Barrier Certificate Generation for Safety Verification of Hybrid Systems for a Given Period of Time

Extended Abstract

Ting Gan, Liyun Dai and Bican Xia

Embedded systems make use of computer units to control physical devices so that the behavior of the controlled devices meets expected requirements, which have become ubiquitous in our modern life. How to design correct embedded systems is a grand challenge for computer science and control theory. Model-driven development (MDD) was considered as an effective way of developing correct complex embedded systems, and has been successfully applied in industry [9, 14]. In the framework of MDD, a formal model of the system to be developed is defined at the beginning, and then extensive analysis and verification are done based on the formal model so that errors can be detected and corrected at the very early stage of the design of the system. Afterwards, model transformation techniques are applied to transform the abstract formal model into lower level models, even into source code. Hybrid systems combine discrete mode changes with continuous evolutions specified in the form of differential equations. With mathematically precise semantics, hybrid systems can serve as an appropriate model of embedded systems [15, 2].

There are many previous work about how to prove the safety of hybrid systems without time bounded [1, 8, 13] . On the another hand most actions of embedded system have a time limit [20, 6, 3]. In this paper we provide a method that can generate a barrier certificate which is sufficient to prove the safety of a hybrid system for a given period of time based on the previous work [17, 11]. We have three main contributions in this paper: (A) we present a barrier certificate condition, called *Exponential-Linear condition*, which is proved to be a sufficient condition for the safety of the given hybrid system in a bounded time; (B) for the semi-algebraic hybrid systems (where all functions involved are polynomials), we propose a sound method to generate barriers using the semidefinite programming method; (C) we give some examples to illustrate the effectiveness of our method.

A continuous system is defined by an ordinary differential equation (ODE)

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

where $x \in \mathbb{R}^n$ and f is a Lipschitz continuous vector function from $\mathbb{R}^n$ to $\mathbb{R}^n$. Given a continuous system (1) and an initial set, the set of all the points that the system can reach from the initial set, following the vector fields $f(x)$, is called the reachable set.

Our problem is: For a given system (1), an initial set, an unsafe set and a given period of time, verify that the system will never reach a point in the unsafe set for the given period of time. In other words, prove the intersection of the unsafe set and the reachable set in the bounded time is empty.

M. Kosta and T. Sturm, eds. Proceedings of the MACIS 2013, Nanning, China, December 11-13, 2013.

Lemma 1. *Given a continuous system (1), an initial set* $\mathbf{I}$ *and an unsafe set* $\mathbf{U}$*, for any given* $\lambda, \eta \in \mathbb{R}, \lambda < 0, \eta > 0$*, if there exists a real-valued function* $\varphi(x) \in \mathcal{C}^1(\mathbb{R}^n)$ *satisfying the following formulae:*

$$\forall x \in \mathbf{I} : \varphi(x) \leq 0 \tag{2}$$

$$\forall x \in \mathbb{R}^n : \mathcal{L}_f\varphi(x) - \lambda\varphi(x) - \eta \leq 0 \tag{3}$$

$$\forall x \in \mathbf{U} : \varphi(x) \geq \eta \tag{4}$$

then the safety property is satisfied by the system $\mathbf{S}$ *when* $t \in [0, 1]$.

Before prove this lemma, we first proof another lemma.

Lemma 2. *For a real-valued function* $\theta(t) \in \mathcal{C}^1(\mathbb{R}^n)$*, if*

$$\begin{cases} \frac{\partial\theta}{\partial t} - \lambda\theta(t) - \eta = 0 \\ \theta(0) \leq 0 \end{cases}$$

where $\lambda, \eta \in \mathbb{R}, \lambda < 0, \eta > 0$*, then* $\forall 0 \leq \xi \leq 1, \theta(\xi) < \eta$.

Proof. Let $\beta\lambda = \eta, \theta_0 = \theta(0)$, then $\beta < 0, \theta_0 \leq 0$.

$$\begin{aligned} & \frac{\partial\theta}{\partial t} - \lambda\theta(t) - \eta = 0 \\ \Rightarrow & \frac{\partial\theta}{\partial t} = \lambda\theta + \eta \\ \Rightarrow & \frac{\partial\theta}{\lambda\theta + \eta} = \partial t \\ \Rightarrow & \frac{d\theta}{\lambda(\theta + \beta)} = dt \\ \Rightarrow & \frac{d\theta}{\theta + \beta} = \lambda dt \\ \Rightarrow & \theta + \beta = (\theta_0 + \beta)e^{\lambda t} \\ \Rightarrow & \theta(t) = \theta_0 e^{\lambda t} + \beta(e^{\lambda t} - 1). \end{aligned}$$

