On Completeness of SDP-Based Barrier Certificate Synthesis over Unbounded Domains

Hao Wu[1], Shenghua Feng[2], Ting Gan[3], Jie Wang[4], Bican Xia[5], and Naijun Zhan[1,6(✉)]

[1] State Key Laboratory of Computer Science, Institute of Software, University of Chinese Academy of Sciences, Beijing, China
{wuhao,znj}@ios.ac.cn
[2] Zhongguancun Laboratory, Beijing, China
fengsh@zgclab.edu.cn
[3] School of Computer Science, Wuhan University, Wuhan, China
ganting@whu.edu.cn
[4] Academy of Mathematics and Systems Science, CAS, Beijing, China
wangjie212@amss.ac.cn
[5] School of Mathematical Sciences, Peking University, Beijing, China
xbc@math.pku.edu.cn
[6] School of Computer Science, Peking University, Beijing, China

Abstract. Barrier certificates, serving as differential invariants that witness system safety, play a crucial role in the verification of cyber-physical systems (CPS). Prevailing computational methods for synthesizing barrier certificates are based on semidefinite programming (SDP) by exploiting *Putinar Positivstellensatz*. Consequently, these approaches are limited by the *Archimedean condition*, which requires all variables to be bounded, i.e., systems are defined over bounded domains. For systems over unbounded domains, unfortunately, existing methods become incomplete and may fail to identify potential barrier certificates.

In this paper, we address this limitation for the unbounded cases. We first give a complete characterization of polynomial barrier certificates by using *homogenization*, a recent technique in the optimization community to reduce an unbounded optimization problem to a bounded one. Furthermore, motivated by this formulation, we introduce the definition of *homogenized systems* and propose a complete characterization of a family of non-polynomial barrier certificates with more expressive power. Experimental results demonstrate that our two approaches are more effective while maintaining a comparable level of efficiency.

Keywords: Safety · Barrier certificates · Semidefinite programming · Homogenization

1   Introduction

With recent advancements in optimization theory and computational techniques, Cyber-Physical Systems (CPS), which involve the seamless integration of physical components and software systems, have proliferated across various application domains. A significant subset of CPS, known as safety-critical systems, presents a heightened level of concern. Failures or malfunctions in such systems can lead to severe safety risks for individuals and the environment. Examples of safety-critical CPS include aircraft, automobiles, integrated medical devices, nuclear power plants, and biological systems. As a result, ensuring the safety of these systems has become a primary focus of extensive academic research.

One of the key challenges in CPS verification is the safety problem (or dually, the reachability problem), i.e., to demonstrate that a system, starting from its initial states, never enters an unsafe region. In general, the safety problem of CPS is undecidable [16]. The most challenging aspect of such problem lies in reasoning about the continuous dynamics, which are typically described by ordinary differential equations (ODEs).

Deductive verification, derived from Hoare-style program verification [17], offers a method to verify safety without directly computing the reachable set. At the core of deductive verification lies the synthesis of *differential invariants* [24,28], which extend the concept of inductive invariants to the continuous-time domain. Specifically, a differential invariant is a set of states from which any trajectories starting from it can never escape. With a priori specified template, the invariant generation problem boils down to solving the constraints encoding the invariant condition. When all involved constraints are polynomial, the problem is decidable but has time complexity doubly exponential in the number of variables [24], according to Tarski's theorem [39] and the complexity for the quantifier elimination procedure [9]. Consequently, considerable efforts have been dedicated to identifying differential invariants that allow for efficient synthesis.

In their seminal work [29], Prajna and Jadbabaie introduced the concept of barrier certificates as witnesses to safety. Namely, a barrier certificate is a real-valued function whose zero sub-level set serves as a differential invariant, separating the set of initial states and the unsafe region. It is important to note that, for the purpose of efficient synthesis, the barrier certificate condition strengthens the general condition of differential invariants. Since then, various definitions of barrier certificates have been proposed, aiming to relax the original barrier certificate conditions while still allowing for efficient synthesis. Examples of such definitions include exponential-type barrier certificates [21], Darboux-type barrier certificates [45], general convex barrier certificates [8] and vector barrier certificates [37], and invariant barrier certificates [41]. Moreover, similar notions of barrier certificates have been developed for verification problems that involve control inputs [2,44], disturbances [42], stochastic dynamics [11,18,20,30], and temporal logic specifications [25,43]. These extensions broaden the applicability of barrier certificates in various domains. Recently, there are also works aim at generalizing the notion of k-inductiveness for safety verification, leading to the definitions of t-barrier certificates [6] and k-inductive barrier certificates [3,4].

