



Synthesizing Invariant Barrier Certificates via Difference-of-Convex Programming

Qiuye Wang^{1,2}(✉) , Mingshuai Chen³(✉) , Bai Xue^{1,2}(✉) ,
Naijun Zhan^{1,2}(✉) , and Joost-Pieter Katoen³(✉) 

¹ SKLCS, Institute of Software, CAS, Beijing, China

² University of Chinese Academy of Sciences, Beijing, China
{wangqye,xuebai,znj}@ios.ac.cn

³ RWTH Aachen University, Aachen, Germany
{chenms,katoen}@cs.rwth-aachen.de



Abstract. A barrier certificate often serves as an inductive invariant that isolates an unsafe region from the reachable set of states, and hence is widely used in proving safety of hybrid systems possibly over the infinite time horizon. We present a novel condition on barrier certificates, termed the *invariant barrier-certificate condition*, that witnesses unbounded-time safety of differential dynamical systems. The proposed condition is by far the least conservative one on barrier certificates, and can be shown as the weakest possible one to attain inductive invariance. We show that discharging the invariant barrier-certificate condition—thereby synthesizing invariant barrier certificates—can be encoded as solving an *optimization problem subject to bilinear matrix inequalities* (BMIs). We further propose a synthesis algorithm based on difference-of-convex programming, which approaches a local optimum of the BMI problem via solving *a series of convex optimization problems*. This algorithm is incorporated in a branch-and-bound framework that searches for the global optimum in a divide-and-conquer fashion. We present a weak completeness result of our method, in the sense that a barrier certificate is guaranteed to be found (under some mild assumptions) whenever there exists an inductive invariant (in the form of a given template) that suffices to certify safety of the system. Experimental results on benchmark examples demonstrate the effectiveness and efficiency of our approach.

1 Introduction

Hybrid systems are mathematical models that capture the interaction between continuous physical dynamics and discrete switching behaviors, and hence are widely used in modelling cyber-physical systems (CPS). These CPS may be

This work has been partially funded by the NSFC under grant No. 61625206, 61732001, 61872341, and 61836005, by the ERC Advanced Project FRAPPANT under grant No. 787914, and by the CAS Pioneer Hundred Talents Program.

© The Author(s) 2021

A. Silva and K. R. M. Leino (Eds.) CAV 2021, LNCS 12759, pp. 443–466, 2021.

https://doi.org/10.1007/978-3-030-81685-8_21

complex and safety-critical, with sensitive variables of the environment in its sphere of control. Everyday examples include process control at all scales, ranging from household appliances to nuclear power plants, or embedded systems in transportation domain, such as autonomous driving maneuvers in automotive, aircraft collision-avoidance protocols in avionics, or automatic train control applications, as well as a broad range of devices in health technologies, such as cardiac pacemakers.

The safety-critical feature of these CPS, with increasingly complex behaviors, has initiated automatic safety or, dually, reachability verification of hybrid systems [1, 15]. The problem of reachability verification is undecidable in general [1], albeit with decidable families of sub-classes (see, e.g., [2, 16–18, 31]) identified in the literature. The hard core of the verification problem lies in reasoning about the continuous dynamics, which are often characterized by ordinary differential equations (ODEs). In particular, when nonlinearity arises in the ODEs, the explicit computation of the exact reachable set is usually intractable even for purely continuous dynamics [49].

Therefore in the literature, a plethora of approximation schemes, as surveyed in [15], for reachability analysis of hybrid systems has been developed, including an invariant-style reasoning scheme known as *barrier certificate* [41]. A barrier certificate often serves as an inductive invariant that isolates an unsafe region from the reachable set, thereby witnessing safety of hybrid systems possibly over the infinite time horizon. A common way to synthesize barrier certificates is to reduce the condition defining barrier certificates to a numerical optimization or constraint solving problem. There is, however, a trade-off between the expressiveness of the barrier-certificate condition and the efficiency in discharging the reduced constraints. Hence, to enable efficient algorithmic synthesis of barrier certificates via, e.g., linear programming (LP), second-order cone programming (SOCP), semidefinite programming (SDP) and interval analysis [11, 30], the general condition on inductive invariance (that a barrier certificate defines an invariant, see [8, 51]) has been strengthened into a spectrum of different shapes, e.g., [8, 29, 51, 60, 62]. It has been, nevertheless, a long-standing challenge to *find a barrier-certificate condition that is as weak as possible while admitting efficient synthesis algorithms*.

In this paper, we present a new condition on barrier certificates, termed the *invariant barrier-certificate condition*, based on the sufficient and necessary condition on being an inductive invariant [36]. Our invariant barrier-certificate condition is by far, to the best of our knowledge, the least conservative one on barrier certificates, and can be shown as the weakest possible one to attain inductive invariance. We show, by leveraging Putinar’s Positivstellensatz [32], that discharging the invariant barrier-certificate condition —thereby synthesizing invariant barrier certificates— can be encoded as solving an optimization problem subject to *bilinear matrix inequalities* (BMIs). We further show that general bilinear matrix-valued functions can be decomposed as a difference of two psd-convex (extension of convexity to matrix-valued functions) functions using eigendecomposition, thus resulting in a synthesis algorithm as per *difference-of-convex programming* (DCP) [33, 52], which solves a series of convex sub-problems (in the form of *linear matrix inequalities* (LMIs)) that approaches (arbitrarily

close to) a local optimum of the BMI problem. This algorithm is incorporated in a branch-and-bound framework that searches for the global optimum in a divide-and-conquer fashion. We present a weak completeness result of our method, in the sense that a barrier certificate is guaranteed to be found (under some mild assumptions) whenever there exists an inductive invariant (in the form of a given template) that suffices to certify the system’s safety. A similar result on completeness is previously provided only by symbolic approaches, yet to the best of our knowledge, not by methods base on numerical constraint solving, e.g., [4, 60, 61]. Experiments on a collection of examples suggested that our invariant barrier-certificate condition recognizes more barrier certificates than existing conditions, and that our DCP-based algorithm is more efficient than directly solving the BMIs via off-the-shelf solvers.

Due to space restrictions, proofs and benchmark details have been omitted; they are found in an extended version of this paper [57].

2 A Bird’s-Eye Perspective

We use the following example to give a bird’s-eye view of our approach.

Example 1 (overview [11]). Consider the following continuous-time dynamical system modelled by an ordinary differential equation:

$$\dot{\mathbf{x}} = \begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ x_1x_2 - 0.5x_2^2 + 0.1 \end{pmatrix}.$$

The verification obligation is to show that the system trajectory originating from any state in the initial set $\mathcal{X}_0 = \{\mathbf{x} \mid \mathcal{I}(\mathbf{x}) \leq 0\}$ with $\mathcal{I}(\mathbf{x}) = x_1^2 + (x_2 - 2)^2 - 1$ will never enter the unsafe set $\mathcal{X}_u = \{\mathbf{x} \mid \mathcal{U}(\mathbf{x}) \leq 0\}$ with $\mathcal{U}(\mathbf{x}) = x_2 + 1$. \triangleleft

A barrier certificate satisfying our condition in Definition 4 serves as an inductive invariant that suffices to isolate the unsafe region \mathcal{X}_u from the set of reachable states from \mathcal{X}_0 , thereby proving safety of the system over the infinite time horizon. To this end, we proceed in the following steps.

1) Encode as Sum-of-Squares (SOS) Constraints. We set a (polynomial) barrier-certificate template $B(\mathbf{a}, \mathbf{x}) = ax_2$ with unknown coefficient $a \in \mathbb{R}$. According to Theorem 1, we only need to consider Lie derivatives up to order $N_{B,f} = 1$, i.e., $\mathcal{L}_f^0 B(\mathbf{a}, \mathbf{x}) = ax_2$ and $\mathcal{L}_f^1 B(\mathbf{a}, \mathbf{x}) = a(x_1x_2 - 0.5x_2^2 + 0.1)$.

By Theorem 5, $B(\mathbf{a}, \mathbf{x})$ is an invariant barrier certificate if there exists a polynomial $v(\mathbf{x})$, SOS polynomials $\sigma(\mathbf{x}), \sigma'(\mathbf{x})$ and a constant $\epsilon > 0$ such that

$$-\underbrace{ax_2}_B + \sigma(\mathbf{x}) \underbrace{(x_1^2 + (x_2 - 2)^2 - 1)}_{\mathcal{I}}, \tag{1.1, initial}$$

$$-a \underbrace{(x_1x_2 - 0.5x_2^2 + 0.1)}_{\mathcal{L}_f^1 B} + v(\mathbf{x}) \underbrace{ax_2}_{\mathcal{L}_f^0 B}, \tag{1.2, Lieconsecution}$$

$$\underbrace{ax_2}_B + \sigma'(\mathbf{x}) \underbrace{(x_2 + 1)}_{\mathcal{U}} - \epsilon \tag{1.3, separation}$$

are SOS polynomials. We set $\epsilon = 0.01$ in this example.

2) Reduce to a BMI Optimization Problem. Observe that the above SOS constraints can be formulated as BMI constraints. For instance, let us assume that (1.2) is an SOS polynomial of degree at most 2 and $v(\mathbf{s}, \mathbf{x}) = s_0 + s_1x_1 + s_2x_2$ is a template polynomial with unknown coefficients \mathbf{s} . Then constraint (1.2) is equivalent to the BMI constraint

$$\mathcal{F}_2(\mathbf{a}, \mathbf{s}) = - \begin{pmatrix} -0.1a & 0 & 0.5as_0 \\ 0 & 0 & 0.5(as_1 - a) \\ 0.5as_0 & 0.5(as_1 - a) & as_2 + 0.5a \end{pmatrix} \preceq 0$$

meaning that the bilinear matrix (LHS of \preceq) is negative semidefinite. Note that the bilinearity arises due to the coupling of the unknown coefficients \mathbf{a} and \mathbf{s} .

Constraints (1.1) and (1.3) can be reduced to BMI constraints in an analogous way¹, yielding \mathcal{F}_1 and \mathcal{F}_3 . It then follows that, to solve the SOS constraints, we need to find a feasible solution (\mathbf{a}, \mathbf{s}) such that²

$$\mathcal{F}_1(\mathbf{a}, \mathbf{s}) \preceq 0 \wedge \mathcal{F}_2(\mathbf{a}, \mathbf{s}) \preceq 0 \wedge \mathcal{F}_3(\mathbf{a}, \mathbf{s}) \preceq 0. \tag{2}$$

To exploit well-developed optimization techniques, the feasibility problem (2) is transformed to an optimization problem subject to BMI constraints:

$$\begin{aligned} & \underset{\lambda, \mathbf{a}, \mathbf{s}}{\text{maximize}} && \lambda \\ & \text{subject to} && \mathcal{B}_i(\lambda, \mathbf{a}, \mathbf{s}) \hat{=} \mathcal{F}_i(\mathbf{a}, \mathbf{s}) + \lambda I \preceq 0, \quad i = 1, 2, 3 \end{aligned} \tag{3}$$

where I is the identity matrix with compatible dimensions. Note that problem (2) has a feasible solution if and only if the optimal value λ^* in (3) is non-negative.

