Proceedings of the
44th IEEE Conference on Decision and Control, and
the European Control Conference 2005
Seville, Spain, December 12-15, 2005

Methods for Safety Verification of Time-Delay Systems

Stephen Prajna and Ali Jadbabaie

Abstract— **This paper addresses the safety verification of systems with time-delay. It extends the barrier certificate methodology previously proposed for safety verification of systems described by ordinary differential equations to the functional differential equations setting. For verifying the safety of a time-delay system, a functional of states is used as a barrier certificate. The forms of the functionals resemble the Lyapunov-Razumikhin functions or the Lyapunov-Krasovskii functionals used in stability analysis of time-delay systems. When the description of the system is given in terms of polynomials, such a barrier certificate can be searched using sum of squares programming.**

I. Introduction

Safety verification addresses the question whether an "unsafe" or "bad" region in the state space is reachable by some system trajectories starting from a given set of possible initial states. The need for safety verification arises as the complexity of the system increases, and is also underscored by the safety critical nature of the system. For discrete state systems, such as finite automata, this problem has been studied extensively in the computer science literature (see, e.g., [4]) and has applications in, for example, the verification of correctness of computer protocols, algorithms, and software.

In the recent years, there has been a great interest in safety verification of systems with continuous or hybrid (i.e., mixed discrete-continuous) states [1]–[3], [8], [20], [21]. This is motivated by the fact that many safety critical applications such as air traffic control [21] or life support systems [5] involve continuous or even hybrid states. Various methods have been proposed for safety verification of continuous or hybrid systems, many of which require computing the propagation of initial states (see e.g. [1], [3], [21]). Unfortunately, although these methods allow us to compute an exact or near exact approximation of reachable sets, it is difficult to perform such a computation due to the uncountability of the state space. The computation is harder when the system is nonlinear and uncertain, and clearly becomes even more intractable if the state space is infinite dimensional.

Infinite dimensional state space is encountered, for example, when there are time-delay elements in the system. Time-delay systems appear in various application areas such as communications [19], process control [18], and biology [10]. Many systems in these areas are safety critical, and we expect that many more safety critical systems involving time-delay will be introduced in the future when control is performed over communication channels. While the field of time-delay systems is a mature area (see, e.g., [6], [7], [11]), most of the available analysis results are focused on stability, robustness, or input-output properties — and not on safety or reachability. This is what motivates us to develop a methodology for safety verification of time-delay systems in this paper.

In previous work [13], [14], we proposed a framework based on functions of states termed barrier certificates combined with deductive inference to prove safety. A barrier certificate is a function of state satisfying some inequalities on both the function itself and its time derivative along the flow of the system. The idea here is to prove that the system is safe by finding a proper barrier certificate, without the need to compute the flow of the system or to propagate sets of states. Computation of barrier certificates can be performed using sum of squares programming [15] when the system is described in terms of polynomials. This method can be extended for handling time-delay systems by using functionals of states as barrier certificates, which we will present in this paper.

The outline of the paper is as follows. In Section II, we will give a brief overview of the previous results on safety verification using barrier certificates. The methodology will be extended to the time-delay setting in Section III. An example will be studied in Section IV, and finally the paper will be ended by some conclusions in Section V.

A. Notations

We denote the spaces of m-times continuously differentiable functions mapping $\mathcal{X} \subseteq \mathbb{R}^n$ to $\mathbb{R}^\ell$ by $C^m(\mathcal{X}, \mathbb{R}^\ell)$, and $\mathcal{X}$ to $\mathbb{R}$ by $C^m(\mathcal{X})$. The corresponding spaces of continuous functions are denoted by $C(\mathcal{X}, \mathbb{R}^\ell)$ and $C(\mathcal{X})$. For a set $\mathcal{X} \subseteq \mathbb{R}^n$, $\partial\mathcal{X}$ denotes the boundary of $\mathcal{X}$.

II. Verification Using Barrier Certificates

In this section, we will provide a review of previous results on safety verification using barrier certificates. Consider a system described by ordinary differential equations

$$\dot{x}(t) = f(x(t), d(t)), \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state of the system, $d(t) \in \mathcal{D} \subseteq \mathbb{R}^m$ is a collection of uncertain disturbance inputs, and $f \in C(\mathbb{R}^{n+m}, \mathbb{R}^n)$. We will be mostly dealing with a bounded disturbance set $\mathcal{D}$. In the safety verification problem, we will be interested only in segments of system trajectories that are contained in a given set $\mathcal{X} \subseteq \mathbb{R}^n$. Now suppose also that

S. Prajna is with the Control and Dynamical Systems option, California Institute of Technology, Pasadena, CA 91125, USA. E-mail: prajna@cds.caltech.edu

A. Jadbabaie is with the Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia, PA 19104, USA. E-mail: jadbabai@seas.upenn.edu

0-7803-9568-9/05/$20.00 ©2005 IEEE

a set of possible initial states $\mathcal{X}_0 \subseteq \mathcal{X}$ and a set of unsafe states $\mathcal{X}_u \subseteq \mathcal{X}$ are given. Our objective is to prove that the system is safe in the following sense.