Sum-of-squares optimization is a well-established computational technique for synthesizing barrier certificates and has been employed in most of the works mentioned above. Typically, the barrier certificate conditions are first encoded into constraints involving sum-of-squares polynomials. These constraints are then translated into SDP and solved by numerical solvers. In scenarios where the domains are bounded, one can choose to rely on either a sound characterization or a complete characterization to encode the conditions. The differences between these two characterizations are often overlooked, as their formulations are quite similar. However, when dealing with systems defined over unbounded domains, the sound characterization tends to be conservative while the complete characterization can not be utilized due to the violation of the Archimedean condition in Putinar's Positivstellensatz. In such unbounded cases, existing methods solely rely on the sound characterization, potentially leading to conservative results.

Besides sum-of-squares optimization, much effort have been devoted to incorporate other numerical methods for solving the obtained constraints, for instance, interval arithmetic [10,12,13], linear programming [35], and data-driven approaches [1,27,33,46,47].

Contributions. Our main contributions are threefold:

1. We explicitly clarify the connection between the soundness and the completeness of the sum-of-squares characterization of barrier certificates, which is mostly overlooked in existing works. This can be considered as a minor contribution. (See Sect. 3)
2. We utilize the *homogenization* technique from [19] to derive the first complete sum-of-squares characterization of polynomial barrier certificates over unbounded domains. (See Sect. 4)
3. We introduce the definition of homogenized systems and consider a specific class of non-polynomial barrier certificates with more expressive power. We also propose a complete sum-of-squares characterization for this class of non-polynomial barrier certificates. (See Sect. 5)

Finally, we implement algorithms for synthesizing barrier certificates based on the existing incomplete characterization and our two novel complete characterizations. These algorithms are tested over a set of benchmarks with unbounded domains adapted from the literature. Experimental results demonstrate that the two complete characterizations are more expressive while maintaining a comparable level of efficiency. (See Sect. 6)

Organization. The rest of this paper is organized as follows: Sect. 2 introduces algebraic tools that will be used. Section 3 formulates the barrier certificate synthesis problems and explains the connection between the sound and the complete characterization in the bounded case. Section 4 proposes the first complete characterization of polynomial barrier certificates over unbounded domains. Section 5 introduces the definition of homogenized systems and extends the results to a class of non-polynomial barrier certificates. Finally, Sect. 6 reports the experimental results and Sect. 7 concludes the paper.

2   Preliminaries

In this section, we fix basic notations and introduce necessary concepts concerning sum-of-squares optimization. For interested readers, we recommend [7,23] for a detailed treatment of this topic.

Basic Notations. Let $\mathbb{N}$, $\mathbb{R}$, $\mathbb{R}_{\geq 0}$, and $\mathbb{R}_{>0}$ denote the set of all natural numbers, the set of reals, non-negative real numbers and the set of positive real numbers, respectively. The set of continuously differentiable functions over $\mathbb{R}^n$ is denoted by $\mathcal{C}^1(\mathbb{R}^n)$. By convention, we use boldface letters to denote vectors and vector-valued functions, e.g., $\boldsymbol{x} = (x_1, \ldots, x_n)$ denotes a state variable and $\boldsymbol{f} = (f_1, \ldots, f_n)$ denotes a vector field. For vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$, $\langle \boldsymbol{x}, \boldsymbol{y} \rangle \;\hat{=}\; \sum_{i=1}^n x_i y_i$ represents the inner product of $\boldsymbol{x}$ and $\boldsymbol{y}$, and $\|\boldsymbol{x}\| \;\hat{=}\; \sqrt{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}$ denotes the standard Euclidean norm.

Let $\mathbb{R}[\boldsymbol{x}]$ denote the set of polynomials in variables $\boldsymbol{x}$ with real coefficients. A basic semialgebraic set $\mathcal{K} \subseteq \mathbb{R}^n$ is of the form $\{\boldsymbol{x} \in \mathbb{R}^n \mid p_1(\boldsymbol{x}) \rhd 0, \ldots, p_m(\boldsymbol{x}) \rhd 0\}$, where $p_i(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ and $\rhd \in \{\geq, >\}$. An equality $p(\boldsymbol{x}) = 0$ can be represented by two inequalities $p(\boldsymbol{x}) \geq 0$ and $-p(\boldsymbol{x}) \geq 0$. A basic semialgebraic set is considered *closed* when its defining polynomials contain only non-strict inequalities. Semialgebraic sets are formed as unions of basic semialgebraic sets. i.e., $\bigcup_{i=1}^n \mathcal{K}_i$, where each $\mathcal{K}_i$ is a basic semialgebraic set.