3) Decompose as Difference-of-Convex Problems. The problem (3) contains non-convex constraints and hence does not admit efficient (polynomial-time) algorithms tailored for convex optimizations. However, by our technique presented in Sect. 5, a non-convex function $\mathcal{B}_i(\lambda, \mathbf{a}, \mathbf{s})$ can be decomposed as the difference of two psd-convex (defined later) matrix-valued functions:

$$\mathcal{B}_i(\lambda, \mathbf{a}, \mathbf{s}) = \mathcal{B}_i^+(\lambda, \mathbf{a}, \mathbf{s}) - \mathcal{B}_i^-(\lambda, \mathbf{a}, \mathbf{s}). \tag{4}$$

The decomposition of $\mathcal{B}_2(\lambda, \mathbf{a}, \mathbf{s})$, for instance, gives

$$\begin{aligned} \mathcal{B}_2^+(\lambda, \mathbf{a}, \mathbf{s}) &= \\ \frac{1}{8} & \begin{pmatrix} 8\lambda + 0.08a + a^2 + 0.408s_0^2 & 0.408s_0s_1 & -2as_0 + 0.816s_0s_2 \\ 0.408s_0s_1 & 8\lambda + a^2 + 0.408s_1^2 & 4a - 2as_1 + 0.816s_1s_2 \\ -2as_0 + 0.816s_0s_2 & 4a - 2as_1 + 0.816s_1s_2 & 8\lambda - 4a + 2.449a^2 - 4as_2 + s_0^2 + s_1^2 + 1.632s_2^2 \end{pmatrix} \\ \mathcal{B}_2^-(\lambda, \mathbf{a}, \mathbf{s}) &= \\ \frac{1}{8} & \begin{pmatrix} a^2 + 0.408s_0^2 & 0.408s_0s_1 & 2as_0 + 0.816s_0s_2 \\ 0.408s_0s_1 & a^2 + 0.408s_1^2 & 2as_1 + 0.816s_1s_2 \\ 2as_0 + 0.816s_0s_2 & 2as_1 + 0.816s_1s_2 & 2.449a^2 + 4as_2 + s_0^2 + s_1^2 + 1.632s_2^2 \end{pmatrix}. \end{aligned}$$

¹ Despite that no bilinearity is involved in constraints (1.1) and (1.3), they can be processed in the same way as (1.2), yielding LMI constraints.

² Extra constraints on $\sigma(\mathbf{x})$ and $\sigma'(\mathbf{x})$ being SOS polynomials can be encoded analogously in the feasibility problem, yet are omitted here for the sake of simplicity.

4) Solve a Series of Convex Sub-problems. Now, we apply a standard iterative procedure in difference-of-convex programming [10] as follows. Given a feasible solution $\mathbf{z}^k = (\lambda^k, \mathbf{a}^k, \mathbf{s}^k)$ to the BMI optimization problem (3), the concave part $-\mathcal{B}_i^-(\lambda, \mathbf{a}, \mathbf{s})$ in (4) is linearized around \mathbf{z}^k , thus yielding a series of convex programs ($k = 0, 1, \dots$):

$$\begin{aligned} & \underset{\lambda, \mathbf{a}, \mathbf{s}}{\text{maximize}} && \lambda \\ & \text{subject to} && \mathcal{B}_i^+(\mathbf{z}) - \mathcal{B}_i^-(\mathbf{z}^k) - \mathcal{D}\mathcal{B}_i^-(\mathbf{z}^k)(\mathbf{z} - \mathbf{z}^k) \leq 0, \quad i = 1, 2, 3 \end{aligned} \quad (5)$$

where $\mathcal{D}\mathcal{B}_i^-$ denotes the derivative of the matrix-valued function \mathcal{B}_i^- .

The soundness of our approach asserts that the feasible set of the linearized program (5) under-approximates the feasible set of the original BMI program (3). Therefore, if $\lambda^k \geq 0$ after iteration k , we can safely claim that $(\mathbf{a}^k, \mathbf{s}^k)$ is a feasible solution to (2). A barrier certificate $B(\mathbf{x})$ is then obtained by substituting \mathbf{a}^k in $B(\mathbf{a}, \mathbf{x})$. Moreover, if we take the optimum $\mathbf{z}^{*,k}$ of (5) to be the next linearization point \mathbf{z}^{k+1} , the solution sequence $\{\mathbf{z}^k\}_{k \in \mathbb{N}}$ converges to a local optimum of (3).

We show that the linearized program (5) is equivalent to an LMI optimization problem admitting polynomial-time algorithms, say the well-known *interior-point methods* supported by most off-the-shelf SDP solvers. Our iterative procedure starts with a strictly feasible initial solution \mathbf{z}^0 to program (3) and terminates with $\lambda^2 \geq 0$ (subject to numerical round-off) and $a^2 = -0.00363421$, yielding the barrier certificate

$$B(\mathbf{a}^2, \mathbf{x}) = -0.00363421x_2 \leq 0.$$

Figure 1 depicts the system dynamics and the synthesized barrier certificate.

We remark that the aforementioned iterative procedure on solving a series of convex optimizations converges only to a local optimum of the BMI problem (3). This means that, in some cases, it may miss the global optimum that induces a non-negative λ^* . We will present in Sect. 6 a solution to this problem by incorporating our iterative procedure into a branch-and-bound framework that searches for the global optimum in a divide-and-conquer fashion.

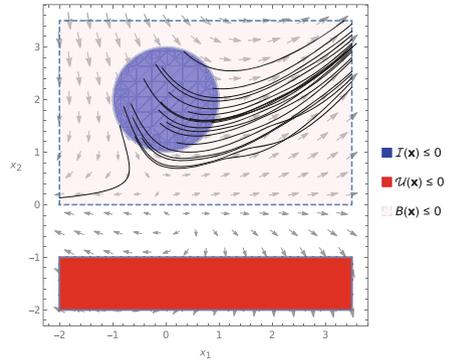


Fig. 1. Phase portrait of the system in Example 1. The arrows indicate the vector field and the solid curves are randomly sampled trajectories.

3 Mathematical Foundations

Notations. Let $\mathbb{N}, \mathbb{N}^+, \mathbb{R}, \mathbb{R}^+$ and \mathbb{R}_0^+ be respectively the set of natural, positive natural, real, positive real and non-negative real numbers. For a vector $\mathbf{x} \in \mathbb{R}^n$, x_i refers to its i -th component and $\|\mathbf{x}\|$ denotes the ℓ^2 -norm; for a matrix $A \in$

$\mathbb{R}^{n \times m}$, $A(i, j)$ refers to its (i, j) -th element. Let $\mathbb{R}[\mathbf{x}]$ be the polynomial ring in \mathbf{x} over the field \mathbb{R} . A polynomial $h \in \mathbb{R}[\mathbf{x}]$ is *sum-of-squares* (SOS) iff there exist polynomials $g_1, \dots, g_k \in \mathbb{R}[\mathbf{x}]$ such that $h = \sum_{i=1}^k g_i^2$. We denote by $\Sigma[\mathbf{x}] \subset \mathbb{R}[\mathbf{x}]$ the set of SOS polynomials over \mathbf{x} . \mathcal{S}^n denotes the space of $n \times n$ real, symmetric matrices. For $A \in \mathcal{S}^n$, $A \succeq 0$ means that A is *positive semidefinite* (psd, for short)³, i.e., $\forall \mathbf{x} \in \mathbb{R}^n: \mathbf{x}^\top A \mathbf{x} \geq 0$. A matrix-valued function $\mathcal{B}: \mathbb{R}^n \rightarrow \mathcal{S}^m$ is *psd-convex* on a convex set $\mathcal{C} \subseteq \mathbb{R}^n$ if $\forall \mathbf{x}_1, \mathbf{x}_2 \in \mathcal{C}, \forall \mu \in (0, 1): \mathcal{B}(\mu \mathbf{x}_1 + (1 - \mu) \mathbf{x}_2) \preceq \mu \mathcal{B}(\mathbf{x}_1) + (1 - \mu) \mathcal{B}(\mathbf{x}_2)$.

Differential Dynamical Systems. We consider a class of continuous dynamical systems modelled by ordinary differential equations of the autonomous type:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) \tag{6}$$

where $\mathbf{x} \in \mathbb{R}^n$ is the *state* vector, $\dot{\mathbf{x}}$ denotes its temporal derivative $d\mathbf{x}/dt$, with $t \in \mathbb{R}_0^+$ modelling time, and $\mathbf{f}: \mathbb{R}^n \rightarrow \mathbb{R}^n$ is a polynomial *flow field* (or *vector field*) that governs the evolution of the system. A polynomial vector field is local Lipschitz, and hence for some $T \in \mathbb{R}^+ \cup \{\infty\}$, there exists a unique *solution* (or *trajectory*) $\zeta_{\mathbf{x}_0}: [0, T) \rightarrow \mathbb{R}^n$ originating from any initial state $\mathbf{x}_0 \in \mathbb{R}^n$ such that (1) $\zeta_{\mathbf{x}_0}(0) = \mathbf{x}_0$, and (2) $\forall \tau \in [0, T): \frac{d\zeta_{\mathbf{x}_0}}{d\tau} \Big|_{t=\tau} = \mathbf{f}(\zeta_{\mathbf{x}_0}(\tau))$. We assume in the sequel that T is the maximal instant up to which $\zeta_{\mathbf{x}_0}$ exists for all \mathbf{x}_0 .

Remark 1. Our techniques on synthesizing barrier certificates in this paper focus on differential dynamics of the form (6). However, we foresee no substantial difficulties in extending the results to multi-mode hybrid systems where extra constraints on the system evolution, e.g., guards, are present.

Safety Verification Problem. Given a domain set $\mathcal{X} \subseteq \mathbb{R}^n$, an initial set $\mathcal{X}_0 \subseteq \mathcal{X}$ and an unsafe set $\mathcal{X}_u \subseteq \mathcal{X}$, the *reachable set* of a dynamical system of the form (6) at time instant $t \in [0, T)$ is defined as $\mathcal{R}_{\mathcal{X}_0}(t) \triangleq \{\zeta_{\mathbf{x}_0}(t) \mid \mathbf{x}_0 \in \mathcal{X}_0\}$. We denote by $\mathcal{R}_{\mathcal{X}_0}$ the aggregated reachable set, i.e., the union of $\mathcal{R}_{\mathcal{X}_0}(t)$ over $t \in [0, T)$ ⁴. The system is said to be *safe* iff $\mathcal{R}_{\mathcal{X}_0} \cap \mathcal{X}_u = \emptyset$, and *unsafe* otherwise. For simplicity, we consider $\mathcal{X} = \mathbb{R}^n$ throughout this paper.

