SCIENCE CHINA
Information Sciences

• LETTER •

March 2017, Vol. 60 039102:1–039102:3
doi: 10.1007/s11432-015-0980-7

Linear invariant generation for verification of nonlinear hybrid systems via conservative approximation

Xia ZENG[1], Wang LIN[2,3*], Zhengfeng YANG[1] & Zhenbing ZENG[4]

[1]*Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai* 200062*, China;*
[2]*College of Mathematics and Information Science, Wenzhou University, Zhejiang* 325035*, China;*
[3]*State Key Laboratory for Novel Software Technology, Nanjing University, Jiangsu* 210093*, China;*
[4]*Department of Mathematics, Shanghai University, Shanghai* 200444*, China*

Received February 22, 2016; accepted April 22, 2016; published online September 27, 2016

Citation Zeng X, Lin W, Yang Z F, et al. Linear invariant generation for verification of nonlinear hybrid systems via conservative approximation. Sci China Inf Sci, 2017, 60(3): 039102, doi: 10.1007/s11432-015-0980-7

Dear editor,

Hybrid systems are widely used in modeling safety-critical systems [1]. In recent years, safety verification of hybrid systems, whose aim is to decide whether the systems will reach a dangerous or unwanted configuration, has attracted much research attention. Due to the intrinsic complexity, verification of such systems presents a grand challenge.

In recent years, several methods, based on numeric computation and symbolic computation, have been proposed to compute invariants for safety verification of hybrid systems. For example, polynomial optimization [2] via semidefinite programming (SDP) is utilized to compute invariants for polynomial hybrid systems [3, 4]. Taking advantage of the error-free property, several symbolic methods [5–7] are applied to providing mathematical proofs of the existence of invariants of hybrid systems. However, some are subject to numerical errors and some suffer from high computational complexity. Furthermore, the methods for handling polynomial hybrid systems cannot be extended to a more general class of non-polynomial hybrid systems. To resolve this issue, Ref. [8] proposed a symbolic abstraction approach for reducing non-polynomial hybrid systems to polynomial ones, and then studied properties of the latter systems instead.

In this letter, we suggest a new method for safety verification of general nonlinear hybrid systems. The main task can be reformulated as how to compute linear over-approximations for the nonlinear functions. For a given nonlinear function over a compact set, we propose a linear model (LM), composed of a linear approximate function and an error bound, as its over-approximation. The problem of computing the optimal LM is equivalent to dealing with a nonlinear optimization problem with universal quantifiers, which is computationally hard. To reduce the computational complexity, we present a new sampling-based relaxation approach to compute a tight LM, as the guaranteed over-approximation of the nonlinear function. Our linear approximation method can be easily applied to transform nonlinear hybrid systems into the associated linear ones with uncertain parameters, which is highly efficient and applicable to non-polynomial hybrid systems.

Safety verification. Let $\boldsymbol{H} : \langle V, L, \mathcal{T}, \Theta, \mathcal{D}, \Psi,$

* Corresponding author (email: linwang@wzu.edu.cn)

The authors declare that they have no conflict of interest.

$\ell_0\rangle$ be a hybrid system with the set V of system variables, the finite set L of locations, the set $\mathcal{T}$ of discrete transitions, the assertion Θ specifying the initial condition, the differential rule $\mathcal{D}(\ell)$ and location condition $\Psi(\ell)$ for each $\ell \in L$, and the initial location $\ell_0 \in L$. Given an unsafe assertion X_u, we determine whether $\boldsymbol{H}$ is safe, namely, trajectories of $\boldsymbol{H}$ starting from the initial condition Θ at the initial location ℓ_0, cannot evolve to any state specified by X_u.

As said in [2, 9], safety verification of the hybrid system $\boldsymbol{H}$ can be reduced to finding inequality inductive invariants $\varphi_\ell(\boldsymbol{x}) \geqslant 0$ for each location $\ell \in L$, which satisfy the following requirements:

Initiation: $\Theta \models \varphi_{\ell_0}(\boldsymbol{x}) \geqslant 0$,

Discrete consecution:

$$\varphi_\ell(\boldsymbol{x}) \geqslant 0 \wedge \mathcal{T} \models \varphi_{\ell'}(\boldsymbol{x}') \geqslant 0,$$

Continuous consecution:

$$\varphi_\ell(\boldsymbol{x}) = 0 \wedge \Psi(\ell) \models \dot{\varphi}_\ell(\boldsymbol{x}) > 0,$$

Safety: $X_u(\ell) \models \varphi_\ell(\boldsymbol{x}) < 0$.