Sum-of-Squares Polynomials. Given $S \subseteq \mathbb{R}^n$, we say $p(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ is *nonnegative* (resp. *strictly positive*) over S if $p(\boldsymbol{x}) \geq 0$ (resp. $p(\boldsymbol{x}) > 0$) for any $\boldsymbol{x} \in S$. Sum-of-squares (SOS) polynomials are an important subset of globally nonnegative polynomials over $\mathbb{R}^n$. A polynomial $p(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ is said to be a *sum-of-squares* polynomial if it can be expressed as $p(\boldsymbol{x}) = \sum_{i=1}^m p_i(\boldsymbol{x})^2$, where $p_i(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ for each i. We use $\Sigma[\boldsymbol{x}]$ to denote the set of SOS polynomials in variables $\boldsymbol{x}$.

Putinar's Theorem. Given polynomials $p_1, \ldots, p_m \in \mathbb{R}[\boldsymbol{x}]$. Let $\mathcal{K}$ be a closed basic semialgebraic set described by

$$\mathcal{K} \;\hat{=}\; \{\boldsymbol{x} \in \mathbb{R}^n \mid p_1(\boldsymbol{x}) \geq 0, \ldots, p_m(\boldsymbol{x}) \geq 0\}. \tag{1}$$

The set of polynomials

$$\mathbf{QM}(p_1, p_2, \ldots, p_m) \;\hat{=}\; \Big\{ \sigma_0 + \sum_{i=1}^m \sigma_i p_i \mid \sigma_i \in \Sigma[\boldsymbol{x}] \text{ for } i = 0, 1, \ldots, m \Big\}$$

is called the *quadratic module* generated by $p_1, \ldots, p_m$. A quadratic module $\mathbf{QM}$ is *Archimedean*, or satisfies the *Archimedean condition*, if $N - \|\boldsymbol{x}\|^2 \in \mathbf{QM}$ for some constant $N \in \mathbb{N}$. Since a sum-of-squares polynomial $\sigma(\boldsymbol{x}) \in \Sigma[\boldsymbol{x}]$ is nonnegative over $\mathbb{R}^n$, the following result trivially holds.

Proposition 1. *Given $\mathcal{K}$ as defined in Eq. (1), then*

$$f(\boldsymbol{x}) \in \mathbf{QM}(p_1, \ldots, p_m) \implies f(\boldsymbol{x}) \geq 0 \text{ over } \mathcal{K}.$$

An important result in real algebraic geometry is Putinar's Positivstellensatz, which states that, under the Archimedean condition, the quadratic module $\mathbf{QM}(p_1, \ldots, p_m)$ contains all polynomials strictly positive over $\mathcal{K}$.

Theorem 1 (Putinar's Positivstellensatz [23,31]). *Given $\mathcal{K}$ as defined in Eq. (1) and a polynomial $f \in \mathbb{R}[\boldsymbol{x}]$, if $\mathbf{QM}(p_1, \ldots, p_m)$ is Archimedean, then*

$$f(\boldsymbol{x}) > 0 \ over \ \mathcal{K} \implies f(\boldsymbol{x}) \in \mathbf{QM}(p_1, \ldots, p_m).$$

Here, the condition "$\mathbf{QM}(p_1, \ldots, p_m)$ is Archimedean" can be intuitively understood as $\mathcal{K}$ in Eq. (1) is bounded. In one direction, if $\mathbf{QM}(p_1, \ldots, p_m)$ is Archimedean, by Proposition 1, we have $N - \|\boldsymbol{x}\|^2 \geq 0$ over $\mathcal{K}$, hence $\mathcal{K}$ is bounded. In the other direction, when $\mathcal{K}$ is bounded within a ball $\{\boldsymbol{x} \in \mathbb{R}^n \mid N - \|\boldsymbol{x}\|^2 \geq 0\}$, then we can assume a redundant constraint $p_{m+1} = N - \|\boldsymbol{x}\|^2$ and the new quadratic module $\mathbf{QM}(p_1, \ldots, p_m, p_{m+1})$ is Archimedean. In general, note that Proposition 1 does not necessarily imply that $\mathcal{K}$ is bounded.

3   Problem Formulation

In this section, we formally define the barrier certificate synthesis problem of interest, and discuss the relation between the sound and the complete sum-of-squares characterization of polynomial barrier certificates over bounded domains. The majority of the existing literature, such as [8,21,29,37], primarily focus on the sound characterization. As far as we are aware, complete characterization is only mentioned in [41]. Subsequently, we clarify the connection between these two characterizations, which can be considered as a minor contribution.

