tag{19}$$

for all $t \in [0, T]$.

Proof. Consider the last interval of the trajectory, that is $t \in [t_{N-1}, T]$. By Proposition 3, we have that for any $\tilde{x}_{N-1} \in L^{x_{N-1}}_{\phi_N, \beta_N}$,

$$\xi(t; \tilde{x}_{N-1}, t_{N-1}) \notin \texttt{Unsafe}, \tag{20}$$
$$(\xi(t; x_{N-1}, 0), \xi(t; \tilde{x}_{N-1}, 0)) \in \cup_{i=1}^N \mathcal{D}_i, \tag{21}$$

for all $t \in [t_{N-1}, T]$. Also, for any $i = 1, \ldots, N-1$, using the same proposition, we can conclude that for any $\tilde{x}_{i-1} \in L^{x_{i-1}}_{\phi_i, \beta_i}$,

$$\xi(t; \tilde{x}_{i-1}, t_{i-1}) \notin \texttt{Unsafe}, \tag{22}$$
$$(\xi(t; x_{i-1}, t_{i-1}), \xi(t; \tilde{x}_{i-1}, t_{i-1})) \in \cup_{i=1}^N \mathcal{D}_i, \tag{23}$$
$$\xi(t_i; \tilde{x}_{i-1}, t_{i-1}) \in L^{x_i}_{\phi_i, \alpha_i}. \tag{24}$$

By construction, $L^{x_i}_{\phi_i, \alpha_i} \subset L^{x_i}_{\phi_{i+1}, \beta_{i+1}}$. Hence, from (24) we can obtain

$$\xi(t_i; \tilde{x}_{i-1}, t_{i-1}) \in L^{x_i}_{\phi_{i+1}, \beta_{i+1}}.$$

Therefore, by repeated application of Proposition 3, we can prove that this theorem holds.

The result given in Theorem 1 can be easily extended by replacing the barrier functions with constant growth bounds with those with linear growth bounds. In this case, the proof will follow Proposition 4.

4 Computation of Barrier Functions and the Domains of Validity

4.1 General Scheme

In the previous sections we have established some results that describe how to construct a finite-time safety/ reachability type guarantee based on the barrier function ϕ and its domain of validity $\mathcal{D}$. In this section, we propose a computational scheme to construct such barrier function and domain of validity.

Consider the dynamical system in (1).

Proposition 5. *Suppose that the functions $\phi(x)$ and $\gamma(x)$ satisfy*

$$\nabla_x \phi(x) f(x) - k \leq \varepsilon(x)\gamma(x), \tag{25}$$

for some strictly positive function $\varepsilon(x)$, and $k \in \mathbb{R}$. Then $\phi(x)$ is a barrier function with k as its constant growth bound and $\mathcal{D} := \{x \mid \gamma(x) \leq 0\}$ is its domain of validity,

Proof. This construction is based on the S-procedure. From (25), it follows that $\gamma(x) \leq 0$ implies

$$\nabla_x \phi(x) f(x) \leq k.$$

The linear growth bound version of this proposition can be found by replacing k in (25) with $k\phi(x)$. We can use this proposition to generate a barrier function ϕ for a given domain of validity $\mathcal{D}$.

$$\begin{aligned} &\text{Given } \gamma(x), \text{ find } \phi(x) \text{ and } \varepsilon(x) \text{ satisfying} \\ &\nabla_x \phi(x) f(x) - \varepsilon(x)\gamma(x) - k \leq 0,\ \varepsilon(x) \geq 0. \end{aligned} \tag{26}$$

Extending this scheme for safety verification amounts to finding a barrier function $\phi : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ that is valid in a domain given by $\gamma(x, y) \leq 0$. This can be done by solving the following problem.

$$\begin{aligned} &\text{Given } \gamma(x,y), \text{ find } \phi(x,y) \text{ and } \varepsilon(x,y) \text{ satisfying} \\ &\nabla_x \phi(x,y) f(x) + \nabla_y \phi(x,y) f(y) - \varepsilon(x,y)\gamma(x,y) - k \leq 0,\ \varepsilon(x,y) \geq 0. \end{aligned} \tag{27}$$

For a special class of systems, we can explicitly outline a computational technique that implements this general scheme, as described in the next subsection.