A new method for safety verification of general nonlinear hybrid systems is suggested in this letter. We focus on how to transform a nonlinear hybrid system into an associated over-approximate linear system, whose safety property can be easily verified by quantifier elimination method. The key problem is how to compute the linear over-approximations for the nonlinear functions.

Linear approximation. A linear model (LM) over a compact set $\mathcal{D} \subset \mathbb{R}^n$ is a pair (ρ, X) of a linear function ρ over variables $\boldsymbol{x} \in \mathbb{R}^n$ and a remainder interval $X \in \mathbb{IR}$. We say that (ρ, X) is an over-approximation of a function $\phi : \mathcal{D} \to \mathbb{R}$, written as $\phi \in (\rho, X)$, iff for each $\boldsymbol{x} \in \mathcal{D}$ we have $\phi(\boldsymbol{x}) \in \rho(\boldsymbol{x}) + X := \{\rho(\boldsymbol{x}) + \kappa | \kappa \in X\}$, i.e., $\phi \in (\rho, X) \Longleftrightarrow \phi(\boldsymbol{x}) - \rho(\boldsymbol{x}) \in X$ for each $\boldsymbol{x} \in \mathcal{D}$.

Intuitively, one may try to compute the tightest LM, which can be done by computing $\boldsymbol{v}$ and a, b such that

$$\boldsymbol{v}^{\mathrm{T}} \cdot \boldsymbol{x} + a \leqslant \phi(\boldsymbol{x}) \leqslant \boldsymbol{v}^{\mathrm{T}} \cdot \boldsymbol{x} + b, \quad \forall \boldsymbol{x} \in \mathcal{D},$$

where $\boldsymbol{v} \in \mathbb{R}^n$, $\boldsymbol{v} \neq \boldsymbol{0}$, and the distance of two hyperplanes, that is $\frac{|b-a|}{\sqrt{\|\boldsymbol{v}\|_2^2+1}}$, is minimal. Therefore, the problem for searching the minimum-distance hyperplanes can be reformulated as follows:

$$\left.\begin{array}{l} \inf\limits_{\boldsymbol{v},a,b} \frac{(b-a)^2}{\|\boldsymbol{v}\|_2^2+1} \\ \text{s.t. } \phi(\boldsymbol{x}) - \boldsymbol{v}^{\mathrm{T}} \cdot \boldsymbol{x} - a \geqslant 0, \quad \forall \boldsymbol{x} \in \mathcal{D}, \\ \qquad \phi(\boldsymbol{x}) - \boldsymbol{v}^{\mathrm{T}} \cdot \boldsymbol{x} - b \leqslant 0, \quad \forall \boldsymbol{x} \in \mathcal{D}. \end{array}\right\} \tag{1}$$

To solve (1), we need to deal with an optimization problem with universal quantifiers, which is computationally hard. Hence, we propose a learning-based method to compute a suboptimal solution to (1) by using a relaxation technique. As shown in Figure 1, we first construct sampling hyperplanes $y - \boldsymbol{v}^{*\mathrm{T}} \cdot \boldsymbol{x} - a^* = 0$ and $y - \boldsymbol{v}^{*\mathrm{T}} \cdot \boldsymbol{x} - b^* = 0$ (dashed ones) by utilizing the sample points in $\mathcal{D}$, then relax these two hyperplanes to the verified ones (solid ones), which enclose $\phi(\boldsymbol{x})$ for all $\boldsymbol{x} \in \mathcal{D}$ and the distance is tight.

Let $c = \frac{2}{b-a}$, $d = \frac{a+b}{b-a}$ and $\boldsymbol{w} = c \cdot \boldsymbol{v}$, we have $\frac{(b-a)^2}{\|\boldsymbol{v}\|_2^2+1} = \frac{4}{c^2+\|\boldsymbol{w}\|_2^2}$. Therefore, Eq. (1) can be transformed into the following optimization problem:

$$\left.\begin{array}{l} p := \sup\limits_{\boldsymbol{w},c,d} \|\boldsymbol{w}\|_2^2 + c^2 \\ \text{s.t. } c\,\phi(\boldsymbol{x}) - \boldsymbol{w}^{\mathrm{T}} \cdot \boldsymbol{x} - d + 1 \geqslant 0, \ \forall \boldsymbol{x} \in \mathcal{D}, \\ \qquad c\,\phi(\boldsymbol{x}) - \boldsymbol{w}^{\mathrm{T}} \cdot \boldsymbol{x} - d - 1 \leqslant 0, \ \forall \boldsymbol{x} \in \mathcal{D}. \end{array}\right\} \tag{2}$$