Definition 1 (Safety): Given a system (1) and the sets $\mathcal{X}$, $\mathcal{D}$, $\mathcal{X}_0$ and $\mathcal{X}_u$, we say that the system safety property holds if there do not exist a time instant $T \geq 0$, a bounded and piecewise continuous disturbance input $d : [0, T] \to \mathcal{D}$, and a corresponding trajectory $x : [0, T] \to \mathbb{R}^n$ such that $x(0) \in \mathcal{X}_0$, $x(T) \in \mathcal{X}_u$, and $x(t) \in \mathcal{X}\ \forall t \in [0, T]$.

The safety of the system (1) can be shown by the existence of a barrier certificate [13]. A barrier certificate is a function of state satisfying some Lyapunov-like conditions on both the function itself and its time derivative along the flow of the system, stated in Proposition 2 below. The main idea is to ask that the value of the function at the initial set $\mathcal{X}_0$ to be non-positive, the time derivative of the function to be non-positive on $\mathcal{X}$, and the value of the function at the unsafe set $\mathcal{X}_u$ to be strictly positive. If a function satisfying such a property can found, then we can conclude that no trajectory of the system starting from $\mathcal{X}_0$ can reach $\mathcal{X}_u$.

Proposition 2 ([13]): Let the system (1) and the sets $\mathcal{X} \subseteq \mathbb{R}^n$, $\mathcal{D} \subseteq \mathbb{R}^m$, $\mathcal{X}_0 \subseteq \mathcal{X}$ and $\mathcal{X}_u \subseteq \mathcal{X}$ be given, with $f \in C(\mathbb{R}^{n+m}, \mathbb{R}^n)$. Suppose there exists a function $B \in C^1(\mathbb{R}^n)$ that satisfies the following conditions:

$$B(x) \leq 0 \quad \forall x \in \mathcal{X}_0, \tag{2}$$

$$B(x) > 0 \quad \forall x \in \mathcal{X}_u, \tag{3}$$

$$\frac{\partial B}{\partial x}(x) f(x, d) \leq 0 \quad \forall (x, d) \in \mathcal{X} \times \mathcal{D}, \tag{4}$$

then the safety of the system (1) in the sense of Definition 1 is guaranteed.

The above method is analogous to the Lyapunov method for stability analysis. Contrary to stability analysis, however, no notion of equilibrium, stability, or convergence is required in safety verification. For example, the system does not even need to have an equilibrium.

The conditions in Proposition 2 define a convex set of barrier certificates $\{B(x)\}$. This is a very beneficial property, as a barrier certificate inside this set can be searched using convex optimization. For example, when the vector field $f(x, d)$ is polynomial and the sets $\mathcal{X}$, $\mathcal{D}$, $\mathcal{X}_0$, $\mathcal{X}_u$ are semialgebraic, i.e., defined by polynomial inequalities and equalities, a computational framework called *sum of squares optimization* [15] that is based on semidefinite programming can be utilized to search for a polynomial barrier certificate. In particular, the software SOSTOOLS [15] is available for this computation.

We would like to mention that the method can also be extended to handle safety verification of hybrid systems [13], stochastic continuous and hybrid systems [14], and even to verification of other temporal properties such as reachability, eventuality, and their combinations [17]. An application case study can be found in [5]. Finally, a converse statement of Proposition 2 for systems without disturbance input has also been obtained recently [16], stating that under some reasonable technical conditions, the existence of a function $B(x)$ satisfying the conditions of the theorem is also necessary for safety.

III. Conditions for Verification of Time-Delay Systems

We will now extend the method described in the previous section to time-delay systems. In this context, the system is a set of retarded functional differential equations

$$\dot{x}(t) = f(x_t, d(t)) \tag{5}$$

where the disturbance input $d(t)$ still takes its value in the finite dimensional space $\mathcal{D} \subseteq \mathbb{R}^n$, whereas the state of the system is now in an infinite dimensional space, $x_t \in C([-r, 0], \mathbb{R}^n)$, with $r \geq 0$. Here we use the following notation:

$$x_t(\theta) = x(t + \theta),$$

where $\theta \in [-r, 0]$. The right hand side of (5) is a functional $f : C([-r, 0], \mathbb{R}^n) \times \mathcal{D} \to \mathbb{R}^n$, and the dot on the left hand side of the equation denotes the right hand Dini derivative. In most cases of interest, the right hand side of (5) will be of the form

$$f(x_t, d(t)) = \hat{f}(x(t), x(t - r_1), \ldots, x(t - r_\ell), d(t))$$

for $\hat{f} \in C(\mathbb{R}^{(\ell+1)n+m}, \mathbb{R}^n)$ and some $r_1, \ldots, r_\ell \in [0, r]$. We will consider this form, i.e., systems

$$\dot{x}(t) = \hat{f}(x(t), x(t - r_1), \ldots, x(t - r_\ell), d(t)) \tag{6}$$

throughout the rest of the paper. It is also assumed that the delays are time-invariant, and therefore without loss of generality an ordering

$$0 \leq r_1 \leq \cdots \leq r_\ell = r$$

can be imposed.