4.2 Affine Systems

If $f(x)$ in (1) is a linear function,

$$f(x) = Ax + b,\ x \in \mathbb{R}^n,\ A \in \mathbb{R}^{n \times n},\ b \in \mathbb{R}^{n \times 1}$$

we can constrain a barrier function to be a quadratic function

$$\phi(x, y) = (x - y)^T M (x - y),$$

for some $M > 0$. If the matrix A is Hurwitz, for barrier function with linear growth bound the domain of validity of the barrier function can be extended globally, by choosing $\gamma(x, y) = 0$. In this case, (27) becomes

$$\nabla_x \phi(x,y) f(x) + \nabla_y \phi(x,y) f(y) - k\phi(x,y) = (x-y)^T (MA + A^T M - kM)(x-y) \leq 0 \quad (28)$$

which is a Lyapunov equation that can be solved for $k \geq 2\lambda(A)$, where $\lambda(A)$ is the largest eigenvalue of A. Obviously, a similar approach also works for nonpositive constant growth bound.

If the matrix A is not Hurwitz, then for barrier function with linear growth bound (28) can still be solved if $k \geq 2\lambda(A)$. For barrier functions with positive constant growth bound, the domain of validity must be bounded. If we choose, for the domain of validity, an ellipsoidal set given by $\gamma(x, y) \leq 0$, where $\gamma(x, y) = (x-y)^T Q (x-y) - 1$, for some $Q > 0$, then (27) becomes finding M and $\varepsilon(x, y)$ satisfying

$$(x-y)^T \left(MA + A^T M - \varepsilon(x,y)Q\right)(x-y) + \varepsilon(x,y) - k \leq 0,\ \varepsilon(x,y) \geq 0, \quad (29)$$

which can be solved by taking $\varepsilon(x, y) = 1$ and M small enough such that $MA + A^T M \leq Q$. Once M is determined, we can find the tightest constant growth bound by solving the following optimization problem

$$\text{minimize } k \text{ subject to (29)},$$

with k and $\varepsilon(x, y)$ as the optimization variables. In this case, we can bound k as

$$k \leq \inf_{\varepsilon \in \mathbb{R}} \{\varepsilon \mid MA + A^T M \leq \varepsilon Q\}. \quad (30)$$

4.3 Locally Linearized Systems

For a locally linearized system $f(x)$ in (1) can be written as,

$$f(x) = Ax + b + \omega(x),\ x \in \mathcal{D} \subset \mathbb{R}^n.$$

Here $Ax + b$ is the linearized model and $\omega(x)$ is the residual term. Suppose that $\mathcal{D}$ is bounded and its diameter is given by

$$\rho(D) := \sup_{x,y \in \mathcal{D}} \|x - y\|,$$

and there exists a $\delta > 0$ such that $\|\omega(x)\| \leq \delta$, for all $x \in \mathcal{D}$. That is, we assume that we can bound the magnitude of the linearization residue in $\mathcal{D}$.

We propose to construct a quadratic barrier function in the form of $\phi(x, y) = (x-y)^T M (x-y)$, $M > 0$. In this case, we obtain

$$\begin{aligned}\nabla_x \phi(x,y) f(x) + \nabla_y \phi(x,y) f(y) &= (x-y)^T (MA + A^T M)(x-y) \\ &\quad + 2(x-y)^T M (\rho(x) - \rho(y)), \\ &\leq (x-y)^T (MA + A^T M)(x-y) + 4\|M\| \delta \rho(D),\end{aligned}$$

where $\|M\|$ is the largest singular value of M.

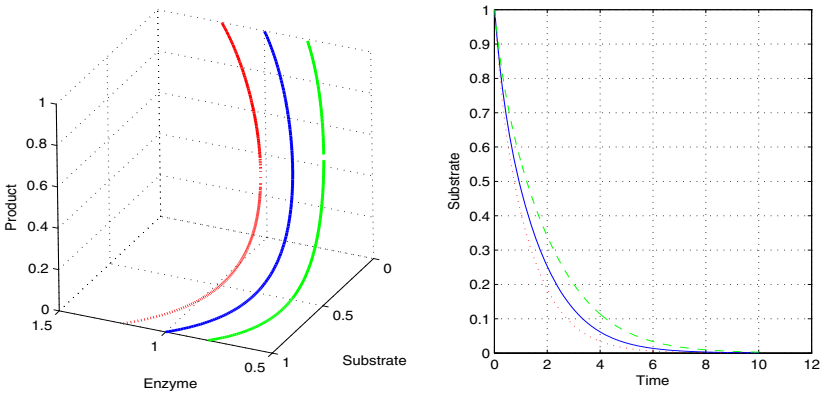

Fig. 5. Three trajectories of the system in Example 1 with varying enzyme availability. In the right panel we can see that smaller enzyme concentration implies slower consumption of the substrate.