To avoid the explicit computation of the exact reachable set, which is usually intractable for nonlinear hybrid systems (cf., e.g., [15]), barrier-certificate methods make use of a partial differential operator, termed the *Lie derivative*, to capture the evolution of a barrier function along the vector field:

Definition 1 (Lie Derivative [28]). Given a vector field $\mathbf{f}: \mathbb{R}^n \rightarrow \mathbb{R}^n$ over \mathbf{x} , the Lie derivative of a polynomial function $B(\mathbf{x})$ along \mathbf{f} , $\mathcal{L}_{\mathbf{f}}^k B: \mathbb{R}^n \rightarrow \mathbb{R}$ of order $k \in \mathbb{N}$, is

$$\mathcal{L}_{\mathbf{f}}^k B(\mathbf{x}) \triangleq \begin{cases} B(\mathbf{x}), & k = 0, \\ \left\langle \frac{\partial}{\partial \mathbf{x}} \mathcal{L}_{\mathbf{f}}^{k-1} B(\mathbf{x}), \mathbf{f}(\mathbf{x}) \right\rangle, & k > 0 \end{cases}$$

³ More generally, for $A, B \in \mathcal{S}^n$, $A \preceq B$ indicates that $B - A$ is positive semidefinite.

⁴ This subsumes the problem of unbounded-time safety verification where a unique solution exists over the infinite time horizon $[0, \infty)$.

where $\langle \cdot, \cdot \rangle$ is the inner product of vectors, i.e., $\langle \mathbf{u}, \mathbf{v} \rangle \hat{=} \sum_{i=1}^n u_i v_i$ for $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$.

The Lie derivative $\mathcal{L}_f^k B(\mathbf{x})$ is essentially the k -th temporal derivative of the (barrier) function $B(\mathbf{x})$, and thus captures the change of $B(\mathbf{x})$ over time.

An *inductive invariant* $\Psi \subseteq \mathbb{R}^n$ of a dynamical system is a set of states such that all the trajectories starting from within Ψ remain in Ψ :

Definition 2 (Inductive Invariant [40]). *Given a system (6), a set $\Psi \subseteq \mathbb{R}^n$ is an inductive invariant of system (6) if and only if*

$$\forall \mathbf{x}_0 \in \Psi. \forall t \in [0, T): \zeta_{\mathbf{x}_0}(t) \in \Psi. \quad (7)$$

In the sequel, we refer to inductive invariants simply as invariants. In [36], a sufficient and necessary condition on being a polynomial invariant is proposed:

Theorem 1 (Invariant condition [36]). *Given a polynomial $B \in \mathbb{R}[\mathbf{x}]$, its zero sub-level set $\{\mathbf{x} \mid B(\mathbf{x}) \leq 0\}$ is an invariant of system (6) if and only if⁵*

$$B \leq 0 \implies \bigvee_{i=0}^{N_{B,f}} \left(\left(\bigwedge_{j=0}^{i-1} \mathcal{L}_f^j B = 0 \right) \wedge \mathcal{L}_f^i B < 0 \right) \vee \bigwedge_{i=0}^{N_{B,f}} \mathcal{L}_f^i B = 0 \quad (8)$$

where $N_{B,f} \in \mathbb{N}^+$ is a completeness threshold, i.e., a finite positive integer that bounds the order of Lie derivatives, which can be computed using Gröbner bases⁶.

In contrast, a *barrier certificate* is a function whose zero sub-level set isolates an unsafe region \mathcal{X}_u from the reachable set $\mathcal{R}_{\mathcal{X}_0}$ w.r.t. some initial set \mathcal{X}_0 :

Definition 3 (Semantic Barrier Certificate [51]). *Given a system (6), an initial set \mathcal{X}_0 and an unsafe set \mathcal{X}_u , a barrier certificate of (6) is a differentiable function $B: \mathbb{R}^n \rightarrow \mathbb{R}$ satisfying*

$$\forall \mathbf{x}_0 \in \mathcal{X}_0. \forall t \in [0, T): B(\zeta_{\mathbf{x}_0}(t)) \leq 0 \quad \text{and} \quad \forall \mathbf{x} \in \mathcal{X}_u: B(\mathbf{x}) > 0. \quad (9)$$

The existence of such a barrier certificate trivially implies safety of the system. Moreover, one may readily verify that if some set $\Psi = \{\mathbf{x} \mid B(\mathbf{x}) \leq 0\}$ is an invariant and satisfies $(\mathcal{X}_0 \subseteq \Psi) \wedge (\Psi \cap \mathcal{X}_u = \emptyset)$, then $B(\mathbf{x})$ is a barrier certificate.

As observed in [51], however, the semantic statement in Definition 3 encodes merely the general *principle of barrier certificates* [8], yet in itself is not that useful for safety verification because it explicitly involves the system solutions. Therefore, in order to enable efficient synthesis, the semantic condition on barrier certificates has been strengthened into a handful of different shapes (see, e.g., [8, 29, 41, 60], which all imply inductive invariance). It has been yet a long-standing challenge to find a barrier-certificate condition that is as weak as possible while admitting efficient synthesis algorithms.

Our BMI encoding of the invariant barrier-certificate condition (cf. Sect. 4) roots in Putinar's Positivstellensatz, which characterizes positivity of polynomials on a semi-algebraic set defined by a system of polynomial inequalities:

⁵ In (8), $\bigwedge_{j=0}^{i-1} \mathcal{L}_f^j B = 0$ is true for $i = 0$ by default. This applies in the sequel.

⁶ $N_{B,f}$ is the minimal i such that $\mathcal{L}_f^{i+1} B$ is in the polynomial ideal generated by $\mathcal{L}_f^0 B, \mathcal{L}_f^1 B, \dots, \mathcal{L}_f^i B$. The ideal membership can be decided via Gröbner basis.

Theorem 2 (Putinar’s Positivstellensatz [32]). *Let $\mathcal{K} = \{\mathbf{x} \mid \bigwedge_{i=1}^m g_i(\mathbf{x}) \geq 0\}$ be a compact semi-algebraic set defined by $g_1, \dots, g_m \in \mathbb{R}[\mathbf{x}]$. Assume the Archimedean condition holds⁷, i.e., there exists $L \in \mathbb{R}^+$ such that $L - \|\mathbf{x}\|^2 = \sigma_0(\mathbf{x}) + \sum_{i=1}^m \sigma_i(\mathbf{x})g_i(\mathbf{x})$ for some $\sigma_0, \dots, \sigma_m \in \Sigma[\mathbf{x}]$. If $h \in \mathbb{R}[\mathbf{x}]$ is strictly positive on \mathcal{K} , then*

$$h(\mathbf{x}) = \sigma_0(\mathbf{x}) + \sum_{i=1}^m \sigma_i(\mathbf{x})g_i(\mathbf{x})$$

holds for some SOS polynomials $\sigma_0, \dots, \sigma_m \in \Sigma[\mathbf{x}]$.

We now recall a key technique used in our reduction to semidefinite optimizations. Given a symmetric matrix $X \in \mathcal{S}^n$ partitioned as $X = \begin{pmatrix} A & C \\ C^\top & D \end{pmatrix}$ with invertible A , the Schur complement of A in X is defined as $X/A \hat{=} D - C^\top A^{-1}C$. An important property of the Schur complement X/A is that it characterizes the positive semidefiniteness of the block matrix X :

Theorem 3 (Schur Complement [3]). *If $A \succ 0$, then $X \succeq 0$ iff $X/A \succeq 0$.*

We apply the Schur complement in Sect. 5 to transform nonlinear convex constraints into linear constraints.

4 Invariant Barrier-Certificate Condition as BMIs

In this section, we present our *invariant barrier-certificate condition* (see Definition 4) based on the necessary and sufficient condition on being an inductive invariant (cf. Theorem 1), and show how to encode it as BMI constraints.

4.1 Invariant Barrier-Certificate Condition

Definition 4 (Invariant Barrier Certificate). *Given a system (6), an initial set \mathcal{X}_0 and an unsafe set \mathcal{X}_u , a polynomial function $B: \mathbb{R}^n \rightarrow \mathbb{R}$ is an invariant barrier certificate of system (6) if and only if*

1. (initial): $\forall \mathbf{x} \in \mathcal{X}_0: B(\mathbf{x}) \leq 0$;
2. (consecution): $\forall \mathbf{x} \in \mathbb{R}^n: \bigwedge_{i=1}^{N_{B,f}} \left(\left(\bigwedge_{j=0}^{i-1} \mathcal{L}_f^j B(\mathbf{x}) = 0 \right) \implies \mathcal{L}_f^i B(\mathbf{x}) \leq 0 \right)$;
3. (separation): $\forall \mathbf{x} \in \mathcal{X}_u: B(\mathbf{x}) > 0$.

Notice that the consecution constraint in Definition 4 involves Lie derivatives of orders up to $N_{B,f} \in \mathbb{N}^+$, as is the case in Theorem 1. Our invariant barrier-certificate condition hence generalizes existing conditions on barrier certificates, e.g., [4, 60, 63], which consider Lie derivatives only up to the first order.

The consecution condition in Definition 4 is in fact equivalent to the invariant condition (8) in Theorem 1 (cf. [57, Lemma 2]), thereby revealing the relation between an inductive invariant and an invariant barrier certificate:

⁷ This condition can be met by adding a (redundant) constraint $g_{m+1}(\mathbf{x}) = L_0 - \|\mathbf{x}\|^2 \leq 0$, provided that a bound $L_0 \in \mathbb{R}^+$ is known such that $\forall \mathbf{x} \in \mathcal{K}: L_0 - \|\mathbf{x}\|^2 \geq 0$.

Theorem 4 (Inductive Invariance). *Given a system (6), an initial set \mathcal{X}_0 and an unsafe set \mathcal{X}_u . If $B(\mathbf{x})$ is an invariant barrier certificate, then $\Psi = \{\mathbf{x} \mid B(\mathbf{x}) \leq 0\}$ is an invariant. Conversely, if $\Psi = \{\mathbf{x} \mid B(\mathbf{x}) \leq 0\}$ is an invariant satisfying $\mathcal{X}_0 \subseteq \Psi$ and $\Psi \cap \mathcal{X}_u = \emptyset$, then $B(\mathbf{x})$ is an invariant barrier certificate.*

It follows from Theorem 4 that our invariant barrier-certificate condition is the least conservative one on barrier certificates to attain inductive invariance.

Remark 2. We do not employ the invariant condition (8) in Theorem 1 as the constraint on the consecution of Lie derivatives. This is because our consecution condition in Definition 4 is simpler, and in particular, amenable to more straightforward transformations to SOS constraints via Putinar’s Positivstellensatz, as shown later in Subsect. 4.2.

Remark 3. For a fixed $0 < \mathfrak{N} < N_{B,f}$, the consecution condition in Definition 4 can be strengthened in the following way while preserving inductive invariance:

$$\forall \mathbf{x} \in \mathbb{R}^n : \bigwedge_{i=1}^{\mathfrak{N}-1} \left(\left(\bigwedge_{j=0}^{i-1} \mathcal{L}_f^j B(\mathbf{x}) = 0 \right) \implies \mathcal{L}_f^i B(\mathbf{x}) \leq 0 \right) \wedge \\ \left(\left(\bigwedge_{j=0}^{\mathfrak{N}-1} \mathcal{L}_f^j B(\mathbf{x}) = 0 \right) \implies \mathcal{L}_f^{\mathfrak{N}} B(\mathbf{x}) < 0 \right)$$

where for the \mathfrak{N} -th Lie derivative, one needs $\mathcal{L}_f^{\mathfrak{N}} B(\mathbf{x}) < 0$ (rather than $\mathcal{L}_f^{\mathfrak{N}} B(\mathbf{x}) \leq 0$). In practice, using such a strengthened consecution condition —with less sub-constraints to solve— may yield more efficient synthesis.