Differential Dynamical Systems. We consider a class of dynamical systems featuring differential dynamics governed by ordinary differential equations (ODEs) of autonomous type:

$$\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}) \tag{2}$$

where $\boldsymbol{x} \in \mathbb{R}^n$ is the state vector, $\dot{\boldsymbol{x}}$ denotes its temporal derivative dx/dt, and $\boldsymbol{f} : \mathbb{R}^n \to \mathbb{R}^n$ is a polynomial vector field, i.e., each component f_i of $\boldsymbol{f}$ is a polynomial. Since a polynomial vector field is locally Lipschitz continuous, ODE (2) admits an unique *solution* (or *trajectory*), denoted as $\xi_{\boldsymbol{x}_0} : \mathbb{R}_{\geq 0} \to \mathbb{R}^n$, from any initial state $\boldsymbol{x}_0 \in \mathbb{R}^n$, such that (1) $\xi_{\boldsymbol{x}_0}(0) = \boldsymbol{x}_0$ (2) for any $t' \in \mathbb{R}_{\geq 0}$, $\frac{\mathrm{d}\xi_{\boldsymbol{x}_0}}{\mathrm{d}t}\big|_{t=t'} = \boldsymbol{f}(\xi_{\boldsymbol{x}_0}(t'))$.

Safety Verification Problems. Given dynamical system Eq. (2) with domain $\mathcal{X} \subseteq \mathbb{R}^n$, initial set $\mathcal{I} \subset \mathcal{X}$, and unsafe set $\mathcal{U} \subset \mathcal{X}$, the *safety verification problem* asks whether $\mathcal{U}$ is reachable from any state in $\mathcal{I}$ within $\mathcal{X}$. Formally, let $\mathcal{R}$ denote the reachable set,

$$\mathcal{R} \ \hat{=} \ \{\boldsymbol{x} \in \mathcal{X} \mid \exists t \in \mathbb{R}_{\geq 0}, \exists \boldsymbol{x}_0 \in \mathcal{I}. \ \boldsymbol{x} = \xi_{\boldsymbol{x}_0}(t)\},$$

where we assume that a trajectory will never leave the domain. The system is said to be *safe* if $\mathcal{U} \cap \mathcal{R} = \emptyset$, and *unsafe* otherwise.

In this paper, we restrict our focus to the case when $\mathcal{X}$, $\mathcal{I}$, and $\mathcal{U}$ are closed basic semialgebraic sets described by

$$
\begin{aligned}
\mathcal{X} &\triangleq \left\{ \boldsymbol{x} \in \mathbb{R}^n \mid g_i^{\mathcal{X}}(\boldsymbol{x}) \geq 0, \text{ for } i = 1, \ldots, m_x \right\}, \\
\mathcal{I} &\triangleq \left\{ \boldsymbol{x} \in \mathcal{X} \mid g_i^{\mathcal{I}}(\boldsymbol{x}) \geq 0, \text{ for } i = 1, \ldots, m_i \right\}, \\
\mathcal{U} &\triangleq \left\{ \boldsymbol{x} \in \mathcal{X} \mid g_i^{\mathcal{U}}(\boldsymbol{x}) \geq 0, \text{ for } i = 1, \ldots, m_u \right\}.
\end{aligned}
$$

Invariants. A *differential invariant* is a subset $\Phi \subseteq \mathcal{X}$ such that any trajectory starting from Φ stays within Φ forever, i.e.,

$$\forall \boldsymbol{x}_0 \in \Phi, \forall t \in \mathbb{R}_{\geq 0}.\ \xi_{\boldsymbol{x}_0}(t) \in \Phi.$$

Utilizing this concept, we can verify the safety of a system without explicitly computing the reachable set, which is typically intractable for the majority of nonlinear systems. The idea therein is to find a differential invariant $\Phi \subseteq \mathcal{X}$ such that $\mathcal{I} \subseteq \Phi$ and $\mathcal{U} \subseteq \mathcal{X} \backslash \Phi$. According to the definition, the differential invariant Φ serves as an over-approximation of the reachable set $\mathcal{R}$, thereby substantiating safety of the system.

Barrier Certificates. Barrier certificates encapsulate the conditions requisite for a zero sub-level set of the form $\{\boldsymbol{x} \in \mathbb{R}^n \mid B(\boldsymbol{x}) \leq 0\}$ to become a differential invariant, where $B \in \mathcal{C}^1(\mathbb{R}^n)$. For the ease of explanation, we focus on exponential-type barrier certificates and refer to them as barrier certificates for simplicity. The technique presented in this paper can be readily extended to other types of barrier certificates [8,37,41] and hybrid systems (systems containing discrete transitions and continuous evolution) [29].