If A is Hurwitz, then by following the same computation as in the previous subsection, we can construct a barrier function with constant growth bound by solving the Lyapunov equation $(MA + A^T M) \leq 0$ and the growth bound is $4 \|M\| \delta\rho(D)$. If A is not Hurwitz, for any choice of M we can construct a positive constant growth bound for the barrier function by adding $4 \|M\| \delta\rho(D)$ to an upper bound of $(x-y)^T (MA + A^T M)(x-y)$ for $x, y \in \mathcal{D}$. This can be done by using the technique described in the previous subsection, or by using the following (possibly conservative) bound

$$(x-y)^T (MA + A^T M)(x-y) \leq \rho(D)^2 \left\| MA + A^T M \right\|. \tag{31}$$

4.4 Polynomial Systems

If $f(x)$ in (1) is a polynomial, and if we assume that $\phi(x)$, $\varepsilon(x)$, and $\gamma(x)$ are polynomials, the semidefinite constraints in (26) can be recast as sum-of-squares constraints. Similar situation applies to (27) for safety verification. In this case, the computation can be implemented by using computational tools for sum-of-squares programming, such as SOSTOOLS [31].

Example 1. A standard model of the dynamics of an enzymatic reaction

$$\text{Enzyme} + \text{Substrate} \rightleftarrows \text{Enz.Sub} \rightarrow \text{Enzyme} + \text{Product}$$

is given by

$$\frac{d}{dt}\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} -k_f x_1 x_2 + (k_b + k_m) x_3 \\ -k_f x_1 x_2 + k_b x_3 \\ k_f x_1 x_2 - (k_b + k_m) x_3 \\ k_m x_3 \end{bmatrix},$$

where the state variables are the concentrations of the enzyme, substrate, enzyme-substrate complex, and product, respectively. The constants k_f, k_b, and k_m are

reaction constants that determines the speed of the reactions. Several trajectories of this system are shown in Figure 5. In this simulation, we take $k_b = 0.1$ and $k_f = k_m = 1$. Consider the middle trajectory in Figure 5, which starts at the initial condition $(1, 1, 0, 0)$. Suppose that we take this trajectory as our test trajectory and we want to construct a local barrier function for this system for a given domain of validity. The circular domain of validity is expressed as

$$\gamma(x, y) := (x - c)^T(x - c) + (x - y)^T(x - y) - r^2 \leq 0,$$

where the vector $c = (0.70, 0.51, 0.30.0.19)^T$ defines the center of the circle in the state space and $r = 0.2$ is its radius. We assume that the barrier function can be written as

$$\phi(x, y) := \frac{1}{2}(x - y)^T M(x - y),$$

with M a 4×4 symmetric positive semidefinite matrix. Finding a suitable barrier function by using sum-of-squares programming can be cast as

$$\begin{gathered} \text{minimize } 0 \text{ subject to} \\ -\nabla_x \phi(x, y) f(x) - \nabla_y \phi(x, y) f(x) + \varepsilon(x, y)\gamma(x, y) + k = \text{sos}, \\ \phi(x, y) = \text{sos}, \ \varepsilon(x, y) = \text{sos}. \end{gathered}$$

Solving this problem with SOSTOOLS, we get

$$M = \begin{bmatrix} 0.28 & -0.07 & 0.21 & -0.07 \\ * & 0.19 & 0.11 & 0.19 \\ * & * & 0.16 & 0.11 \\ * & * & * & 0.19 \end{bmatrix}, \ k = 0.02.$$

Notice that we replace nonnegativity of the polynomials with sum-of-squares property, which is more restrictive and can lead to some conservativeness. However, through this step, the program can then be solved using available SOS computational tools.