4.2 Encoding as BMI Optimizations

Next, we show how to encode synthesizing an invariant barrier certificate (cf. Definition 4) as an optimization problem subject to BMIs. To this end, we first recast the invariant barrier-certificate condition into a collection of SOS constraints⁸.

Theorem 5 (Sufficient Condition for Invariant Barrier Certificate).

Given a system (6), an initial set $\mathcal{X}_0 = \{\mathbf{x} \mid \mathcal{I}(\mathbf{x}) \leq 0\}$ and an unsafe set $\mathcal{X}_u = \{\mathbf{x} \mid \mathcal{U}(\mathbf{x}) \leq 0\}$. A polynomial $B \in \mathbb{R}[\mathbf{x}]$ is an invariant barrier certificate of (6) if for some $\epsilon \in \mathbb{R}^+$, there exist $v_{i,j} \in \mathbb{R}[\mathbf{x}]$ and SOS polynomials $\sigma(\mathbf{x}), \sigma'(\mathbf{x})$ s.t.

1. $-B(\mathbf{x}) + \sigma(\mathbf{x})\mathcal{I}(\mathbf{x})$,
2. for all $1 \leq i \leq N_{B,f}$, $-\mathcal{L}_f^i B(\mathbf{x}) + \sum_{j=0}^{i-1} v_{i,j}(\mathbf{x})\mathcal{L}_f^j B(\mathbf{x})$,
3. $B(\mathbf{x}) + \sigma'(\mathbf{x})\mathcal{U}(\mathbf{x}) - \epsilon$

are SOS polynomials.

By enforcing the Archimedean condition and applying Putinar’s Positivstellensatz, we further derive a necessary condition of invariant barrier certificate:

⁸ For simplicity, we assume that \mathcal{X}_0 and \mathcal{X}_u are both captured by a single polynomial. Our formulations, however, apply also to cases with basic semi-algebraic \mathcal{X}_0 or \mathcal{X}_u .

Theorem 6 (Necessary Condition for Invariant Barrier Certificate).

Given a system (6), an initial set $\mathcal{X}_0 = \{\mathbf{x} \mid \mathcal{I}(\mathbf{x}) \leq 0\}$ and an unsafe set $\mathcal{X}_u = \{\mathbf{x} \mid \mathcal{U}(\mathbf{x}) \leq 0\}$. If $B \in \mathbb{R}[\mathbf{x}]$ is an invariant barrier certificate of (6), then for some $\epsilon \in \mathbb{R}^+$, there exist $v_{i,j} \in \mathbb{R}[\mathbf{x}]$ and SOS polynomials $\sigma(\mathbf{x}), \sigma'(\mathbf{x}), \rho(\mathbf{x}), \rho'(\mathbf{x}), \rho_i''(\mathbf{x})$ s.t. for any $L \in \mathbb{R}^+$,

1. $-B(\mathbf{x}) + \rho(\mathbf{x})(\|\mathbf{x}\|^2 - L) + \sigma(\mathbf{x})\mathcal{I}(\mathbf{x}) + \epsilon,$
2. for all $1 \leq i \leq N_{B,f}, -\mathcal{L}_f^i B(\mathbf{x}) + \rho_i''(\mathbf{x})(\|\mathbf{x}\|^2 - L) + \sum_{j=0}^{i-1} v_{i,j}(\mathbf{x})\mathcal{L}_f^j B(\mathbf{x}) + \epsilon,$
3. $B(\mathbf{x}) + \rho'(\mathbf{x})(\|\mathbf{x}\|^2 - L) + \sigma'(\mathbf{x})\mathcal{U}(\mathbf{x})$

are SOS polynomials.

Notice that a polynomial $B(\mathbf{x})$ satisfying the sufficient condition in Theorem 5 suffices as an invariant barrier certificate that witnesses safety of the system. In contrast, a polynomial $B(\mathbf{x})$ satisfying the necessary condition in Theorem 6 may serve as a candidate invariant barrier certificate, and safety of the system can be concluded via a posterior check⁹ of $B(\mathbf{x})$ per Definition 4.

Next we show how to encode an SOS constraint of the shape “ $h(\mathbf{x}) \in \Sigma[\mathbf{x}]$ ” in Theorems 5 and 6 as a BMI constraint. To this end, we first set a *template polynomial*¹⁰ $B(\mathbf{a}, \mathbf{x})$ parameterized by unknown real coefficients \mathbf{a} as the barrier certificate. We then proceed by setting templates for the remaining unknown polynomials (e.g., $v_{i,j}(\mathbf{x})$) and SOS polynomials (e.g., $\sigma(\mathbf{x})$ and $\rho(\mathbf{x})$) in $h(\mathbf{x})$, with all the parameters in these templates grouped into \mathbf{s} . Observe that the parameterized SOS polynomial $h(\mathbf{a}, \mathbf{s}, \mathbf{x})$ is of a bilinear form on the parameter spaces, i.e., $h(\mathbf{a}, \mathbf{s}, \mathbf{x})$ is linear in \mathbf{a} and \mathbf{s} separately. However, nonlinearity arises in the combined parameter space (\mathbf{a}, \mathbf{s}) due to the product couplings of \mathbf{a} and \mathbf{s} , i.e., $v_{i,j}(\mathbf{s}_{i,j}, \mathbf{x})\mathcal{L}_f^j B(\mathbf{a}, \mathbf{x})$ in the consecution constraint.

Now the problem of synthesizing an invariant barrier certificate boils down to searching for an instantiation of the parameters \mathbf{a} and \mathbf{s} such that the sufficient condition in Theorem 5 holds (or alternatively, the necessary condition in Theorem 6 holds and the posterior check passed). Such an instantiation of \mathbf{a} (making $B(\mathbf{a}, \mathbf{x})$ an invariant barrier certificate) will be called *valid* in the sequel.

Suppose that a parameterized SOS polynomial $h(\mathbf{a}, \mathbf{s}, \mathbf{x})$ is of degree at most $2d$, with user-specified $d \in \mathbb{N}$. Then $h(\mathbf{a}, \mathbf{s}, \mathbf{x})$ can always be written in *quadratic form* as $h(\mathbf{a}, \mathbf{s}, \mathbf{x}) = \mathbf{b}^\top Q(\mathbf{a}, \mathbf{s})\mathbf{b}$, where $\mathbf{b} = (1, x_1, x_2, x_1x_2, \dots, x_n^d)$ is the *basis vector* of size $p = \binom{n+d}{n}$ containing all monomials of degree up to d , and $Q(\mathbf{a}, \mathbf{s}) \in \mathcal{S}^p$ is a parameterized real symmetric matrix known as the *Gram matrix* [6]¹¹. An important fact states that $h(\mathbf{a}, \mathbf{s}, \mathbf{x})$ is SOS if and only if $Q(\mathbf{a}, \mathbf{s}) \succeq 0$.

Let $\mathcal{F}(\mathbf{a}, \mathbf{s}) = -Q(\mathbf{a}, \mathbf{s})$. As per $h(\mathbf{a}, \mathbf{s}, \mathbf{x})$, the matrix-valued function $\mathcal{F}(\mathbf{a}, \mathbf{s})$ is bilinear in (\mathbf{a}, \mathbf{s}) . Observe that $h(\mathbf{a}, \mathbf{s}, \mathbf{x})$ is SOS if and only if the BMI constraint $\mathcal{F}(\mathbf{a}, \mathbf{s}) \preceq 0$ holds. See Example 1 for an illustration of this BMI encoding.

⁹ Such a check inherits decidability of the first-order theory of real-closed fields [53].

¹⁰ A template polynomial $g(\mathbf{a}, \mathbf{x})$ is required to be linear in its parameters \mathbf{a} .

¹¹ Extracting the Gram matrix amounts to solving a system of linear equations resulting from coefficient matching. The derived Gram matrix may contain extra unknowns if the system of linear equations admits multiple solutions, which nevertheless can be encoded in our subsequent workflow by enumerating the basis of its null space.

In general, $\mathcal{F}(\mathbf{a}, \mathbf{s})$ can be flattened in an expanded bilinear form as

$$\mathcal{F}(\mathbf{a}, \mathbf{s}) = F + \sum_{i=1}^m a_i H_i + \sum_{j=1}^n s_j G_j + \sum_{i=1}^m \sum_{j=1}^n a_i s_j F_{i,j}$$

where m and n are the size of \mathbf{a} and \mathbf{s} , respectively; $F, H_i, G_j, F_{i,j} \in \mathcal{S}^p$ are constant matrices. Discharging the conditions of invariant barrier certificates hence amounts to solving the BMI feasibility problem of finding \mathbf{a} and \mathbf{s} s.t.

$$\mathcal{F}_\iota(\mathbf{a}, \mathbf{s}) \preceq 0, \quad \iota = 1, 2, \dots, l. \quad (10)$$

Here $\mathcal{F}(\mathbf{a}, \mathbf{s})$ is indexed by ι and l is the number of SOS constraints involved.

To exploit well-developed techniques in optimization, the feasibility problem (10) is transformed to an optimization problem subject to BMI constraints:

$$\begin{aligned} & \underset{\lambda, \mathbf{a}, \mathbf{s}}{\text{maximize}} && \lambda \\ & \text{subject to} && \mathcal{F}_\iota(\mathbf{a}, \mathbf{s}) + \lambda I \preceq 0, \quad \iota = 1, 2, \dots, l. \end{aligned} \quad (11)$$

A solution $(\lambda, \mathbf{a}, \mathbf{s})$ to (11) is *feasible* if it satisfies the BMIs in (11), and *strictly feasible* if all the BMIs are satisfied with strict inequalities. We sometimes drop the λ component in the solution when it is clear from the context. Notice that *problem (10) has a feasible solution if and only if the optimal value λ^* in the BMI optimization problem (11) is non-negative.*

To achieve (weak) completeness of our method in subsequent sections on solving the BMI optimization problem, we make the following assumption on the boundedness of the search space (\mathbf{a}, \mathbf{s}) of the optimization.

Assumption 1 (Boundedness on the Parameters). *Every feasible solution (\mathbf{a}, \mathbf{s}) to the BMI problem (11) is in a compact set with non-empty interior, i.e.,*

$$(\mathbf{a}, \mathbf{s}) \in \mathcal{C}_{\mathbf{a}} \times \mathcal{C}_{\mathbf{s}} = \left\{ (\mathbf{a}, \mathbf{s}) \mid \|\mathbf{a}\|^2 \leq L_{\mathbf{a}}, \|\mathbf{s}\|^2 \leq L_{\mathbf{s}} \right\}$$

for some known bounds $L_{\mathbf{a}}, L_{\mathbf{s}} \in \mathbb{R}^+$.