In addition to the above, three sets are also given: a set $\mathcal{X} \subseteq \mathbb{R}^n$, an initial set $\mathcal{X}_0 \subseteq \mathcal{X}$ and an unsafe set $\mathcal{X}_u \subseteq \mathcal{X}$, with $\mathcal{X}_0 \cap \mathcal{X}_u = \emptyset$. For the safety verification problem, we are again interested only in segments of trajectories that are contained in $\mathcal{X}$. With all these, we can define the notion of unsafe trajectory and the safety property for the time-delay system (5) as follows.

Definition 3 (Unsafe trajectory): A trajectory segment $x : [-r, T] \to \mathbb{R}^n$ of the system (6) is an unsafe trajectory, if $x(\theta) \in \mathcal{X}_0\ \forall \theta \in [-r, 0]$, $x(T) \in \mathcal{X}_u$, and $x(t) \in \mathcal{X}\ \forall t \in [-r, T]$.

Definition 4 (Safety — Systems with Time Delay): Given a system (5) and the sets $\mathcal{X}$, $\mathcal{D}$, $\mathcal{X}_0$ and $\mathcal{X}_u$, we say that the safety property holds if there exist no time instant $T > 0$, and bounded, piecewise continuous disturbance input $d : [0, T] \to \mathcal{D}$ which gives rise to an unsafe trajectory $x : [-r, T] \to \mathbb{R}^n$ as per Definition 3.

Within this setting, it is crucial to note that the initial and unsafe regions $\mathcal{X}_0$ and $\mathcal{X}_u$ are given as sets in a finite dimensional space $\mathbb{R}^n$, where $x(t)$ takes its value, but on the other hand, the state of the system is an element of the infinite dimensional space $C([-r, 0], \mathbb{R}^n)$. With Definition 4

in mind, it is straightforward to define the set of initial states of interest as

$$X_0 = \{x_0 \in C([-r,0],\mathbb{R}^n) : x_0(\theta) \in \mathcal{X}_0 \ \forall \theta \in [-r,0]\}. \tag{7}$$

Defining the set of unsafe states requires more thought: using $\{x_u \in C([-r,0],\mathbb{R}^n) : x_u(\theta) \in \mathcal{X}_u \ \forall \theta \in [-r,0]\}$ as the set of unsafe states is not enough, since it is possible for the system to violate the safety property in Definition 4 without its state ever been in this set. The correct set of unsafe states is in fact

$$X_u = \{x_u \in C([-r,0],\mathbb{R}^n) : x_u(0) \in \partial\mathcal{X}_u, \\ x_u(\theta) \in \mathcal{X} \setminus \mathcal{X}_u \ \forall \theta \in [-r,0)\}. \tag{8}$$

Using X_u as the set of unsafe states, the following lemma holds.

Lemma 5: Under the assumption that $\mathcal{X}_0 \cap \mathcal{X}_u = \emptyset$, the safety property in Definition 4 is violated by an unsafe trajectory $x : [-r,T] \to \mathcal{X}$ if and only if $x_t \in X_u$ for some $t \in [0,T]$.

Proof: Straightforward, since we assume that $\mathcal{X}_0$ and $\mathcal{X}_u$ are disjoint and we consider a trajectory that starts with $x_0 \in X_0$. ∎

The safety verification method presented in the previous section can be extended to handle time-delay systems. For this purpose, we use a *functional* of system states as a barrier certificate. The idea is similar to what used in Section II. We ask that the value of functional for any trajectory of the system starting with $x_0 \in X_0$ be (i) non-positive initially; (ii) non-increasing along time; and (iii) positive at some time instant, if the unsafe region is reached. Using a contradiction, we can then conclude that the system is safe if such a barrier certificate can be found.

In the rest of this section, we will consider several classes of functionals with increasingly complex structures, to be used as barrier certificates.

A. Functional Structure 1

The first functional structure that we will consider depends only on the "head" of the state x_t, and is of the following form:

$$B(x_t) = B_0(x(t)),$$

where $B_0 \in C^1(\mathbb{R}^n)$. It is the kind of functions used in the Lyapunov-Razumikhin theorem for proving delay-independent stability of time-delay systems [9]. Using these functionals, it is possible to obtain conditions guaranteeing delay-independent safety, stated in the following proposition.