When $0 < \xi \leq 1$, then $\lambda\xi < 0$. So we have $e^{\lambda\xi} > 1 + \lambda\xi$ and thus $e^{\lambda\xi} - 1 > \lambda\xi$. For $\beta < 0$, then we have $\beta(e^{\lambda\xi} - 1) < \beta\lambda\xi = \eta\xi \leq \eta$, so, $\beta(e^{\lambda\xi} - 1) < \eta$. Since $\theta_0 e^{\lambda\xi} \leq 0$, it is clear that

$$\forall 0 \leq \xi \leq 1, \theta(\xi) < \eta.$$

□

Now, we use Lemma 2 to prove Lemma 1.

Proof. Suppose there exists a real-valued function $\varphi(x)$ satisfying the three conditions in Lemma 1. From the second condition we have:

$$\mathcal{L}_f\varphi - \lambda\varphi - \eta \leq 0.$$

Since

$$\frac{\partial\varphi(x(t))}{\partial t} = \frac{\partial\varphi}{\partial x}\frac{\partial x}{\partial t} = \frac{\partial\varphi}{\partial x}f(x) = \mathcal{L}_f\varphi,$$

we have

$$\frac{\partial\varphi}{\partial t} - \lambda\varphi - \eta \leq 0. \tag{5}$$

Suppose θ is a function satisfying $\theta_0 = \theta(0) = \varphi(0) = \varphi_0 \leq 0$ and

$$\frac{\partial\theta}{\partial t} - \lambda\theta - \eta = 0, \tag{6}$$

then from Lemma 2 we know that

$$\forall 0 \leq t \leq 1, \theta(t) < \eta. \tag{7}$$

From inequality (5) and equation (6) we have

$$\begin{cases} (\varphi - \theta)_0 = \varphi(0) - \theta(0) = 0, \\ \frac{\partial(\varphi-\theta)}{\partial t} - \lambda(\varphi - \theta) \leq 0. \end{cases} \tag{8}$$

Therefore, $\varphi - \theta \leq 0$ is guaranteed by Theorem 1 in [11]. Since the condition (7) hold for θ, we have

$$\forall 0 \leq t \leq 1, \varphi(t) < \eta.$$

It means that $\varphi(x) < \eta$ for any point x that the continuous system (1) can reach with $t \in [0, 1]$. But $\varphi(x) \geq \eta$ for all the points in the unsafe set. So the safety property is satisfied when $t \in [0, 1]$. □

Theorem 3. (**Exponential − Linear condition**) *Given a continuous system* $\mathbf{S}$*, an initial set* $\mathbf{I}$*, an unsafe set* $\mathbf{U}$ *and a bounded time* $T > 0$*, for any given* $\lambda, \eta \in \mathbb{R}, \lambda < 0, \eta > 0$*, if there exists a real-valued function* $\varphi(x) \in \mathcal{C}^1(\mathbb{R}^n)$ *satisfying the following formulae:*

$$\begin{aligned} \forall x \in \mathbf{I} : \varphi(x) &\leq 0 \\ \forall x \in \mathbb{R}^n : \mathcal{L}_f\varphi(x) - \lambda\varphi(x) - \frac{\eta}{T} &\leq 0 \\ \forall x \in \mathbf{U} : \varphi(x) &\geq \eta \end{aligned}$$

then the safety property is satisfied by the system $\mathbf{S}$ *when* $t \in [0, T]$.

Proof. The difference between the conditions in Lemma 1 and Theorem 3 is just the second condition. Then, we convert the second condition in Theorem 3 to the same form as the second condition in Lemma 1. Let $p = \frac{t}{T}$, and take the place of t in Theorem 3, then we have

$$\begin{aligned} \forall x \in \mathbf{I} : \varphi(x) &\leq 0 \\ \forall x \in \mathbb{R}^n : \mathcal{L}_{\hat{f}}\varphi(x) - T\lambda\varphi(x) - \eta &\leq 0 \\ \forall x \in \mathbf{U} : \varphi(x) &\geq \eta \end{aligned}$$

where $\hat{f} = Tf$. Since $T\lambda < 0$, by Lemma 1 we know

$$\forall 0 \leq p \leq 1, \varphi(p) < \eta.$$

Because $p = \frac{t}{T}$,

$$\forall 0 \leq t \leq T, \varphi(t) < \eta.$$

Therefore the safety property is satisfied when $t \in [0, T]$. □

Remark 4. If the conditions of Theorem 3 are satisfied, then $\varphi(x) = \eta$ is called a *bounded time barrier certificate*.