Remark 4. The boundedness on \mathbf{a} in Assumption 1 makes sense in practice since we usually prefer barrier certificates with bounded coefficients. Moreover, when the bilinear functions $\mathcal{F}_\iota(\mathbf{a}, \mathbf{s})$ in (11) are affine in \mathbf{a} and \mathbf{s} , i.e., with a zero constant matrix F , the parameters \mathbf{a} and \mathbf{s} can be scaled independently by any positive factor. Therefore in this case, w.l.o.g, one may simply set $L_{\mathbf{a}} = L_{\mathbf{s}} = 1$.

5 Solving BMI Optimizations via DCP

The BMI optimization problem (11), derived from the synthesis problem, is known to be NP-hard and contains non-convex constraints [55], and hence is not amenable to efficient (polynomial-time) algorithms committed to solving convex optimizations. In this section, we present an algorithm for solving general BMI

optimizations via difference-of-convex programming [33, 52], which solves a series of convex sub-problems that approaches a local optimum of (11).

For brevity, we consider optimization problems with a single BMI constraint¹²:

$$\begin{aligned} & \underset{\mathbf{z}=(\mathbf{x}, \mathbf{y})}{\text{maximize}} && g(\mathbf{z}) \\ & \text{subject to} && \mathcal{B}(\mathbf{x}, \mathbf{y}) \hat{=} F + \sum_{i=1}^m x_i H_i + \sum_{j=1}^n y_j G_j + \sum_{i=1}^m \sum_{j=1}^n x_i y_j F_{i,j} \preceq 0 \end{aligned} \quad (12)$$

where the objective function $g: \mathbb{R}^{m+n} \rightarrow \mathbb{R}$ is linear in $\mathbf{z} = (\mathbf{x}, \mathbf{y})$; $F, H_i, G_j, F_{i,j} \in \mathcal{S}^p$ are constant symmetric matrices.

5.1 Difference-of-Convex Decomposition

The key challenge in solving the BMI problem (12) is its non-convexity, that is, the matrix-valued function $\mathcal{B}(\mathbf{x}, \mathbf{y})$ is, in general, not psd-convex.

There have been attempts, most pertinently in [10], to decompose a bilinear function as a difference between two psd-convex functions, known as the *difference-of-convex* (DC) *decomposition*, such that the optimization in its decomposed form enjoys well-established techniques in difference-of-convex programming [33, 52]. The DC decomposition in [10], however, is confined to BMIs of a specific structure, namely, $X^\top Y + Y^\top X \preceq 0$, where X and Y are matrix variables containing variables x_i and y_j , respectively. The more general bilinear function $\mathcal{B}(\mathbf{x}, \mathbf{y})$ in (12) does unfortunately not admit straightforward forms of decomposition such as those in [10, Lemma 3.1].

In what follows, we present a difference-of-convex decomposition of the matrix-valued function $\mathcal{B}(\mathbf{x}, \mathbf{y})$, inspired by [58], using eigendecomposition.

First, observe that the function $\mathcal{B}(\mathbf{x}, \mathbf{y})$ can be written as

$$\mathcal{B}(\mathbf{x}, \mathbf{y}) = \begin{pmatrix} \mathbf{x} \otimes I \\ \mathbf{y} \otimes I \end{pmatrix}^\top \begin{pmatrix} 0 & \Gamma \\ \Gamma^\top & 0 \end{pmatrix} \begin{pmatrix} \mathbf{x} \otimes I \\ \mathbf{y} \otimes I \end{pmatrix} + (\Omega_1 \ \Omega_2) \begin{pmatrix} \mathbf{x} \otimes I \\ \mathbf{y} \otimes I \end{pmatrix} + F \quad (13)$$

where \otimes denotes the Kronecker product: for two matrices $A \in \mathbb{R}^{a \times b}$ and $B \in \mathbb{R}^{c \times d}$, $A \otimes B \hat{=} [A(1, 1)B, \dots, A(1, b)B; \dots; A(a, 1)B, \dots, A(a, b)B] \in \mathbb{R}^{ac \times bd}$, 0 represents the zero matrices with compatible dimensions, and

$$\Gamma = \frac{1}{2} \begin{pmatrix} F_{1,1} & \dots & F_{1,n} \\ \vdots & \ddots & \vdots \\ F_{m,1} & \dots & F_{m,n} \end{pmatrix}, \quad \Omega_1 = (H_1 \ \dots \ H_m), \quad \Omega_2 = (G_1 \ \dots \ G_n).$$

The form of (13) implies that $\mathcal{B}(\mathbf{x}, \mathbf{y})$ is psd-convex if the matrix $M = \begin{pmatrix} 0 & \Gamma \\ \Gamma^\top & 0 \end{pmatrix}$ is positive semidefinite. Unfortunately, as [58, Theorem 1] points out, for a non-trivial bilinear function $\mathcal{B}(\mathbf{x}, \mathbf{y})$, M may not be positive semidefinite.

¹² Multiple BMI constraints can be joined as a single BMI in a block-diagonal fashion.

Nevertheless, the matrix M can always be decomposed as $M = M_1 - M_2$ with $M_1, M_2 \succeq 0$, i.e., a difference between two psd-matrices. One way to do so is to use the *eigendecomposition* of the (real symmetric¹³) matrix $M \in \mathcal{S}^{(m+n)p}$. That is, $M = V^T D V$, where the orthogonal matrix V contains the eigenvectors of M ; D is a diagonal matrix whose diagonal elements are the eigenvalues of M .

Let D^+ be the matrix obtained by setting all negative elements of D to zero and $D^- = D^+ - D$. We have

$$M = \underbrace{V^T D^+ V}_{M_1} - \underbrace{V^T D^- V}_{M_2}.$$

It follows that $M_1, M_2 \succeq 0$ and therefore we find a DC decomposition of $\mathcal{B}(\mathbf{x}, \mathbf{y})$:

Theorem 7 (Difference-of-Convex Decomposition). *The following form*

$$\mathcal{B}(\mathbf{x}, \mathbf{y}) = \mathcal{B}^+(\mathbf{x}, \mathbf{y}) - \mathcal{B}^-(\mathbf{x}, \mathbf{y}) \quad (14)$$

where

$$\begin{aligned} \mathcal{B}^+(\mathbf{x}, \mathbf{y}) &= \begin{pmatrix} \mathbf{x} \otimes I \\ \mathbf{y} \otimes I \end{pmatrix}^\top M_1 \begin{pmatrix} \mathbf{x} \otimes I \\ \mathbf{y} \otimes I \end{pmatrix} + (\Omega_1 \ \Omega_2) \begin{pmatrix} \mathbf{x} \otimes I \\ \mathbf{y} \otimes I \end{pmatrix} + F \\ \mathcal{B}^-(\mathbf{x}, \mathbf{y}) &= \begin{pmatrix} \mathbf{x} \otimes I \\ \mathbf{y} \otimes I \end{pmatrix}^\top M_2 \begin{pmatrix} \mathbf{x} \otimes I \\ \mathbf{y} \otimes I \end{pmatrix} \end{aligned}$$

is a difference-of-convex decomposition of $\mathcal{B}(\mathbf{x}, \mathbf{y})$. Namely, the matrix-valued functions $\mathcal{B}^+(\mathbf{x}, \mathbf{y})$ and $\mathcal{B}^-(\mathbf{x}, \mathbf{y})$ are psd-convex on \mathbb{R}^{m+n} .

Remark 5. In practice, the aforementioned matrices M , M_1 and M_2 induced by eigendecomposition are often highly sparse. One can hence exploit the sparsity to improve the algorithmic performance of the DCP-based synthesis approach.

5.2 Reduction to LMIs

On top of the DC decomposition (cf. Theorem 7), we can now apply a standard iterative procedure in difference-of-convex programming [10] to solve the BMIs.

The core idea of the procedure is to iteratively solve a series of convex sub-problems. More specifically, given a feasible solution $\mathbf{z}^k = (\mathbf{x}^k, \mathbf{y}^k)$ to the BMI optimization problem (12), the ‘‘concave part’’ $-\mathcal{B}^-(\mathbf{x}, \mathbf{y})$ in (14) is linearized around \mathbf{z}^k , thereby yielding a series of convex programs ($k = 0, 1, \dots$):

$$\begin{aligned} \underset{\mathbf{z}=(\mathbf{x},\mathbf{y})}{\text{maximize}} \quad & g(\mathbf{z}) + \frac{1}{2}\delta \|\mathbf{z} - \mathbf{z}^k\|^2 \\ \text{subject to} \quad & \mathcal{B}^+(\mathbf{z}) - \mathcal{B}^-(\mathbf{z}^k) - \mathcal{DB}^-(\mathbf{z}^k)(\mathbf{z} - \mathbf{z}^k) \preceq 0 \end{aligned} \quad (15)$$

where $\mathcal{DB}^-(\mathbf{z}): \mathbb{R}^{m+n} \rightarrow \mathcal{S}^p$ is the derivative of the matrix-valued function \mathcal{B}^- at \mathbf{z} , i.e., a linear mapping from a vector $\mathbf{u} \in \mathbb{R}^{m+n}$ to a matrix in \mathcal{S}^p :

$$\mathcal{DB}^-(\mathbf{z})(\mathbf{u}) \triangleq \sum_{i=1}^{n+m} u_i \frac{\partial \mathcal{B}^-}{\partial z_i}(\mathbf{z}).$$

¹³ M thus only has real eigenvalues.

Algorithm 1: BMI-DC: Solving BMIs based on DC decomposition

input: A BMI optimization problem (12) with a strictly feasible initial solution \mathbf{z}^0 .
output: A sequence of feasible solutions $S = \{\mathbf{z}^0, \dots, \mathbf{z}^k\}$ to the BMI optimization.

- 1 $k \leftarrow 0$; $S \leftarrow \{\mathbf{z}^0\}$;
- 2 $M \leftarrow$ reformulation of (12) as (13);
- 3 $(M_1, M_2) \leftarrow$ DC decomposition of M as in (14);
- 4 **repeat**
- 5 Construct the convex sub-problem (15) out of (M_1, M_2) linearized around \mathbf{z}^k ;
- 6 $\mathbf{z}^{k+1} \leftarrow$ optimum of the program (15);
- 7 $S \leftarrow S \cup \{\mathbf{z}^{k+1}\}$; $\triangleright S$ keeps track of visited points
- 8 $k \leftarrow k + 1$;
- 9 **until** $\|\mathbf{z}^k - \mathbf{z}^{k-1}\| < \varepsilon$ for a given tolerance $\varepsilon \in \mathbb{R}_0^+$;
- 10 **return** S ;

An extra regularization term $\frac{1}{2}\delta\|\mathbf{z} - \mathbf{z}^k\|^2$ with $\delta < 0$ is added in (15) to enforce that $g(\mathbf{z})$ strictly increases after each iteration until it stabilizes, which can be encoded as a second-order cone constraint and embedded in SDP solving.