Proposition 6: Let the system (6) and the sets $\mathcal{X} \subseteq \mathbb{R}^n$, $\mathcal{D} \subseteq \mathbb{R}^m$, $\mathcal{X}_0 \subseteq \mathcal{X}$ and $\mathcal{X}_u \subseteq \mathcal{X}$ be given, with $\hat{f} \in C(\mathbb{R}^{(\ell+1)n+m},\mathbb{R}^n)$ and $\mathcal{X}_0 \cap \mathcal{X}_u = \emptyset$. Suppose there exists a function $B_0 \in C^1(\mathbb{R}^n)$ that satisfies the following conditions:

$$B_0(x) \le 0 \quad \forall x \in \mathcal{X}_0, \tag{9}$$

$$B_0(x) > 0 \quad \forall x \in \mathcal{X}_u, \tag{10}$$

$$\frac{\partial B_0}{\partial x}(x)\hat{f}(x,\hat{x}_1,\ldots,\hat{x}_\ell,d) \le 0 \\ \forall (x,\hat{x}_1,\ldots,\hat{x}_\ell,d) \in \mathcal{X}^{(\ell+1)} \times \mathcal{D}, \tag{11}$$

then the safety of the system (6) in the sense of Definition 4 is guaranteed.

Proof: Suppose that a function $B_0(x)$ satisfying the conditions in the proposition can be found, but there exist $T > 0$, a piecewise continuous and bounded disturbance input $d : [0,T] \to \mathcal{D}$, and a corresponding unsafe trajectory $x : [-r,T] \to \mathcal{X}$. Consider the evolution $B_0(x(t))$ along time for this trajectory. Conditions (9) and (11) assert respectively that $B_0(x(0))$ is non-positive and that the time derivative of $B_0(x(t))$ is non-positive on the time interval $[0,T]$. On the other hand, condition (11) implies that $B_0(x(T))$ is strictly positive. We obtain a contradiction, and therefore we conclude that such an unsafe trajectory cannot exist — the system is safe. ∎

Remark 7: Notice that no information about the delays is used in Proposition 6. In fact, the safety of the system as guaranteed by the proposition is *delay independent*: the system is safe for arbitrary (but finite) time delays $r_1, r_2, \ldots, r_\ell$.

For many systems, the safety property is dependent on the size of the time delay. For example, the system could be safe when the delay is small, but unsafe for large delay. If we are interested only in small delay, then the conditions given in Proposition 6 is too conservative. To relax this conservatism we will consider another class of functionals in the next subsections.

Remark 8: If the vector field $\hat{f}(\cdot)$ is polynomial and the sets $\mathcal{X}$, $\mathcal{X}_0$, $\mathcal{X}_u$, $\mathcal{D}$ are semialgebraic, then a polynomial function $B_0(x)$ satisfying (9)–(11) can be searched using sum of squares programming. A similar statement can be made regarding the barrier certificates satisfying the conditions in the next subsections. The way this search is performed is analogous to what described in [13].

B. Functional Structure 2

In the second class of functionals, we will add first order integral terms to the functional $B(x_t)$. More specifically, the functional is of the form

$$B(x_t) = B_0(x(t)) + \sum_{i=1}^{\ell} \int_{-r_i}^{0} B_i(x(t+\theta))d\theta \tag{12}$$

where $B_0 \in C^1(\mathbb{R}^n)$ and $B_i \in C(\mathbb{R}^n)$, $i = 1,\ldots,\ell$. Notice that this functional reduces to the one we used in the previous subsection if $B_i(x) = 0$, $i = 1,\ldots,\ell$. Functionals of the form (12) are among the classes of functionals used with the Lyapunov-Krasovskii theorem for stability analysis of time-delay systems [6], [12].

Conditions guaranteeing safety when the above functional is used are stated in the following theorem.

Theorem 9: Let the system (6) and the sets $\mathcal{X} \subseteq \mathbb{R}^n$, $\mathcal{D} \subseteq \mathbb{R}^m$, $\mathcal{X}_0 \subseteq \mathcal{X}$ and $\mathcal{X}_u \subseteq \mathcal{X}$ be given, with $\hat{f} \in C(\mathbb{R}^{(\ell+1)n+m}, \mathbb{R}^n)$ and $\mathcal{X}_0 \cap \mathcal{X}_u = \emptyset$. Suppose there exist a positive constant ϵ and functions $B_0 \in C^1(\mathbb{R}^n)$, and $B_i \in C(\mathbb{R}^n)$, $i = 1, \ldots, \ell$ that satisfy the following conditions:

$$B_0(x) + \sum_{i=1}^{\ell} r_i B_i(\hat{x}_i) \leq -\epsilon \quad \forall (x, \hat{x}_1, \ldots, \hat{x}_\ell) \in \mathcal{X}_0^{\ell+1}, \tag{13}$$

$$B_0(x) + \sum_{i=1}^{\ell} r_i B_i(\hat{x}_i) \geq \epsilon \quad \forall (x, \hat{x}_1, \ldots, \hat{x}_\ell) \in \partial\mathcal{X}_u \times (\mathcal{X} \setminus \mathcal{X}_u)^\ell, \tag{14}$$

$$\frac{\partial B_0}{\partial x}(x)\hat{f}(x, \hat{x}_1, \ldots, \hat{x}_\ell, d) + \sum_{i=1}^{\ell}[B_i(x) - B_i(\hat{x}_i)] \leq 0 \quad \forall (x, \hat{x}_1, \ldots, \hat{x}_\ell, d) \in \mathcal{X}^{(\ell+1)} \times \mathcal{D}, \tag{15}$$

then the safety of the system (6) in the sense of Definition 4 is guaranteed.