Theorem 2 (Exponential-type Barrier Certificates, Modified from [21]). *Given the system (2) with sets $\mathcal{X}$, $\mathcal{I}$, and $\mathcal{U}$. For any $\lambda \in \mathbb{R}$, the system is safe if there exists an exponential-type barrier certificate, namely a real-valued function $B(\boldsymbol{x}) \in \mathcal{C}^1(\mathbb{R}^n)$ satisfying the following conditions*

$$\forall \boldsymbol{x} \in \mathcal{I}.\ B(\boldsymbol{x}) \leq 0, \tag{3}$$

$$\forall \boldsymbol{x} \in \mathcal{U}.\ B(\boldsymbol{x}) \geq \epsilon_e, \tag{4}$$

$$\forall \boldsymbol{x} \in \mathcal{X}.\ \mathfrak{L}_{\boldsymbol{f}} B(\boldsymbol{x}) - \lambda B(\boldsymbol{x}) \leq 0, \tag{5}$$

for some real constant $\epsilon_e \in \mathbb{R}_{>0}$, where $\mathfrak{L}_{\boldsymbol{f}} p(\boldsymbol{x}) \triangleq \langle \frac{\partial}{\partial \boldsymbol{x}} p(\boldsymbol{x}), \boldsymbol{f}(\boldsymbol{x}) \rangle$ is the Lie derivative of $p(\boldsymbol{x})$ over the vector filed $\boldsymbol{f}$.

The difference between our Theorem 2 and its original formulation in [21] lies in Eq. (4), which was written as

$$\forall \boldsymbol{x} \in \mathcal{U}.\ B(\boldsymbol{x}) > 0. \tag{4'}$$

When the unsafe region $\mathcal{U}$ is bounded (compact), the two condition Eq. (4) and Eq. (4') coincide, as a continuous function over a compact set always attains

a minimum. However, when $\mathcal{U}$ is unbounded, our formulation is stricter in the sense that $\mathcal{I}$ and $\mathcal{U}$ can not be arbitrarily close, otherwise we would be unable to distinguish between them, as shown in the following Exmp. 1. In theory, ϵ_e can be any real constant in $\mathbb{R}_{>0}$, and the corresponding $B(\boldsymbol{x})$ will be equivalent up to a constant factor.

Example 1. Consider a system $\boldsymbol{f}(x_1, x_2) = (x_1, 0)$ with $\mathcal{X} = \mathbb{R}^2$, $\mathcal{I} = \{(x_1, x_2) \mid x_1 x_2 + 1 \leq 0, x_1 \leq 0\}$, and $\mathcal{U} = \{(x_1, x_2) \mid x_1 x_2 - 1 \geq 0, x_1 \geq 0\}$. The function $B(x_1, x_2) = x_1$ is not a valid barrier certificate according to our definition, as the condition Eq. (4) is not satisfiable for any $\epsilon_e > 0$ (though when $\epsilon_e = 0$ Eq. (4') is satisfied). In other words, the sets $\mathcal{I}$ and $\mathcal{U}$ are indistinguishable in practice when x_2 goes to infinity, and our Theorem 2 rules out such cases.

To ensure computational tractability, the barrier certificate $B(\boldsymbol{x})$ is commonly constrained to polynomial forms. One of the prevailing computational methods for synthesizing $B(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ is based on the sum-of-squares optimization. Now we present the sound and complete sum-of-squares characterizations of polynomial barrier certificate over bounded domains.

Theorem 3 (Bounded Case). *Let $\mathcal{X}$, $\mathcal{I}$, and $\mathcal{U}$ be bounded, i.e., the corresponding quadratic module is Archimedean. Given $\lambda \in \mathbb{R}$ and $\epsilon_e \in \mathbb{R}_{>0}$, consider the following constraints with parameter ϵ,*

$$
\begin{aligned}
& -B(\boldsymbol{x}) + \epsilon = \sigma_0^{\mathcal{I}} + \sum_{i=1}^{m_i} g_i^{\mathcal{I}}(\boldsymbol{x}) \sigma_i^{\mathcal{I}} \\
& B(\boldsymbol{x}) - \epsilon_e + \epsilon = \sigma_0^{\mathcal{U}} + \sum_{i=1}^{m_u} g_i^{\mathcal{U}}(\boldsymbol{x}) \sigma_i^{\mathcal{U}} \\
& \lambda B(\boldsymbol{x}) - \mathfrak{L}_{\boldsymbol{f}} B(\boldsymbol{x}) + \epsilon = \sigma_0^{\mathcal{X}} + \sum_{i=1}^{m_x} g_i^{\mathcal{X}}(\boldsymbol{x}) \sigma_i^{\mathcal{X}} \\
& \sigma_0^{\mathcal{I}}, \dots, \sigma_{m_i}^{\mathcal{I}}, \sigma_0^{\mathcal{U}}, \dots, \sigma_{m_u}^{\mathcal{U}}, \sigma_0^{\mathcal{X}}, \dots, \sigma_{m_x}^{\mathcal{X}} \in \Sigma[\boldsymbol{x}].
\end{aligned}
\tag{6}
$$