Note that the linearized problem (15) is convex and therefore can be solved efficiently¹⁴ via methods including, among others, augmented Lagrangian methods [35] and gradient descent methods [3]. Furthermore, the Schur complement in Theorem 3 implies that (15) can be reformulated as an LMI problem:

Theorem 8. *The quadratic matrix inequality (QMI) constraint*

$$\mathcal{B}^+(\mathbf{z}) - \mathcal{B}^-(\mathbf{z}^k) - \mathcal{D}\mathcal{B}^-(\mathbf{z}^k)(\mathbf{z} - \mathbf{z}^k) \preceq 0$$

in (15) is equivalent to the LMI constraint¹⁵

$$\begin{pmatrix} -I & & N(\mathbf{z} \otimes I) \\ (\mathbf{z} \otimes I)^T N^T & -\mathcal{B}^-(\mathbf{z}^k) - \mathcal{D}\mathcal{B}^-(\mathbf{z}^k)(\mathbf{z} - \mathbf{z}^k) + \Omega(\mathbf{z} \otimes I) + F & \end{pmatrix} \preceq 0$$

where N is the square root matrix of M_1 , i.e., $M_1 = N^T N$, and $\Omega = (\Omega_1 \ \Omega_2)$.

Theorem 8 entails that the series of linearized convex sub-problems of the form (15) can be solved alternatively by most off-the-shelf SDP solvers designated for discharging LMIs via polynomial-time algorithms, say the interior-point methods. Furthermore, by taking the optimum of the k -th sub-problem to be the next linearization point \mathbf{z}^{k+1} , we obtain an iterative procedure for solving general BMIs, as depicted in Algorithm 1.

Algorithm 1 falls into the DCP framework [10] and thus enjoys useful properties, e.g., soundness, termination and convergence as follows.

¹⁴ The global optimum of (15) is attainable under standard assumptions, e.g., Slater’s condition and the second-order sufficient KKT conditions [3].

¹⁵ This transforms a QMI with matrices in \mathcal{S}^p to an LMI with matrices in $\mathcal{S}^{(m+n+1)p}$.

Theorem 9 (Soundness). *Every solution $\mathbf{z}^i = (\mathbf{x}^i, \mathbf{y}^i) \in S$ with $i = 0, \dots, k$ returned by Algorithm 1 is a feasible solution to the original BMI problem (12).*

The result below states termination and convergence of Algorithm 1 in terms of *KKT points* of (12), i.e., solutions fulfilling the KKT conditions [3] of (12)¹⁶.

Theorem 10 (Termination and convergence). *If (12) has finitely many KKT points, then (1) for $\varepsilon \in \mathbb{R}^+$, Algorithm 1 terminates; (2) for $\varepsilon = 0$, Algorithm 1 visits an infinite sequence of solutions converging to a KKT point.*

We remark that, under some sufficient KKT conditions and regularity conditions [3], a KKT point suffices as a local optimum. In this case, the infinite sequence $\{\mathbf{z}^i\}_{i \in \mathbb{N}}$ of points visited by Algorithm 1 (for $\varepsilon = 0$) converges to a local optimum of (12).

5.3 Finding the Initial Solution

The iterative procedure in Algorithm 1 starts with a fed-by-oracle strictly feasible initial solution \mathbf{z}^0 to the BMI problem (12). Finding such an initial solution, however, is non-trivial in general due to the non-convexity of (12). We argue though, that a strictly feasible initial solution can be obtained for the BMI problem of the form (11) induced by the barrier-certificate synthesis problem.

Recall that in the BMI problem (11), bilinearity arises from the multiplication of $B(\mathbf{a}, \mathbf{x})$ with some unknown multiplier polynomials parameterized by \mathbf{s} . One way to reduce the BMI constraints to LMIs is to fix every multiplier polynomial to be a non-negative constant, thereby yielding a linear program:

$$\begin{aligned} & \underset{\lambda, \mathbf{a}}{\text{maximize}} && \lambda \\ & \text{subject to} && \mathcal{F}_\ell(\mathbf{a}, \mathbf{s})|_{\mathbf{s}=(c_\ell, 0, \dots, 0)} + \lambda I \preceq 0, \quad \ell = 1, 2, \dots, l \end{aligned} \quad (16)$$

where \mathbf{s} in $\mathcal{F}_\ell(\mathbf{a}, \mathbf{s})$ is substituted by $(c_\ell, 0, \dots, 0)$ with $c_\ell \in \mathbb{R}_0^+$, which encodes a non-negative constant multiplier polynomial. Observe that no \mathbf{s} -variable is involved in (16) and the constraints therein are linear in \mathbf{a} .

Apparently, a strictly feasible solution (λ, \mathbf{a}) to (16) induces a strictly feasible solution $(\lambda, \mathbf{a}, (c_\ell, 0, \dots, 0))$ to (11) as well. Moreover, we have

Lemma 1. *The LMI program (16) always has a strictly feasible solution.*

As a consequence, a strictly feasible solution to the BMI problem (11) can be obtained by solving the LMI problem (16). In fact, when considering Lie derivatives only up to the first order, solving (the feasibility counterpart of) (16) is exactly the procedure to synthesize either an *exponential barrier certificate* [29] (with $c_\ell \in \mathbb{R}^+$) or a *convex barrier certificate* [41] (with $c_\ell = 0$). Algorithm 1 therefore subsumes existing synthesis techniques in the sense that any valid barrier certificate synthesized by methods in [29, 41] can also be discovered by Algorithm 1. Moreover, an alternative way to reduce the BMI constraints to LMIs is to fix the multipliers to be some given non-trivial (SOS) polynomials [62].

¹⁶ Addressing the KKT conditions in detail falls outside the scope of this paper.

Algorithm 2: Branch-and-Bound: Searching for a valid parameter $\bar{\mathbf{a}}$

input: A BMI optimization problem of the form (11) with $\mathcal{C}_{\mathbf{a}} = \{\mathbf{a} \mid \|\mathbf{a}\|^2 \leq L_{\mathbf{a}}\}$.
output: A valid parameter $\bar{\mathbf{a}}$, or otherwise \perp indicating a failure.

- 1 **if** $L_{\mathbf{a}} < \eta$ **then return** \perp ; \triangleright abort on fine-enough partitions ($\eta \in \mathbb{R}^+$)
- /* sample-and-check is not necessary if Theorem 6 is used */
- 2 $\bar{\mathbf{a}} \leftarrow$ a randomly-sampled point in $\mathcal{C}_{\mathbf{a}}$;
- 3 **if** $\bar{\mathbf{a}}$ is valid **then return** $\bar{\mathbf{a}}$; \triangleright check validity (inductive invariance)
- 4 **if** $\text{proj}_{\mathbf{a}}(S_{glb}) \cap \mathcal{C}_{\mathbf{a}} = \emptyset$ **then** $\triangleright S_{glb}$ contains a global set of visited points
- 5 $S \leftarrow$ apply BMI-DC in Algorithm 1 to (11) with initial solution in $(\mathcal{C}_{\mathbf{a}}, \mathcal{C}_{\mathbf{s}})$;
- 6 $S_{glb} \leftarrow S_{glb} \cup S$;
- /* checking validity is not necessary if Theorem 5 is used */
- 7 **if** a valid parameter $\bar{\mathbf{a}} \in \text{proj}_{\mathbf{a}}(S)$ is found **then return** $\bar{\mathbf{a}}$;
- 8 $(\mathcal{C}_{\mathbf{a}}^1, \mathcal{C}_{\mathbf{a}}^2) \leftarrow \text{bisect}(\mathcal{C}_{\mathbf{a}})$; \triangleright partition the parameter space
- 9 $\bar{\mathbf{a}} \leftarrow \text{Branch-and-Bound}(\mathcal{C}_{\mathbf{a}}^1)$;
- 10 **if** $\bar{\mathbf{a}} \neq \perp$ **then return** $\bar{\mathbf{a}}$;
- 11 **else return** $\text{Branch-and-Bound}(\mathcal{C}_{\mathbf{a}}^2)$;

Remark 6. Different choices of the multiplier constants c_l in (16) may lead to different initial solutions fed to Algorithm 1, thereby considerably different number of iterations until termination. In practice, techniques like randomization are worth exploring when choosing these multiplier constants.

6 Incorporating in a Branch-and-Bound Framework

The aforementioned iterative procedure on solving a series of convex optimizations converges only to a local optimum of the BMI problem (11) (or more generally, (12)). This means that, in some cases, it may miss the global optimum that induces a non-negative λ^* . We present in this section a solution to this problem by incorporating the iterative procedure into a branch-and-bound framework that searches for the global optimum in a divide-and-conquer fashion, as is a common technique in non-convex optimizations.

The basic idea is as follows. We first try to solve the BMI problem (11) by Algorithm 1 over the compact parameter space $(\mathcal{C}_{\mathbf{a}}, \mathcal{C}_{\mathbf{s}})$. If a valid solution, (i.e., a solution that contains a valid parameter $\bar{\mathbf{a}} \in \mathcal{C}_{\mathbf{a}}$ such that $B(\bar{\mathbf{a}}, \mathbf{x})$ is an invariant barrier certificate) is found, then the corresponding barrier certificate can be obtained. Otherwise, we keep bisecting $\mathcal{C}_{\mathbf{a}}$ and apply Algorithm 1 over each bisection¹⁷. The procedure, as depicted in Algorithm 2 in a recursive manner, terminates when a valid parameter is found or the partition is fine enough.

Algorithm 2 takes as input a BMI problem of the form (11) that encodes either the sufficient condition in Theorem 5 or the necessary condition in Theorem 6 for invariant barrier certificates. In the former case, a sample-and-check process (Line 2-3) is necessary to attain (weak) completeness (see Theorem 11). The conditional statement in Line 4 rules out parameter (sub-)spaces that have

¹⁷ The validity of $\bar{\mathbf{a}} \in \mathcal{C}_{\mathbf{a}}$ does not depend on \mathbf{s} , thus we do not partition $\mathcal{C}_{\mathbf{s}}$.

already been explored, which is the case when the projection of some visited point in S_{glob} (a global set that keeps track of visited points by Algorithm 1, initialized as \emptyset) onto \mathbf{a} is in the current parameter space.

The following theorem claims a weak completeness result: our method guarantees to find a barrier certificate when there exists an inductive invariant (in the form of a given template) that suffices to certify safety of the system.

Theorem 11 (Weak Completeness). *Algorithm 2 returns a valid parameter $\bar{\mathbf{a}} \in \mathcal{C}_{\mathbf{a}}$, if (1) the partition granularity is fine enough (i.e., small enough $\eta \in \mathbb{R}^+$), (2) the degrees of multiplier polynomials and SOS polynomials used to form (11) are large enough, and (3) there exists, for the given template $B(\mathbf{a}, \mathbf{x})$, a strictly valid parameter $\hat{\mathbf{a}} \in \mathcal{C}_{\mathbf{a}}$ (i.e., any parameter in some neighborhood of $\hat{\mathbf{a}}$ is valid).*

Remark 7. The bisection operation in Algorithm 2 induces—in the worst case—an exponential blow-up in the number of branches. In practice, one can prune branches inducing only negative objective values, via, e.g., convex relaxation [26].