Proof: Suppose that functions $B_0(x)$, $B_1(x)$ satisfying the conditions in the proposition can be found, but there exist $T > 0$, a piecewise continuous and bounded disturbance input $d : [0, T] \to \mathcal{D}$, and a corresponding unsafe trajectory $x : [-r, T] \to \mathcal{X}$. Now consider the evolution $B(x_t)$ as defined in (12) along the time interval $[0, T]$ for this trajectory. Since $x_0 \in X_0$ and also condition (13) holds, initially we have

$$\begin{aligned} B(x_0) &= B_0(x(0)) + \sum_{i=1}^{\ell} \int_{-r_i}^{0} B_i(x(t+\theta))d\theta \\ &\leq B_0(x(0)) + \sum_{i=1}^{\ell} r_i \sup_{\theta \in [-r_i, 0]} B_i(x(\theta)) \\ &\leq \sup_{x \in \mathcal{X}_0} B_0(x) + \sum_{i=1}^{\ell} r_i \sup_{\hat{x}_i \in \mathcal{X}_0} B_i(\hat{x}_i) \\ &\leq 0 \end{aligned}$$

Now, it follows from Lemma 5 that there exists $\tilde{t} \in [0, T]$ such that $x_{\tilde{t}} \in X_u$. At time $\tilde{t}$, we have

$$\begin{aligned} B(x_{\tilde{t}}) &= B_0(x(\tilde{t})) + \sum_{i=1}^{\ell} \int_{-r_i}^{0} B_i(x(\tilde{t}+\theta))d\theta \\ &\geq B_0(x(\tilde{t})) + \sum_{i=1}^{\ell} r_i \inf_{\theta \in [-r_i, 0]} B_i(x(\tilde{t}-\theta)) \\ &\geq \inf_{x \in \partial\mathcal{X}_u} B_0(x) + \sum_{i=1}^{\ell} r_i \inf_{\hat{x}_i \in \mathcal{X} \setminus \mathcal{X}_u} B_i(\hat{x}_i) \\ &> 0, \end{aligned}$$

where the last inequality follows because of (14). Finally, the time derivative for $B(x_t)$ on $t \in [0, \tilde{t}]$ satisfies

$$\begin{aligned} \frac{dB}{dt}(x_t) &= \frac{\partial B_0}{\partial x}(x(t))\hat{f}(x(t), x(t-r_1), ..., x(t-r_\ell), d(t)) \\ &\quad + \sum_{i=1}^{\ell} B_i(x(t)) - B_i(x(t-r_i)) \\ &\leq 0, \end{aligned}$$

as implied by (15). All these generate a contradiction, and thus we conclude that such an unsafe trajectory cannot exist, i.e., the system is safe. ■

Remark 10: Notice that now the delays $r_1, \ldots r_\ell$ appear in the conditions of Theorem 9. Thus, in general, the safety property proven in this case will be delay dependent.

C. Functional Structure 3

For brevity, in this section assume that there is only one delay, i.e., $\ell = 1$; it is straightforward to extend the result to handle multiple delays. The last functional structure that we consider in this paper contains second order integrals:

$$B(x_t) = B_0(x(t)) + \int_{-r}^{0} B_1(\theta, x(t), x(t+\theta))d\theta + \int_{-r}^{0}\int_{t+\theta}^{t} B_2(x(\eta))d\eta d\theta. \tag{16}$$

Lyapunov-Krasovskii functional with this structure has been proposed for stability analysis, e.g., in [12]. The functional is more general than (12), but it may reduce to (12) when $B_1(\theta, x(t), x(t+\theta))$ is independent of its first and second arguments and $B_2(x(\eta))$ is zero. Thus, the safety test in Theorem 11 below will generally be less conservative than the one in Theorem 9. This comes at the expense of more computational cost.

Theorem 11: Let the system $\dot{x}(t) = \hat{f}(x(t), x(t-r), d(t))$ and the sets $\mathcal{X} \subseteq \mathbb{R}^n$, $\mathcal{D} \subseteq \mathbb{R}^m$, $\mathcal{X}_0 \subseteq \mathcal{X}$ and $\mathcal{X}_u \subseteq \mathcal{X}$ be given, with $\hat{f} \in C(\mathbb{R}^{2n+m}, \mathbb{R}^n)$ and $\mathcal{X}_0 \cap \mathcal{X}_u = \emptyset$. Suppose there exist a positive constant ϵ and functions $B_0(x) \in C^1(\mathbb{R}^n)$, $B_1(\theta, x, \hat{x}_1) \in C^1(\mathbb{R}^{1+2n})$, and $B_2(\hat{x}_2) \in C(\mathbb{R}^n)$ that satisfy conditions (17)–(19) on page 5, then the safety of the system in the sense of Definition 4 is guaranteed.