5 Discussion

In this paper we propose a trajectory based reachability analysis using local finite-time invariance property. This method is a generalization of our previous results [17,18], where a global bisimulation is required for each mode of dynamics. We demonstrate that our method captures some other existing methods as special cases, and that for polynomial systems the computation can be implemented using sum-of-squares.

The extension of the method proposed in this paper to analysis of hybrid systems is relatively straightforward. The method proposed in [17] for hybrid systems performs the analysis on a hybrid test trajectory by piecing together trajectory segments between mode transitions in a way analogous to Theorem 1. We can therefore apply the local analysis based method to hybrid systems by extending Theorem 1 to handle transition guards in a way similar to Proposition 2 in [17].

In order to develop an effective implementation of the result posed in this paper, we still need to design a comprehensive test algorithm. There are a number of issues that need to be addressed along this direction. For example, the notion of test coverage and automatic test generation based on the coverage need to be developed to get an efficient testing procedure that can quickly cover the set of initial states. We also need to address the issue of optimal placement of the local domains of validity of the barrier functions. The goal is to design the segmentation of trajectories in a way that requires as few segments as possible. Another issue that we have not investigated is the use of constant and linear growth bounds. In the case where both bounds are available, we need to design an algorithm that can optimally choose which bound to use, in order to minimize the conservativeness of the bound.

References

1. Balluchi, A., Di Natale, F., Sangiovanni-Vincentelli, A., van Schuppen, J.H.: Synthesis for idle speed control of an automotive engine. In: Alur, R., Pappas, G.J. (eds.) HSCC 2004. LNCS, vol. 2993, pp. 80–94. Springer, Heidelberg (2004)
2. Platzer, A., Quesel, J.-D.: Logical verification and systematic parametric analysis in train control. In: Egerstedt, M., Mishra, B. (eds.) HSCC 2008. LNCS, vol. 4981, pp. 646–649. Springer, Heidelberg (2008)
3. Tomlin, C., Pappas, G.J., Sastry, S.: Conflict resolution for air traffic management: a study in multi-agent hybrid systems. IEEE Trans. Automatic Control 43, 509–521 (1998)
4. Hu, J., Prandini, M., Sastry, S.: Probabilistic safety analysis in three dimensional aircraft flight. In: Proc. 42nd IEEE Conf. Decision and Control, Maui, USA, pp. 5335–5340 (2003)
5. Belta, C., Schug, J., Dang, T., Kumar, V., Pappas, G.J., Rubin, H., Dunlap, P.: Stability and reachability analysis of a hybrid model of luminescence in the marine bacterium *vibrio fischeri*. In: Proc. IEEE Conf. Decision and Control, Orlando, Florida, pp. 869–874 (2001)
6. Ghosh, R., Amondlirdviman, K., Tomlin, C.: A hybrid systems model of planar cell polarity signaling in drosophila melanogaster wing epithelium. In: Proc. IEEE Conf. Decision and Control, Las Vegas (2002)
7. Kurzhanski, A.B., Varaiya, P.: Ellipsoidal technique for reachability analysis. In: Lynch, N.A., Krogh, B.H. (eds.) HSCC 2000. LNCS, vol. 1790, pp. 202–214. Springer, Heidelberg (2000)
8. Mitchell, I., Tomlin, C.J.: Level set methods in for computation in hybrid systems. In: Lynch, N.A., Krogh, B.H. (eds.) HSCC 2000. LNCS, vol. 1790, pp. 310–323. Springer, Heidelberg (2000)
9. Asarin, E., Bournez, O., Dang, T., Maler, O.: Approximate reachability analysis of piecewise-linear dynamical systems. In: Lynch, N.A., Krogh, B.H. (eds.) HSCC 2000. LNCS, vol. 1790, pp. 21–31. Springer, Heidelberg (2000)
10. Kapinski, J., Krogh, B.H.: A new tool for verifying computer controlled systems. In: Proc. IEEE Conf. Computer-Aided Control System Design, Glasgow, pp. 98–103 (2002)
11. Alur, R., Dang, T., Ivancic, F.: Reachability analysis of hybrid systems via predicate abstraction. In: Tomlin, C.J., Greenstreet, M.R. (eds.) HSCC 2002. LNCS, vol. 2289, pp. 35–48. Springer, Heidelberg (2002)