7 Experimental Results

We have carried out a prototypical implementation¹⁸ of our synthesis techniques in Wolfram MATHEMATICA, which was selected due to its built-in primitives for SDP, polynomial algebra and matrix operations. Given a safety verification problem as input, our implementation works toward discovering an invariant barrier certificate (in the form of a given template) that witnesses unbounded-time safety of the system. A collection of benchmark examples (detailed in [57, Appendix B]) has been evaluated on a 2.10 GHz Intel Xeon processor with 376 GB RAM running 64-bit CentOS Linux 7.

Table 1 reports the empirical results. BMI-DC concerns our locally-convergent Algorithm 1 for solving BMIs (encoding the sufficient condition in Theorem 5) based on DC decomposition. We compare our approach with PENLAB [14]—an off-the-shelf solver in MATLAB for directly discharging the same BMI problems (with no guarantee on convergence)—and SOSTOOLS [39]—for solving LMIs derived from Prajna and Jadbabaie’s original barrier-certificate condition [41]. The comparison is performed under the same problem configurations¹⁹. Due to numerical errors caused by floating-point computations and the fact that reaching the local/global optimum does not necessarily yield a valid barrier certificate, we additionally perform a posterior check, via both the quantifier-elimination procedure in MATHEMATICA and the SMT solver Z3 [37], of the synthesized candidate barrier certificate per Definition 4.

Table 1 shows that BMI-DC suffices to synthesize valid barrier certificates in most of the examples within a reasonable number of iterations (i.e., the number of convex sub-problems solved by SDP). This however does not cover all the cases:

¹⁸ Available at <https://github.com/Chenms404/BMI-DC>.

¹⁹ For PENLAB and SOSTOOLS, we use their optimized, built-in criteria for termination and methods for finding the initial solutions.

Table 1. Empirical results on benchmark examples (time in seconds)

Example name	n_{sys}	d_{flow}	d_{BC}	BMI-DC			PENLAB		SOSTOOLS	
				#iter.	Time	Verified	Time	Verified	Time	Verified
overview [11]	2	2	1	2	0.03	✓	0.31	✓	0.07	✓
contrived	2	1	2	0	0.01	✓	0.48	✓	0.75	✓
lie-der [36]	2	2	1	0	0.01	✓	0.22	✓	0.04	✓
lorenz [11]	3	2	2	8	2.37	✓	75.11	✗	1.47	✗
lti-stable [19]	2	1	2	0	0.01	✓	0.23	✓	0.14	✓
lotka-volterra [21]	3	2	1	3	0.07	✓	0.36	✓	0.21	✓
clock [43]	2	3	1	0	0.01	✓	0.88	✗	0.18	✗
lyapunov [44]	3	3	2	4	1.25	✓	56.98	✗	0.35	✓
arch1 [50]	2	5	2	0	0.01	✓	33.76	✗	0.31	✓
arch2 [50]	2	2	2	5	0.37	✓	0.38	✗	0.17	✗
arch3 [50]	2	3	2	1	0.07	✓	0.54	✓	0.18	✓
arch4 [50]	2	2	1	2	0.09	✓	0.49	✗	0.06	✓
barr-cert1 [41]	2	3	2	12	0.85	✓	2.53	✗	0.09	✗
barr-cert2 [11]	2	2	2	6	1.57	✓	1.16	✗	0.15	✓
barr-cert3 [63]	2	2	1	0	0.01	✓	0.20	✓	0.11	✗
barr-cert4 [63]	2	3	2	13	0.96	✓	0.89	✗	0.23	✗
fitzhugh-nagumo [47]	2	3	2	2	0.16	✓	1.24	✓	0.25	✗
stabilization [48]	3	2	2	9	2.88	✓	55.22	✓	0.11	✓
lie-high-order	2	1	2	32	4.12	✓	1.56	✗	0.25	✗
raychaudhuri [13]	4	2	2	34	9.51	✓	33.64	✗	0.14	✗
focus [42]	2	1	4	100	54.89	✗	0.95	✗	0.48	✗
sys-bio1 [27]	7	2	2	2	73.22	?	101.95	?	1.35	?
sys-bio2 [27]	9	2	1	1	1.03	?	15.54	?	0.16	?
quadcopter [19]	12	1	1	0	0.03	?	65.42	?	0.36	?

n_{sys} : system dimension; d_{flow} : maximal flow-field degree; d_{BC} : degree of the template barrier certificate. #iter.: number of iterations. 0 means that the initial solution (cf. Subsect. 5.3) is valid. verified: the synthesized barrier certificate is valid (✓), invalid (✗) or inconclusive (?), beyond the capability of quantifier elimination in MATHEMATICA and nonlinear reasoning in Z3). time: CPU-time, excluding that for casting the BMIs/LMIs. Boldface marks the winner among ✓'s.

for the focus example, the solution is close enough to a local optimum (after 100 iterations) but yields still an invalid barrier certificate. This problem can be solved (if there exists an invariant barrier certificate as specified) by enforcing the branch-and-bound framework as presented in Sect. 6. The phase portraits of a selected set of examples and the synthesized invariant barrier certificates are depicted in Fig. 2 (see more in [57, Appendix B]).

The comparison in Table 1 suggests that (1) Our invariant barrier-certificate condition recognizes more barrier certificates than the original (more conservative) condition as implemented in SOSTOOLS. In particular, the lie-high-order example does admit an inductive invariant in the form of the given template, but none of the existing barrier-certificate conditions [4, 60, 63] —concerning Lie derivatives only up to the first order— recognizes it, since we have $\mathcal{L}_f^1 B(\mathbf{x}) = 0$

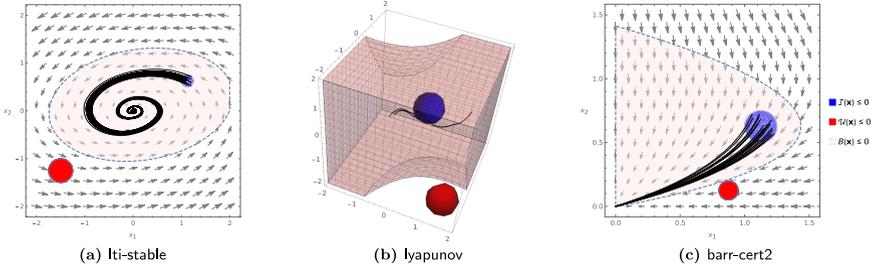


Fig. 2. Phase portraits of a selected set of examples with the synthesized invariant barrier certificates. The arrows indicate the vector field (hidden in 3D-graphics for a clear presentation) and the solid curves are randomly sampled trajectories.

for some \mathbf{x} on the boundary of B and hence it requires to exploit the second-order Lie derivative $\mathcal{L}_f^2 B$; (2) Our DCP-based synthesis algorithm finds more barrier certificates in less time than directly solving the BMI problems via non-convex optimization techniques as implemented in PENLAB.

We remark that symbolic methods based on, e.g., quantifier elimination [36], can hardly deal with any of the examples listed in Table 1 due to the prohibitively high computation complexity. Moreover, it would be desirable to pursue a comparison with the augmented Lagrangian method for solving BMIs as proposed in [4], which unfortunately is not yet possible due to the unavailability of the implementation thereof. We will discuss crucial differences to [4] in Sect. 8.

8 Related Work

As surveyed in [15], the research community has, over the past three decades, extensively addressed the automatic verification of safety-critical hybrid systems. The almost universal undecidability of the unbounded-time reachability problem [1], however, confines the sound key-press routines to either semi-decision procedures or approximation schemes, most of which address bounded-time verification by, e.g., computing the finite-time image of a set of initial states.

Invariant generation [36, 41], amongst others, is a well-established approximation scheme that provides a reliable witness for safety (or equivalently, unreachability) of dynamical systems over the infinite time horizon. Invariants can be constructed in various forms, e.g., barrier certificates [41, 51] and differential invariants [36, 40]. With a priori specified templates, the invariant synthesis problem can be reduced to numerical optimizations or constraint solving, as in, e.g., [22, 25, 46, 54].

Most pertinently, Prajna and Jadbabaie proposed in their seminal work [41] a concept coined *barrier certificate* to encode invariants. To enable efficient synthesis via semidefinite programming, the barrier-certificate condition in [41] strengthens the general condition encoding inductive invariance. Since then, significant efforts have been investigated in developing more relaxed (i.e., weaker)

forms of barrier-certificate condition that still admit efficient synthesis, thereby leading to, e.g., exponential-type barrier certificates [29], Darboux-type barrier certificates [62], general barrier certificates [8] and vector barrier certificates [51]. To attain efficient synthesis, these barrier-certificate conditions share a common property on convexity. That is, if for some $\mathbf{a}_1, \mathbf{a}_2 \in \mathbb{R}^m$, $B(\mathbf{a}_1, \mathbf{x})$ and $B(\mathbf{a}_2, \mathbf{x})$ both satisfy the barrier-certificate condition, then for any $0 < \mu < 1$, $B(\mu\mathbf{a}_1 + (1 - \mu)\mathbf{a}_2, \mathbf{x})$ must also satisfy the barrier-certificate condition.

However, neither the semantic barrier-certificate condition (9) encoding the general principle of barrier certificates [8, 51] nor the inductive invariant condition (8) is convex. This means, when resorting to convex barrier-certificate conditions, one may miss some potential barrier certificates that suffice as inductive invariants witnessing safety. Therefore, non-convex conditions were suggested [60], for which the synthesis problem can be reduced to BMI problems solvable via customized schemes, e.g., the augmented Lagrangian method [4] and the alternating minimization algorithm [63]. Our synthesis techniques also exploit a BMI reduction, with three crucial differences: (1) our invariant barrier-certificate condition is equivalent to the inductive invariant condition in the sense of Theorem 4, and thus is less conservative than all the aforementioned conditions which consider Lie derivatives only up to the first order; (2) our DCP-based techniques for solving BMIs naturally inherit appealing results on convergence and (weak) completeness, which are not (and can hardly be) provided by the approaches in [4, 60, 63]; (3) our DCP-based iterative procedure visits only feasible solutions to the original BMI problem, and hence whenever a solution that induces a non-negative objective value is found, we can safely terminate the algorithm and claim a feasible solution to the original BMI problem, which may yield a valid barrier certificate. This is not the case for the approaches in [4, 60, 63].

Beyond barrier certificates, Wang and Rajamani [58] investigated the feasibility problem of general BMI problems with an application to multi-objective nonlinear observer design. The technique of eigendecomposition was also used therein to conduct the DC decomposition. The decomposed concave part, however, is simply ignored and no iterative procedure that exhibits convergence to a local optimum can be provided.

The idea of augmenting a locally-convergent algorithm with a branch-and-bound framework to find the global optimum has been exploited in the realm of optimization [20] and control [56]. In contrast, our method is designed for the specific problem of barrier-certificate synthesis, and hence our branch-and-bound algorithm concerns only the parameter space of \mathbf{a} , i.e., coefficients of the template barrier certificate.