Now we present a relaxation method to solve (2) by removing universal quantifiers. We first construct a rectangular mesh M in $\mathcal{D}$ with a mesh spacing $s \in \mathbb{R}_+$ (say $s = 0.05$) and mesh point set $\chi = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m\}$. Then, Eq. (2) can be relaxed as the following quadratic programming problem:

$$\left.\begin{array}{l} p^* := \sup\limits_{\boldsymbol{w},c,d} [\boldsymbol{w}, c]^{\mathrm{T}} \cdot [\boldsymbol{w}, c] \\ \text{s.t. } c\,\phi(\boldsymbol{x}_i) - \boldsymbol{w}^{\mathrm{T}} \cdot \boldsymbol{x}_i - d + 1 \geqslant 0, 1 \leqslant i \leqslant m, \\ \qquad c\,\phi(\boldsymbol{x}_j) - \boldsymbol{w}^{\mathrm{T}} \cdot \boldsymbol{x}_j - d - 1 \leqslant 0, 1 \leqslant j \leqslant m, \end{array}\right\} \tag{3}$$

whose objective function is 2-norm square of the variable vector. It is easy to solve (3) by use of its Karush-Kuhn-Tucker (KKT) conditions which becomes a linear programming problem. Suppose $\boldsymbol{w}^*$, c^* and d^* are the optimal solution of (3). Thus, the following sampling hyperplanes

$$\left.\begin{array}{l} c^* y - \boldsymbol{w}^{*\mathrm{T}} \cdot \boldsymbol{x} - d^* - 1 = 0, \\ c^* y - \boldsymbol{w}^{*\mathrm{T}} \cdot \boldsymbol{x} - d^* + 1 = 0, \end{array}\right\} \tag{4}$$

are able to enclose $\phi(\boldsymbol{x}_i)$ with $1 \leqslant i \leqslant m$, i.e., for each $\boldsymbol{x}_i$, the constrain conditions of (3) are satisfied.

Now, the remaining task is to relax the sampling hyperplanes (4) as verified ones, which can tightly enclose $\phi(\boldsymbol{x})$ over domain $\mathcal{D}$, that is, for each $\boldsymbol{x} \in \mathcal{D}$ the following conditions are satisfied exactly:

$$\left.\begin{array}{l} c^* \phi(\boldsymbol{x}) - \boldsymbol{w}^{*\mathrm{T}} \cdot \boldsymbol{x} - d^* - \delta - 1 \leqslant 0, \\ c^* \phi(\boldsymbol{x}) - \boldsymbol{w}^{*\mathrm{T}} \cdot \boldsymbol{x} - d^* + \delta + 1 \geqslant 0, \end{array}\right\} \tag{5}$$

and $\delta \in \mathbb{R}_{>0}$ is as small as possible. From the construction of mesh M in $\mathcal{D}$, for each $\boldsymbol{x} \in \mathcal{D}$, there exists a mesh point $\boldsymbol{x}_i$ in the same mesh with $\boldsymbol{x}$. Following the mean value theorem, $\phi(\boldsymbol{x})$ over

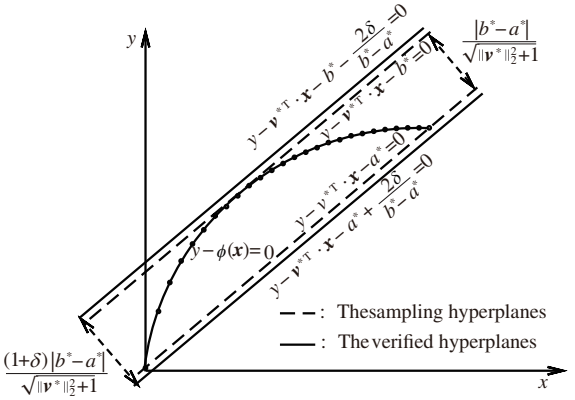

Figure 1 The sampling and verified hyperplanes.

$\boldsymbol{x}\in\mathcal{D}$ can be bounded by $|\phi(\boldsymbol{x})-\phi(\boldsymbol{x}_i)|\leqslant\frac{1}{2}ns\eta$, where $\eta=\sup_{\boldsymbol{x}\in\mathcal{D}}\|\nabla\phi(\boldsymbol{x})\|_\infty$. Thus, by choosing $\delta=\frac{s}{2}\left(c^*n\eta+\|\boldsymbol{w}^*\|_1\right)$, we can easily verify that the conditions in (5) hold, which means two hyperplanes enclosing $\phi(\boldsymbol{x})$ over $\mathcal{D}$ are obtained. Thus, (ρ,X) is a LM of $\phi(\boldsymbol{x})$ over $\mathcal{D}$, where $\rho(\boldsymbol{x})=\frac{\boldsymbol{w}^*}{c^*}\cdot\boldsymbol{x}+\frac{d^*}{c^*}$ and $X=[-\frac{1+\delta}{c^*},\frac{1+\delta}{c^*}]$.