Theorem 5. *Given a continuous system* $\mathbf{S}$*, an initial set* $\mathbf{I}$ *, an unsafe set* $\mathbf{U}$*, a time bound* $T > 0$ *and an over-approximation set* $\mathbb{B}$ *of the reachable set without time bound, for any given* $\lambda, \eta \in \mathbb{R}, \lambda < 0, \eta > 0$*, if there exists a real-valued function* $\varphi(x) \in \mathcal{C}^1(\mathbb{R}^n)$ *satisfying the following formulae:*

$$\begin{aligned} \forall x \in \mathbf{I} : \varphi(x) &\leq 0 \\ \forall x \in \mathbb{B} : \mathcal{L}_f\varphi(x) - \lambda\varphi(x) - \frac{\eta}{T} &\leq 0 \\ \forall x \in \mathbf{U} : \varphi(x) &\geq \eta \end{aligned}$$

then the safety property is satisfied by the system $\mathbf{S}$ *when* $t \in [0, T]$.

Proof. For any given $x_0 \in \mathbf{I}$, let $\mathcal{T}(t) = \{x(\xi)|0 \leq \xi \leq t, x(0) = x_0\}$. Then, we know $\mathcal{T} \subset \mathbb{B}$. Thus the conditions below hold for $\mathcal{T}$

$$\begin{cases} \mathcal{L}_f\varphi(x(t)) - \lambda\varphi(x(t)) - \frac{\eta}{T} \leq 0, \\ \varphi(x(0)) = \varphi(x_0) \leq 0. \end{cases}$$

From the proof of Theorem 3 and Lemma 1, it is easy to see $\varphi(x) < \eta$ for $x \in \mathcal{T}(T)$. Because x_0 is arbitrarily chosen, we know $\varphi(x) < \eta$ hold for any x which is reachable with $t \in [0, T]$. Since $\varphi(x) \geq \eta$ hold for any x in the unsafe set, the safety property hold when $t \in [0, T]$. □

Theorem 3 or Theorem 5 gives a sufficient condition for the safety of the system (1) for a given period of time. It is easy to see that the real-valued function $\varphi(x)$ separate the reachable set and the unsafe set. To find the function $\varphi(x)$ for the semi-algebraic hybrid systems, we can use semidefinite programming tools such as SOSTOOLS [18] to solve the constraints in Theorem 3 and Theorem 5.

Example. Consider the second-order system [17, 11]:

$$\begin{cases} \dot{x} = y, \\ \dot{y} = -x + \frac{1}{3}x^3 - y. \end{cases}$$

Given the initial set $\mathbf{I} = \{(x, y) \in \mathbb{R}^2|(x - 1.5)^2 + y^2 \leq 0.25\}$ and the unsafe set $\mathbf{U} = \{(x, y) \in \mathbb{R}^2|x^2 + y^2 \leq 0.16\}$, we want to verify that the system will never evolve into the unsafe set when starting from the initial set with time from 0 to 0.5.

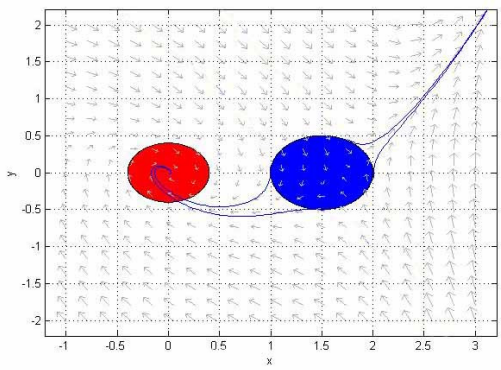

FIGURE 1. The blue region is the reachable set of the system in example without bounded time and the red region is the unsafe set.

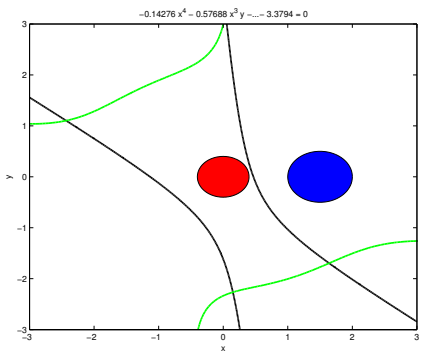

FIGURE 2. The green curve is the boundary of the over-approximation set of the reachable set, the black curve is a time bounded barrier certificate, the blue region is the initial set, and the red region is the unsafe set.