Finally, we refer interested readers to other approaches to solving BMI problems, e.g., rank minimization [23, 38, 45], sequential SDP [7, 12], as well as methods committed to general non-convex optimizations, e.g., interior point trust-region [5, 9, 34], successive linearization [24] and primal-dual interior point [59].

9 Conclusion

Barrier certificates are powerful tools to prove time-unbounded safety of hybrid systems. We have presented a new condition on barrier certificates—the invariant barrier-certificate condition. This condition is by far the least conservative one on barrier certificates, and can be shown as the weakest possible one to attain inductive invariance. We showed that our invariant barrier-certificate condition can be reformulated as an optimization problem subject to bilinear matrix inequalities, which can be solved by our locally-convergent algorithm based on difference-of-convex programming. By incorporating this algorithm into a branch-and-bound framework, we obtained a weak completeness result. Experiments on benchmark examples suggested that our invariant barrier-certificate condition recognizes more barrier certificates than existing conditions, and that our DCP-based algorithm is more efficient than directly solving the BMIs via off-the-shelf solvers.

We stress that our techniques for solving BMIs are of a general nature rather than being confined to barrier-certificate synthesis. Interesting future directions include to extend our method to other synthesis problems, e.g., discovering invariants and/or termination proofs of deterministic/probabilistic programs.

Acknowledgements. The authors would like to thank Hengjun Zhao for the fruitful discussion on differential dynamics requiring high-order Lie derivatives.

References

1. Alur, R., et al.: The algorithmic analysis of hybrid systems. *Theor. Comput. Sci.* **138**(1), 3–34 (1995)
2. Anai, H., Weispfenning, V.: Reach set computations using real quantifier elimination. In: *HSCC* (2001)
3. Boyd, S., Vandenberghe, L.: *Convex Optimization* (2004)
4. Chen, X., et al.: A novel approach for solving the BMI problem in barrier certificates generation. In: *CAV* (2020)
5. Chiu, W.Y.: Method of reduction of variables for bilinear matrix inequality problems in system and control designs. *IEEE SMC* **47**(7), 1241–1256 (2016)
6. Choi, M.D., Lam, T.Y., Reznick, B.: Sums of squares of real polynomials. In: *Proceedings of Symposia in Pure Mathematics* (1995)
7. Correa, R.: A global algorithm for nonlinear semidefinite programming. *SIOPT* **15**(1), 303–318 (2004)
8. Dai, L., et al.: Barrier certificates revisited. *J. Symb. Comput.* **80**, 62–86 (2017)
9. Dennis, J., Heinkenschloss, M., Vicente, L.N.: Trust-region interior-point SQP algorithms for a class of nonlinear programming problems. *SICON* **36**(5), 1750–1794 (1998)
10. Dinh, Q.T., et al.: Combining convex-concave decompositions and linearization approaches for solving BMIs, with application to static output feedback. *IEEE TAC* **57**(6), 1377–1390 (2011)

11. Djabballah, A., et al.: Construction of parametric barrier functions for dynamical systems using interval analysis. *Automatica* **78**, 287–290 (2017)
12. Eggers, A., et al.: Improving the SAT modulo ODE approach to hybrid systems analysis by combining different enclosure methods. In: *SoSyM* (2012)
13. Ferragut, A., Gasull, A.: Seeking Darboux polynomials. *Acta Applicandae Mathematicae* **139**(1), 167–186 (2015)
14. Fiala, J., Kočvara, M., Stingl, M.: PENLAB: A MATLAB solver for nonlinear semidefinite optimization. *CoRR abs/1311.5240* (2013)
15. Fränzle, M., Chen, M., Kröger, P.: In memory of Oded Maler: automatic reachability analysis of hybrid-state automata. *ACM SIGLOG News* **6**(1), 19–39 (2019)
16. Gan, T., et al.: Decidability of the reachability for a family of linear vector fields. In: *ATVA* (2015)
17. Gan, T., et al.: Computing reachable sets of linear vector fields revisited. In: *ECC* (2016)
18. Gan, T., et al.: Reachability analysis for solvable dynamical systems. *IEEE TAC* **63**(7), 2003–2018 (2018)
19. Gao, S., et al.: Numerically-robust inductive proof rules for continuous dynamical systems. In: *CAV* (2019)
20. Goh, K.C., Safonov, M.G., Papavassilopoulos, G.P.: Global optimization for the biaffine matrix inequality problem. *J. Glob. Optim.* **7**(4), 365–380 (1995)
21. Goubault, E., et al.: Finding non-polynomial positive invariants and Lyapunov functions for polynomial systems through Darboux polynomials. In: *ACC* (2014)
22. Gulwani, S., Tiwari, A.: Constraint-based approach for analysis of hybrid systems. In: *CAV* (2008)
23. Ibaraki, S., Tomizuka, M.: Rank minimization approach for solving BMI problems with random search. In: *ACC* (2001)
24. Kanzow, C., et al.: Successive linearization methods for nonlinear semidefinite programs. *Comput. Optim. Appl.* **31**(3), 252–273 (2005)
25. Kapinski, J., et al.: Simulation-guided Lyapunov analysis for hybrid dynamical systems. In: *HSCC* (2014)
26. Kheirandishfard, M., Zohrizadeh, F., Madani, R.: Convex relaxation of bilinear matrix inequalities Part I: Theoretical results. In: *CDC* (2018)
27. Klipp, E., et al.: *Systems Biology in Practice: Concepts, Implementation and Application* (2008)
28. Kolář I., Michor, P.W., Slovák, J.: *Natural Operations in Differential Geometry* (1993)
29. Kong, H., et al.: Exponential-condition-based barrier certificate generation for safety verification of hybrid systems. In: *CAV* (2013)
30. Kong, S., Solar-Lezama, A., Gao, S.: Delta-decision procedures for exists-forall problems over the reals. In: *CAV* (2018)
31. Lafferriere, G., Pappas, G.J., Yovine, S.: Symbolic reachability computation for families of linear vector fields. *J. Symb. Comput.* **32**(3), 23–253 (2001)
32. Lasserre, J.B.: *Moments, Positive Polynomials and Their Applications* (2010)
33. Le Thi, H.A., Dinh, T.P.: DC programming and DCA: thirty years of developments. *Math. Program.* **169**(1), 5–68 (2018)
34. Leibfritz, F., Mostafa, E.: An interior point constrained trust region method for a special class of nonlinear semidefinite programming problems. *SIOPT* **12**(4), 1048–1071 (2002)
35. Li, X., Sun, D., Toh, K.C.: QSDPNAL: a two-phase augmented Lagrangian method for convex quadratic semidefinite programming. *Math. Program. Comput.* **10**(4), 703–743 (2018)

36. Liu, J., Zhan, N., Zhao, H.: Computing semi-algebraic invariants for polynomial dynamical systems. In: EMSOFT (2011)
37. de Moura, L.M., Bjørner, N.: Z3: an efficient SMT solver. In: TACAS (2008)
38. Orsi, R., Helmke, U., Moore, J.B.: A Newton-like method for solving rank constrained linear matrix inequalities. *Automatica* **42**(11), 1875–1882 (2006)
39. Papachristodoulou, A., et al.: SOSTOOLS version 3.00 sum of squares optimization toolbox for MATLAB. CoRR abs/1310.4716 (2013)
40. Platzer, A., Clarke, E.M.: Computing differential invariants of hybrid systems as fixedpoints. In: CAV (2008)
41. Prajna, S., Jadbabaie, A.: Safety verification of hybrid systems using barrier certificates. In: HSCC (2004)
42. Ratschan, S., She, Z.: Constraints for continuous reachability in the verification of hybrid systems. In: AISC (2006)
43. Ratschan, S., She, Z.: Safety verification of hybrid systems by constraint propagation-based abstraction refinement. *ACM TECS* **6**(1), 8-es (2007)
44. Ratschan, S., She, Z.: Providing a basin of attraction to a target region of polynomial systems by computation of Lyapunov-like functions. *SICON* **48**(7), 4377–4394 (2010)
45. Recht, B., Fazel, M., Parrilo, P.A.: Guaranteed minimum-rank solutions of linear matrix equations via nuclear norm minimization. *SIAM Rev.* **52**(3), 471–501 (2010)
46. Sankaranarayanan, S., Sipma, H.B., Manna, Z.: Constructing invariants for hybrid systems. In: HSCC (2004)
47. Sassi, M.A.B., Girard, A., Sankaranarayanan, S.: Iterative computation of polyhedral invariants sets for polynomial dynamical systems. In: CDC (2014)
48. Sassi, M.A.B., Sankaranarayanan, S.: Stability and stabilization of polynomial dynamical systems using Bernstein polynomials. In: HSCC (2015)
49. Smith, W.D.: Church’s thesis meets the n-body problem. *Appl. Math. Comput.* **178**(1), 154–183 (2006)
50. Sogokon, A., Ghorbal, K., Johnson, T.T.: Non-linear continuous systems for safety verification (benchmark proposal). In: ARCH @ CPSWeek (2016)
51. Sogokon, A., et al.: Vector barrier certificates and comparison systems. In: FM (2018)
52. Tao, P.D., Souad, E.B.: Algorithms for solving a class of nonconvex optimization problems. North-Holland Mathematics Studies, Methods of subgradients (1986)
53. Tarski, A.: A Decision Method for Elementary Algebra and Geometry (1951)
54. Tiwari, A.: Approximate reachability for linear systems. In: HSCC (2003)
55. Toker, O., Ozbay, H.: On the NP-hardness of solving bilinear matrix inequalities and simultaneous stabilization with static output feedback. In: ACC (1995)
56. Tuan, H.D., Apkarian, P., Nakashima, Y.: A new Lagrangian dual global optimization algorithm for solving bilinear matrix inequalities. *Int. J. Rob. Nonlinear Control IFAC-Affiliat. J.* **10**(7), 561–578 (2000)
57. Wang, Q., et al.: Synthesizing invariant barrier certificates via difference-of-convex programming (extended version). arXiv abs/2105.14311 (2021)
58. Wang, Y., Rajamani, R.: Feasibility analysis of the bilinear matrix inequalities with an application to multi-objective nonlinear observer design. In: CDC (2016)
59. Yamashita, H., Yabe, H.: Local and superlinear convergence of a primal-dual interior point method for nonlinear semidefinite programming. *Math. Program.* **132**(1–2), 1–30 (2012)
60. Yang, Z., Lin, W., Wu, M.: Exact safety verification of hybrid systems based on bilinear SOS representation. *ACM TECS* **14**(1), 1–19 (2015)

61. Yang, Z., et al.: A linear programming relaxation based approach for generating barrier certificates of hybrid systems. In: FM (2016)
62. Zeng, X., et al.: Darboux-type barrier certificates for safety verification of nonlinear hybrid systems. In: EMSOFT (2016)
63. Zhang, Y., et al.: Safety verification of nonlinear hybrid systems based on bilinear programming. IEEE TCAD **37**(11),(2018)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