Proof: Suppose that functions $B_0(x)$, $B_1(\theta, x, \hat{x}_1)$, $B_2(\hat{x}_2)$ satisfying the conditions in the proposition can be found, but there exist $T > 0$, a piecewise continuous and bounded disturbance input $d : [0, T] \to \mathcal{D}$, and a corresponding unsafe trajectory $x : [-r, T] \to \mathcal{X}$. Consider the evolution $B(x_t)$ of the form (16) along the time interval

$$B_0(x) + rB_1(\theta, x, \hat{x}_1) + \frac{1}{2}r^2 B_2(\hat{x}_2) \leq -\epsilon \quad \forall(\theta, x, \hat{x}_1, \hat{x}_2) \in [-r, 0] \times \mathcal{X}_0^3, \tag{17}$$

$$B_0(x) + rB_1(\theta, x, \hat{x}_1) + \frac{1}{2}r^2 B_2(\hat{x}_2) \geq \epsilon \quad \forall(\theta, x, \hat{x}_1, \hat{x}_2) \in [-r, 0] \times \partial\mathcal{X}_u \times (\mathcal{X} \setminus \mathcal{X}_u)^2, \tag{18}$$

$$\frac{\partial B_0}{\partial x}(x)\hat{f}(x, \hat{x}_1, d) + B_1(0, x, x) - B_1(-r, x, \hat{x}_1) + r\left(\frac{\partial B_1}{\partial x}(\theta, x, \hat{x}_2)\hat{f}(x, \hat{x}_1, d) - \frac{\partial B_1}{\partial \theta}(\theta, x, \hat{x}_2) + B_2(x) - B_2(\hat{x}_2)\right) \leq 0$$
$$\forall(\theta, x, \hat{x}_1, \hat{x}_2, d) \in [-r, 0] \times \mathcal{X}^3 \times \mathcal{D}, \tag{19}$$

$$\begin{aligned}
\frac{dB}{dt}(x_t) &= \frac{\partial B_0}{\partial x}(x(t))\hat{f}(x(t), x(t-r), d(t)) + B_1(0, x(t), x(t)) - B_1(-r, x(t), x(t-r)) \\
&\quad + \int_{-r}^{0}\left[\frac{\partial B_1}{\partial x}(\theta, x(t), x(t+\theta))\hat{f}(x(t), x(t-r), d(t)) - \frac{\partial B_1}{\partial \theta}(\theta, x(t), x(t+\theta)) + B_2(x(t)) - B_2(x(t+\theta))\right] d\theta \\
&= \frac{1}{r}\int_{-r}^{0}\left[\frac{\partial B_0}{\partial x}(x(t))\hat{f}(x(t), x(t-r), d(t)) + B_1(0, x(t), x(t)) - B_1(-r, x(t), x(t-r))\right. \\
&\quad \left. + r\left(\frac{\partial B_1}{\partial x}(\theta, x(t), x(t+\theta))\hat{f}(x(t), x(t-r), d(t)) - \frac{\partial B_1}{\partial \theta}(\theta, x(t), x(t+\theta)) + B_2(x(t)) - B_2(x(t+\theta))\right)\right] d\theta \\
&\leq 0
\end{aligned} \tag{20}$$

$[0, T]$ for this trajectory. Initially, we have

$$\begin{aligned}
B(x_0) &= B_0(x(0)) + \int_{-r}^{0} B_1(\theta, x(0), x(\theta))d\theta \\
&\quad + \int_{-r}^{0}\int_{\theta}^{0} B_2(x(\eta))d\eta d\theta \\
&\leq \sup_{x\in\mathcal{X}_0}\left[B_0(x) + r\sup_{\theta\in[-r,0],\hat{x}_1\in\mathcal{X}_0} B_1(\theta, x, \hat{x}_1)\right] \\
&\quad + \frac{1}{2}r^2 \sup_{\hat{x}_2\in\mathcal{X}_0} B_2(\hat{x}_2) \\
&\leq 0,
\end{aligned}$$

because of (17). Next, from Lemma 5 it follows that there exists $\tilde{t} \in [0, T]$ such that $x_{\tilde{t}} \in X_u$. At time $\tilde{t}$, we have

$$\begin{aligned}
B(x_{\tilde{t}}) &= B_0(x(\tilde{t})) + \int_{-r}^{0} B_1(\theta, x(\tilde{t}), x(\tilde{t}+\theta))d\theta \\
&\quad + \int_{-r}^{0}\int_{\tilde{t}+\theta}^{\tilde{t}} B_2(x(\eta))d\eta d\theta \\
&\geq \inf_{x\in\partial\mathcal{X}_u}\left[B_0(x) + r\inf_{\theta\in[-r,0],\hat{x}_1\in\mathcal{X}\setminus\mathcal{X}_u} B_1(\theta, x, \hat{x}_1)\right] \\
&\quad + \frac{1}{2}r^2 \inf_{\hat{x}_2\in\mathcal{X}\setminus\mathcal{X}_u} B_2(\hat{x}_2) \\
&> 0,
\end{aligned}$$

which is implied by (18). Finally, condition(19) implies that the time derivative $\frac{dB}{dt}(x_t)$ satisfies (20) on page 5, because the term under the last integral is non-positive. This contradicts the first two conditions, and thus the theorem is proven. ∎