It's easy to see from Fig. 1 that the safety of this system must take time into account. We consider the conditions in Theorem 5. First we give an over-approximation set $\mathbf{B}$ of the reachable set by the

SOSTOOLS . Next, also using SOSTOOLS to obtain a time bounded barrier certificate. Fig. 2 is a result obtained in this way.

References

[1] R. Alur, C. Courcoubetis, N. Halbwachs, T. Henzinger, P. H. Ho, X. Nicollin, A. Olivero, J. Sifakis and S. Yovine: The algorithmic analysis of hybrid systems. Theoretical Computer Science, 138(1):3–34. 1995.

[2] R. Alur, C. Courcoubetis, T. A. Henzinger and P. H. Ho: Hybrid automata: An algorithmic approach to the specification and verification of hybrid systems. In Hybrid Systems, LNCS 736, pp. 209–229. Springer, 1993.

[3] S. P. Bhat and D. S. Bernstein: Continuous finite-time stabilization of the translational and rotational double integrators. Automatic Control, IEEE Transactions on, 43(5):678–682, 1998.

[4] L. Bu, Y. Li, L. Wang, X. Chen and X. Li: Bach 2: Bounded reachability checker for compositional linear hybrid systems. In Proceedings of the Conference on Design, Automation and Test in Europe, pp. 1512–1517. European Design and Automation Association, 2010.

[5] L. Dai, B. Xia and N. Zhan: Generating non-linear interpolants by semidefinite programming. In CAV'13, LNCS 8044, pp. 364–380. Springer, 2013.

[6] G. Garcia, S. Tarbouriech and J. Bernussou: Finite-time stabilization of linear time-varying continuous systems. Automatic Control, IEEE Transactions on, 54(2):364–369. 2009.

[7] S. Gulwani and A. Tiwari: Constraint-based approach for analysis of hybrid systems. In CAV'08, LNCS 5123, pp 190–203. Springer, 2008.

[8] T. A. Henzinger and P. H. Ho: Algorithmic analysis of nonlinear hybrid systems. In CAV'95, LNCS 939, pp. 225–238. Springer, 1995.

[9] T. A. Henzinger and J. Sifakis: The embedded systems design challenge. In FM'06, of LNCS 4085, pp. 1–15. Springer, 2006.

[10] H. K. Khalil: Nonlinear systems. Upper Saddle River: Prentice hall, 2002.

[11] H. Kong, F. He, X. Song, W. Hung and M. Gu: Exponential-condition-based barrier certificate generation for safety verification of hybrid systems. In CAV'13, LNCS 8044, pp. 242–257. Springer, 2013.

[12] H. Kong, X. Song, D. Han, M. Gu and J. Sun: A new barrier certificate for safety verification of hybrid systems. The Computer Journal, 2013.

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

[14] E. Lee: What's ahead for embedded software?, IEEE Computer, 33(9):18–26. 2000.

[15] O. Maler, Z. Manna and A. Pnueli: From timed to hybrid systems. In Proceedings of the Real-Time: Theory in Practice, REX Workshop, pp. 447–484. Springer, 1992.

[16] P. A. Parrilo: Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization. PhD thesis, California Inst. of Tech., 2000.

[17] S. Prajna and A. Jadbabaie: Safety verification of hybrid systems using barrier certificates. In HSCC'04, LNCS 2993, pp. 477–492. Springer, 2004.

[18] S. Prajna, A. Papachristodoulou, P. Seiler and P. A. Parrilo: Sostools and its control applications. In Positive polynomials in control, pp. 273–292. Springer, 2005.

[19] A. Puri and P. Varaiya: Decidability of hybrid systems with rectangular differential inclusions. In CAV'94, LNCS 818, pp. 95–104. Springer, 1994

[20] R. G. Sanfelice and A. R. Teel: Dynamical properties of hybrid systems simulators. Automatica, 46(2):239–248. 2010.

[21] N. Zhan, S. Wang and H. Zhao: Formal modelling, analysis and verification of hybrid systems. In Unifying Theories of Programming and Formal Engineering Methods, LNCS 8050, pp. 207–281. Springer, 2013.

Ting Gan
Corresponding author.
LMAM & School of Mathematical Sciences, Peking University
e-mail: gant@pku.edu.cn

Liyun Dai
LMAM & School of Mathematical Sciences, Peking University
Beijing International Center for Mathematical Research, Peking University
e-mail: dailiyun@pku.edu.cn

Bican Xia
LMAM & School of Mathematical Sciences, Peking University
e-mail: xbc@math.pku.edu.cn