Linear invariant generation. Let $\boldsymbol{H}:\langle V,L,\mathcal{T},\Theta,\mathcal{D},\Psi,\ell_0\rangle$ be a hybrid system whose components are all described by polynomial or non-polynomial functions in $\boldsymbol{x}$. By applying the above linear approximation method to compute the over-approximation LM for each nonlinear function involved in $\boldsymbol{H}$, we can obtain an over-approximate linear hybrid system $\boldsymbol{H_u}:\langle V,L,\overline{\mathcal{T}},\overline{\Theta},\overline{\mathcal{D}},\overline{\Psi},\ell_0\rangle$.

As stated above, safety verification of $\boldsymbol{H_u}$ can be reduced to finding inequality inductive invariants $\varphi_\ell(\boldsymbol{x})\geqslant 0$ for each location $\ell\in L$, which imply the safety property, then the safety of the system $\boldsymbol{H_u}$ is guaranteed. We will apply quantifier elimination method to obtain the sufficient and necessary condition on the existence of such inductive invariants of $\boldsymbol{H_u}$. From a computational point of view, we aim to compute a linear invariants $\varphi_\ell(\boldsymbol{x})$ for each $\ell\in L$. We first predetermine a linear template of invariants of the form $\varphi_\ell(\boldsymbol{x})=\alpha_\ell^{\mathrm{T}}\cdot\boldsymbol{x}$ where $\alpha_\ell\in\mathbb{R}^n$ is an unknown vector. We then apply quantifier elimination method to obtain the equivalent quantifier-free formulae with α_ℓ for all $\ell\in L$.

Suppose that $\varphi_\ell(\boldsymbol{x})\geqslant 0,\ell\in L$ are the computed linear invariants for safety verification of the uncertain linear hybrid system $\boldsymbol{H_u}$. Then, the existence of such $\varphi_\ell(\boldsymbol{x})$ also can ensure the safety of the original hybrid system $\boldsymbol{H}$ obviously.

Conclusion. In this letter, we consider the problem of safety verification of general nonlinear hybrid systems. A linear approximation approach, based on quadratic programming, is applied to transforming a given nonlinear hybrid system into an associated linear one with uncertain parameters, and quantifier elimination method is used to obtain linear invariants, which guarantee the safety property of the resulting uncertain linear hybrid system. The efficiency of the presented method is illustrated by some numerical examples.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Grant Nos. 11471209, 61321064) and Innovation Program of Shanghai Municipal Education Commission (Grant No. 14ZZ046).

References

1 Alur R. Formal verification of hybrid systems. In: Proceedings of the International Conference on Embedded Software, New York, 2011. 273–278
2 Parrilo P A. Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization. Dissertation for Ph.D. Degree. Los Angeles: California Institute of Technology, 2000
3 Prajna S, Jadbabaie A, Pappas G J. A framework for worst-case and stochastic safety verification using barrier certificates. IEEE Trans Automat Contr, 2007, 52: 1415–1429
4 Kong H, He F, Song X, et al. Exponential-condition-based barrier certificate generation for safety verification of hybrid systems. In: Proceedings of the International Conference on Computer Aided Verification, Saint Petersburg, 2013. 8044: 242–257
5 Gulwani S, Tiwari A. Constraint-based approach for analysis of hybrid systems. In: Proceedings of the International Conference on Computer Aided Verification, Princeton, 2008. 5123: 190–203
6 Platzer A, Clarke E M. Computing differential invariants of hybrid systems as fixedpoints. Form Methods Syst Des, 2009, 35: 98–120
7 Sankaranarayanan S, Sipma H, Manna Z. Constructing invariants for hybrid systems. Form Methods Syst Des, 2008, 32: 25–55
8 Liu J, Zhan N, Zhao H, et al. Abstraction of elementary hybrid systems by variable transformation. In: Proceedings of the 20th International Symposium on Formal Methods, Norway, 2015. 9109: 360–377
9 Yang Z, Lin W, Wu M. Exact verification of hybrid systems based on bilinear SOS representation. ACM Trans Embed Comput Syst, 2015, 14: 1–19