When $\epsilon = 0$, Eq. (6) gives a sound characterization of polynomial barrier certificates, i.e., any solution $B(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ to the above constraints is a barrier certificate. When $\epsilon > 0$, Eq. (6) gives a complete characterization of polynomial barrier certificates, i.e., any barrier certificate $B(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ satisfies Eq. (6).

Proof. Proposition 1 and Theorem 1 entail soundness and completeness, respectively. □

In fact, in most practical cases, Eq. (6) with $\epsilon = 0$ can be viewed as a *sound and complete* characterization. In this situation, completeness follows from the so-called "finite convergence property" of Theorem 1, which requires the underlying basic semialgebraic sets $\mathcal{X}$, $\mathcal{I}$, and $\mathcal{U}$ to satisfy some side conditions that are generally true [26]. For now, we do not go deep into these details and just consider that soundness and completeness are dependent on the parameter ϵ.

Unfortunately, when the domain $\mathcal{X}$ becomes unbounded, Eq. (6) with $\epsilon > 0$ is no longer a complete characterization due to the violation of the Archimedean condition, while the $\epsilon = 0$ case is still sound. Consequently, we can solely rely on the sound characterization to synthesize barrier certificates, which may fail to identify potential solutions as in the following example. So the problem considered in this paper is, **can we derive a complete characterization similar to Eq. (6) for the unbounded cases?**

Example 2. Consider an 1-dimensional system $f(x_1) = x_1$ with $\mathcal{X} = \mathbb{R}$, $\mathcal{I} = \{x_1 \mid x_1^3 \geq 0\}$, and $\mathcal{U} = \{x_1 \mid x_1 + 1 \leq 0\}$, then $B(x_1) = -x_1$ is a barrier certificate but is not a solution to Eq. (6) with $\epsilon = 0$. To see this, we only need to show that there exists no sum-of-squares polynomials $\sigma_0^{\mathcal{I}}(x_1), \sigma_1^{\mathcal{I}}(x_1) \in \Sigma[x_1]$ such that $x_1 = \sigma_0^{\mathcal{I}}(x_1) + x_1^3 \sigma_1^{\mathcal{I}}(x_1)$. Suppose we have such an expression, by setting $x_1 = 0$, we have $\sigma_0^{\mathcal{I}}(0) = 0$. Assume that $\sigma_0^{\mathcal{I}}$ can be expressed as $\sigma_0^{\mathcal{I}}(x_1) = \sum_i p_i^2(x_1)$, then $\sigma_0^{\mathcal{I}}(0) = 0$ implies that $p_i(0) = 0$ for each i, so each p_i factors as $p_i(x_1) = x_1 p_i'(x_1)$. Therefore, both $\sigma_0^{\mathcal{I}}(x_1)$ and $x_1^3 \sigma_1^{\mathcal{I}}(x_1)$ contain no terms of degree less than 2, which is impossible.

4   A Complete Characterization of Polynomial Barrier Certificates

In this section, we give an affirmative answer to the question raised above. The tool we use is a newly introduced technique in the optimization community, called *homogenization* [19], to transform an unbounded optimization problem into a bounded one. In the following, we utilize the homogenization technique to derive a complete characterization for polynomial barrier certificates purely from a constraint-solving perspective. In the next section, we will take a different view of this technique and consider a family of non-polynomial barrier certificates that arise naturally.