12. Stursberg, O., Krogh, B.H.: Efficient representation and computation of reachable sets for hybrid systems. In: Maler, O., Pnueli, A. (eds.) HSCC 2003. LNCS, vol. 2623, pp. 482–497. Springer, Heidelberg (2003)
13. Han, Z., Krogh, B.H.: Reachability analysis of hybrid control systems using reduced-order models. In: Proc. American Control Conference, pp. 1183–1189 (2004)
14. Prajna, S., Jadbabaie, A.: Safety verification of hybrid systems using barrier certificates. In: Alur, R., Pappas, G.J. (eds.) HSCC 2004. LNCS, vol. 2993, pp. 477–492. Springer, Heidelberg (2004)
15. Frehse, G.: PHAVer: Algorithmic verification of hybrid systems past HyTech. In: Morari, M., Thiele, L. (eds.) HSCC 2005. LNCS, vol. 3414, pp. 258–273. Springer, Heidelberg (2005)
16. Girard, A.: Reachability of uncertain linear systems using zonotopes. In: Morari, M., Thiele, L. (eds.) HSCC 2005. LNCS, vol. 3414, pp. 291–305. Springer, Heidelberg (2005)
17. Julius, A.A., Fainekos, G., Anand, M., Lee, I., Pappas, G.J.: Robust test generation and coverage for hybrid systems. In: Bemporad, A., Bicchi, A., Buttazzo, G. (eds.) HSCC 2007. LNCS, vol. 4416, pp. 329–342. Springer, Heidelberg (2007)
18. Julius, A.A., Pappas, G.J.: Probabilistic testing for stochastic hybrid systems. In: Proc. IEEE Conf. Decision and Control, Cancun, Mexico (2008)
19. Esposito, J.M.: Randomized test case generation for hybrid systems verification. In: Proc. 36th Southeastern Symposium of Systems Theory (2004)
20. Branicky, M.S., Curtiss, M.M., Levine, J., Morgan, S.: RRTs for nonlinear, discrete, and hybrid planning and control. In: Proc. IEEE Conf. Decision and Control, Hawaii, USA (2003)
21. Bhatia, A., Frazzoli, E.: Incremental search methods for reachability analysis of continuous and hybrid systems. In: Alur, R., Pappas, G.J. (eds.) HSCC 2004. LNCS, vol. 2993, pp. 142–156. Springer, Heidelberg (2004)
22. Asarin, A., Dang, T., Girard, A.: Reachability analysis of nonlinear systems using conservative approximation. In: Maler, O., Pnueli, A. (eds.) HSCC 2003. LNCS, vol. 2623, pp. 20–35. Springer, Heidelberg (2003)
23. Han, Z., Krogh, B.H.: Reachability analysis of nonlinear systems using trajectory piecewise linearized models. In: Proc. American Control Conference, Minneapolis (2006)
24. Donzé, A., Maler, O.: Systematic simulation using sensitivity analysis. In: Bemporad, A., Bicchi, A., Buttazzo, G. (eds.) HSCC 2007. LNCS, vol. 4416, pp. 174–189. Springer, Heidelberg (2007)
25. Lohmiller, W., Slotine, J.J.E.: On contraction analysis for nonlinear systems. Automatica 34, 683–696 (1998)
26. Tan, W., Packard, A., Wheeler, T.: Local gain analysis on nonlinear systems. In: Proc. American Control Conference, Minneapolis (2006)
27. Girard, A., Pappas, G.J.: Verification using simulation. In: Hespanha, J.P., Tiwari, A. (eds.) HSCC 2006. LNCS, vol. 3927, pp. 272–286. Springer, Heidelberg (2006)
28. Lerda, F., Kapinski, J., Clarke, E.M., Krogh, B.H.: Verification of supervisory control software using state proximity and merging. In: Egerstedt, M., Mishra, B. (eds.) HSCC 2008. LNCS, vol. 4981, pp. 344–357. Springer, Heidelberg (2008)
29. Boyd, S., El Ghaoui, L., Feron, E., Balakrishnan, V.: Linear Matrix Inequalities in Systems and Control Theory. SIAM, Philadelphia (1994)
30. Khalil, H.K.: Nonlinear Systems, 3rd edn. Prentice-Hall, Englewood Cliffs (2002)
31. Prajna, S., Papachristodoulou, A., Seiler, P., Parillo, P.A.: SOSTOOLS and its control application. In: Positive polynomials in control. Springer, Heidelberg (2005)