IV. Example

Consider a linear damped oscillator with delay:

$$\begin{bmatrix}\dot{x}_1(t) \\ \dot{x}_2(t)\end{bmatrix} = \begin{bmatrix}\gamma x_2(t) + (1-\gamma)x_2(t-r) \\ -\gamma x_1(t) - (1-\gamma)x_1(t-r) - 1.5x_2(t)\end{bmatrix}. \tag{21}$$

In this system, $r > 0$ is the delay, and $\gamma \in [0, 1]$ is a parameter that we will vary. Also given are the sets

$$\begin{aligned}
\mathcal{X} &= \{x \in \mathbb{R}^2 : 0.01 \leq x_1^2 + x_2^2 \leq 4\}, \\
\mathcal{X}_0 &= \{x \in \mathbb{R}^2 : x_1^2 + (x_2 - 1)^2 \leq 0.01\}, \\
\mathcal{X}_u &= \{x \in \mathbb{R}^2 : x_1^2 + (x_2 - 0.5)^2 \leq 0.01\},
\end{aligned}$$

with the interpretation as described in Section III.

Let us first consider $\gamma = 1$, namely the case when there is no time-delay component. The objective of the safety verification is to show that a trajectory starting from $\mathcal{X}_0$ never enters $\mathcal{X}_u$, as long as it stays in $\mathcal{X}$. Since the system is asymptotically stable, all trajectories starting from $\mathcal{X}_0$ will eventually exit $\mathcal{X}$, but we say that the safety property holds if $\mathcal{X}_u$ is not entered beforehand. In this case, a quartic polynomial barrier certificate satisfying the conditions in Proposition 2 can be found using sum of squares programming, and therefore we conclude that the system is safe.

The question now is whether the safety property still holds when γ is not equal to 1. It may be the case that when γ is sufficiently large the system will still be safe for arbitrary delay size, whereas when γ is small the system may be unsafe for some r. In what follows, the safety of the system for various $\gamma \neq 1$ will be verified using the functionals proposed in Section III.

A. Delay-Independent Safety

Using the functional proposed in Section III-A, it is possible to prove safety for $\gamma = 0.98$. We obtain $B_0(x)$ of degree 4 given below:

$$\begin{aligned} B_0(x) = &-4.2979 + 1.1595x_1 + 2.3689x_2 + 50.757x_1^2 \\ &+ 77.613x_2x_1 + 54.871x_2^2 - 164.47x_1^3 \\ &- 318.22x_2x_1^2 - 274.8x_2^2x_1 - 103.64x_2^3 \\ &+ 150.17x_1^4 + 316.84x_2x_1^3 + 340.79x_2^2x_1^2 \\ &+ 192.1x_2^3x_1 + 49.452x_2^4 \end{aligned}$$

The semidefinite program computation can be performed in less than 2 seconds on a Pentium III 600 MHz PC. In this case, $B_0(x)$ proves that the system is safe for arbitrary delay r.

B. Delay-Dependent Safety

We will next use the functional proposed in Section III-B to prove safety. For this, we fix the value of the delay at $r = 1$. Since this functional is more general than the one in Section III-A, we expect that safety for lower values of γ can be proven. In fact, when $B_0(x)$ and $B_1(\hat{x})$ are chosen to be quartic, we are able to prove safety for $\gamma = 0.9$. The values of $B_0(x)$ and $B_1(\hat{x})$ that accomplish this are

$$\begin{aligned} B_0(x) = &-7.9177 + 5.6872x_1 + 13.07x_2 + 136.03x_1^2 \\ &+ 297.32x_2x_1 + 215.56x_2^2 - 493.54x_1^3 \\ &- 1209.6x_2x_1^2 - 1133.3x_1x_2^2 - 430.19x_2^3 \\ &+ 466.83x_1^4 + 1178.8x_2x_1^3 + 1380x_2^2x_1^2 \\ &+ 812.63x_1x_2^3 + 211.14x_2^4, \\ B_1(\hat{x}) = &-7.9177 - .53059\hat{x}_1 + .065907\hat{x}_2 + 12.637\hat{x}_1^2 \\ &+ 8.9339\hat{x}_1\hat{x}_2 + 9.2379\hat{x}_2^2 - 35.061\hat{x}_1^3 \\ &- 39.362\hat{x}_2\hat{x}_1^2 - 28.972\hat{x}_2^2\hat{x}_1 - 17.266\hat{x}_2^3 \\ &+ 35.937\hat{x}_1^4 + 37.503\hat{x}_2\hat{x}_1^3 + 41.468\hat{x}_1^2\hat{x}_2^2 \\ &+ 19.53\hat{x}_2^3\hat{x}_1 + 8.7079\hat{x}_2^4. \end{aligned}$$

The semidefinite program computation was performed in less than 3 seconds on a Pentium III 600 MHz PC.