We first fix some notations. Given $\boldsymbol{x} \in \mathbb{R}^n$, let x_0 be a fresh variable. For a polynomial $p(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ of degree d, its homogenization w.r.t. variable x_0 is a new polynomial $\tilde{p} \in \mathbb{R}[x_0, \boldsymbol{x}]$ defined by $\tilde{p}(x_0, \boldsymbol{x}) \hat{=} x_0^d p(x_1/x_0, \ldots, x_n/x_0)$. For example, let $f(x_1, x_2) = x_1^2 + x_2 + 1$, then $\tilde{f}(x_0, x_1, x_2) = x_1^2 + x_2 x_0 + x_0^2$. Suppose $\mathcal{K} \subseteq \mathbb{R}^n$ is a semialgebraic set as described in Eq. (1), we introduce two related sets in $\mathbb{R}^{n+1}$ as follows:

$$\tilde{\mathcal{K}}_{>0} \hat{=} \left\{ (x_0, \boldsymbol{x}) \mid \tilde{p}_1(x_0, \boldsymbol{x}) \geq 0, \ldots, \tilde{p}_m(x_0, \boldsymbol{x}) \geq 0, \|\boldsymbol{x}\|^2 + x_0^2 = 1, x_0 > 0 \right\},$$
$$\tilde{\mathcal{K}} \hat{=} \left\{ (x_0, \boldsymbol{x}) \mid \tilde{p}_1(x_0, \boldsymbol{x}) \geq 0, \ldots, \tilde{p}_m(x_0, \boldsymbol{x}) \geq 0, \|\boldsymbol{x}\|^2 + x_0^2 = 1, x_0 \geq 0 \right\}.$$

One can see that there exists an one-to-one mapping between $\tilde{\mathcal{K}}_{>0}$ and $\mathcal{K}$:

Lemma 1. *Let $\mathcal{K}$ be as in Eq. (1). Then $\boldsymbol{x} \in \mathcal{K}$ if and only if*

$$\left(\frac{1}{\sqrt{1 + \|\boldsymbol{x}\|^2}}, \frac{x_1}{\sqrt{1 + \|\boldsymbol{x}\|^2}}, \ldots, \frac{x_n}{\sqrt{1 + \|\boldsymbol{x}\|^2}} \right) \in \tilde{\mathcal{K}}_{>0}.$$

Moreover, $(x_0, \boldsymbol{x}) \in \tilde{\mathcal{K}}_{>0}$ if and only if $\left(\frac{x_1}{\sqrt{1 - \|\boldsymbol{x}\|^2}}, \ldots, \frac{x_n}{\sqrt{1 - \|\boldsymbol{x}\|^2}} \right) \in \mathcal{K}$.

Utilizing the above lemma, we can transform a potentially *unbounded* set into a *bounded* set located on the unit sphere within $\mathbb{R}^{n+1}$. Moreover, note that points with $x_0 = 0$ in $\mathbb{R}^{n+1}$ correspond to points at infinity in $\mathbb{R}^n$. This encourages us to take the points at infinity into consideration. The related concept is captured by the following definition.

Definition 1 (Closed at Infinity [26]). *A basic semialgebraic set $\mathcal{K}$ is closed at infinity if $cl(\tilde{\mathcal{K}}_{>0}) = \tilde{\mathcal{K}}$, where $cl(\tilde{\mathcal{K}}_{>0})$ denotes the closure of $\tilde{\mathcal{K}}_{>0}$.*

We would like to emphasize that being closed at infinity is a generic property for semialgebraic sets [15], and its manifestation may be contingent upon the selection of descriptive polynomials. For example, let $S_1 = \{(x_1, x_2) \mid x_1 - x_2^2 \geq 0\}$, then S_1 is not closed at infinity because

$$(0, -1, 0) \notin cl(\tilde{S}_{1>0}) \quad \text{and} \quad (0, -1, 0) \in \tilde{S}_1.$$

However, by adding a redundant polynomial inequality $x_1 \geq 0$ in S_1, we can check $S_2 = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 - x_2^2 \geq 0, x_1 \geq 0\} (= S_1)$ is closed at infinity. In this paper, we assume that $\mathcal{I}, \mathcal{U}$, and $\mathcal{X}$ are all closed at infinity, which is purely a technical assumption. To check whether a semialgebraic set is closed at ∞, one can use [15, Thm. 2.11].

The following theorem lies at the core of the homogenization technique.

Theorem 4 ([19, Lem 3.2]). *When a basic semialgebraic set $\mathcal{K}$ is closed at infinity, for any polynomial $f \in \mathbb{R}[\boldsymbol{x}]$*

$$f(\boldsymbol{x}) \geq 0 \text{ over } \mathcal{K} \iff \tilde{f}(x_0, \boldsymbol{x}) \geq 0 \text{ over } \tilde{\mathcal{K}}.$$

Now we present the homogenized version of Theorem 3, which solves the problem raised at the end of the last section.