Finally, we consider the functional proposed in Section III-C. Again the value of the delay is fixed at $r = 1$. When the B_i's are chosen to be quartic, we are able to prove safety for $\gamma = 0.7$. The expressions of $B_0(x)$, $B_1(\theta, x, \hat{x})$, $B_2(\tilde{x})$ that accomplish this are too long to be written here and therefore are omitted. However, the semidefinite program computation was performed in less than 20 seconds.

V. Conclusions

In the previous sections, we have provided a methodology for safety verification of time-delay systems based on functionals of states used as barrier certificates. A hierarchy of functional structures have been proposed to prove safety with decreasing levels of conservatism. A numerical example has been provided to illustrate the use of the methodology.

Acknowledgements

The work of the first author was financially supported by the Army Institute for Collaborative Biotechnologies, the NSF Award CCF-0326635 "ITR COLLAB: Theory and Software Infrastructure for a Scalable Systems Biology," and the AFOSR Award FA9550-05-1-0032 "Bio Inspired Networks." The first author would also like to thank Antonis Papachristodoulou for the enlightening discussions on time-delay systems.

References

[1] R. Alur, T. Dang, and F. Ivancic. Progress on reachability analysis of hybrid systems using predicate abstraction. In *Hybrid Systems: Computation and Control, LNCS 2623*, pages 4–19. Springer-Verlag, Heidelberg, 2003.

[2] A. Bemporad, F. D. Torrisi, and M. Morari. Optimization-based verification and stability characterization of piecewise affine and hybrid systems. In *Hybrid Systems: Computation and Control, LNCS 1790*, pages 45–58. Springer-Verlag, Heidelberg, 2000.

[3] A. Chutinan and B. H. Krogh. Computational techniques for hybrid system verification. *IEEE Transactions on Automatic Control*, 48(1):64–75, 2003.

[4] E. M. Clarke, Jr., O. Grumberg, and D. A. Peled. *Model Checking*. MIT Press, Cambridge, MA, 2000.

[5] S. Glavaski, A. Papachristodoulou, and K. Ariyur. Controlled hybrid system safety verification: Advanced life support system testbed. To appear in Proceedings of the American Control Conference, 2005.

[6] K. Gu, V. L. Kharitonov, and J. Chen. *Stability of Time–Delay Systems*. Birkhäuser, Boston, MA, 2003.

[7] J. K. Hale and S. M. V. Lunel. *Introduction to Functional Differential Equations*. Springer, New York, NY, 1993.

[8] G. Lafferriere, G. J. Pappas, and S. Yovine. Symbolic reachability computations for families of linear vector fields. *Journal of Symbolic Computation*, 32(3):231–253, 2001.

[9] F. Mazenc and S.-I. Niculescu. Lyapunov stability analysis for nonlinear delay systems. *Systems and Control Letters*, 42(4):245–251, 2001.

[10] J. D. Murray. *Mathematical Biology I: An Introduction*. Springer, New York, NY, 2002.

[11] S.-I. Niculescu. *Delay Effects on Stability: A Robust Control Approach*. Springer-Verlag, New York, NY, 2001.

[12] A. Papachristodoulou. Analysis of nonlinear time–delay systems using the sum of squares decomposition. In *Proceedings of the American Control Conference*, 2004.

[13] S. Prajna and A. Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *Hybrid Systems: Computation and Control, LNCS 2993*, pages 477–492. Springer-Verlag, Heidelberg, 2004.

[14] S. Prajna, A. Jadbabaie, and G. J. Pappas. Stochastic safety verification using barrier certificates. In *Proceedings of the IEEE Conference on Decision and Control*, 2004.

[15] S. Prajna, A. Papachristodoulou, P. Seiler, and P. A. Parrilo. SOSTOOLS and its control applications. In A. Garulli and D. Henrion, editors, *Positive Polynomials in Control*. Springer-Verlag, 2005. Software available at http://www.cds.caltech.edu/sostools and http://www.mit.edu/~parrilo/sostools.

[16] S. Prajna and A. Rantzer. On the necessity of barrier certificates. In *Proceedings of the IFAC World Congress*, 2005.

[17] S. Prajna and A. Rantzer. Primal–dual tests for safety and reachability. In *Hybrid Systems: Computation and Control, LNCS 3414*, pages 542–556. Springer-Verlag, Heidelberg, 2005.

[18] D. E. Seborg, T. F. Edgar, and D. A. Mellichamp. *Process Dynamics and Control*. Wiley, 2004.

[19] R. Srikant. *The Mathematics of Internet Congestion Control*. Birkhäuser, Boston, MA, 2004.

[20] A. Tiwari and G. Khanna. Nonlinear systems: Approximating reach sets. In *Hybrid Systems: Computation and Control, LNCS 2993*, pages 600–614. Springer-Verlag, Heidelberg, 2004.

[21] C. J. Tomlin, I. Mitchell, A. M. Bayen, and M. Oishi. Computational techniques for the verification of hybrid systems. *Proceedings of the IEEE*, 91(7):986–1001, 2003.