Theorem 5. *Assume that $\mathcal{I}, \mathcal{U}$, and $\mathcal{X}$ are all closed at infinity. Given $\lambda \in \mathbb{R}$ and $\epsilon_e \in \mathbb{R}_{>0}$, consider the following constraints with parameter ϵ,*

$$
\begin{aligned}
-\tilde{B}(x_0, \boldsymbol{x}) + \epsilon &= \sigma_0^{\mathcal{I}} + \sum_{i=1}^{m_i+2} \sigma_i^{\mathcal{I}} \tilde{g}_i^{\mathcal{I}} \\
\tilde{B}(x_0, \boldsymbol{x}) - \epsilon_e x_0^d + \epsilon &= \sigma_0^{\mathcal{U}} + \sum_{i=1}^{m_u+2} \sigma_i^{\mathcal{U}} \tilde{g}_i^{\mathcal{U}} \\
\tilde{H}(x_0, \boldsymbol{x}) + \epsilon &= \sigma_0^{\mathcal{X}} + \sum_{i=1}^{m_x+2} \sigma_i^{\mathcal{X}} \tilde{g}_i^{\mathcal{X}} \\
\sigma_0^{\mathcal{I}}, \ldots, \sigma_{m_i+1}^{\mathcal{I}}, \sigma_0^{\mathcal{U}}, &\ldots, \sigma_{m_u+1}^{\mathcal{U}}, \sigma_0^{\mathcal{X}}, \ldots, \sigma_{m_x+1}^{\mathcal{X}} \in \Sigma[x_0, \boldsymbol{x}], \\
\sigma_{m_i+2}^{\mathcal{I}}, \sigma_{m_u+2}^{\mathcal{U}}, &\sigma_{m_x+2}^{\mathcal{X}} \in \mathbb{R}[x_0, \boldsymbol{x}],
\end{aligned}
\tag{7}
$$

where $H(\boldsymbol{x}) \triangleq \lambda B(\boldsymbol{x}) - \mathfrak{L}_f B(\boldsymbol{x})$, d is the degree of $\deg B(\boldsymbol{x})$, $\tilde{g}_{m_i+1}^{\mathcal{I}} = \tilde{g}_{m_u+1}^{\mathcal{U}} = \tilde{g}_{m_x+1}^{\mathcal{X}} = x_0$, and $\tilde{g}_{m_i+2}^{\mathcal{I}} = \tilde{g}_{m_u+2}^{\mathcal{U}} = \tilde{g}_{m_x+2}^{\mathcal{X}} = x_0^2 + \|\boldsymbol{x}\|^2 - 1$. When $\epsilon = 0$, Eq. (7)

gives a sound characterization of polynomial barrier certificates, i.e., any solution $B(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ *of degree d to the above constraints is a barrier certificate. When* $\epsilon > 0$, *Eq.* (7) *gives a complete characterization of polynomial barrier certificates, i.e., any barrier certificate* $B(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ *of degree d satisfies the above constraints.*

Proof. We prove the first constraint corresponding to the initial set $\mathcal{I}$, the other two constraints are similar. By employing homogenization and Theorem 4, the original condition Eq. (3) can be transformed into $-\tilde{B}(x_0, \boldsymbol{x}) \geq 0$ over $\tilde{\mathcal{I}}$. Since the descriptive polynomials in $\tilde{\mathcal{I}}$ contain $\|\boldsymbol{x}\|^2 + x_0^2 = 1$, $\tilde{\mathcal{I}}$ is a closed basic semi-algebraic set and its corresponding quadratic module is Archimedean. Thus, we can apply Proposition 1 and Theorem 1 to obtain the soundness and completeness results, respectively. Note for the other two constraints, we need to homogenize the polynomial $B(\boldsymbol{x}) - \epsilon_e$ and $B(\boldsymbol{x}) - \mathfrak{L}_f B(\boldsymbol{x})$ as a whole.   □

5 Homogenized Systems and Semialgebraic Barrier Certificates

In this section, we take a different perspective of the technique in the last section. The motivation comes from the observation that the homogenization procedure can be viewed as mapping the original system in $\mathbb{R}^n$ into a new system in $\mathbb{R}^{n+1}$. Consequently, the constraints in Eq. (7) can be conceived as barrier certificate conditions for the new system. Employing this idea, we introduce the definition of homogenized systems as follows. To avoid confusion, we will use $(y_0, \boldsymbol{y}) \in \mathbb{R}^{n+1}$ to denote the state variables of the homogenized systems.

Definition 2 (Homogenized System). *Given a system Eq.* (2), *the homogenized system is an associated system in* $\mathbb{R}^{n+1}$. *For each state* $\boldsymbol{x} \in \mathbb{R}^n$ *of the original system, the corresponding state* $(y_0, \boldsymbol{y}) \in \mathbb{R}^{n+1}$ *of the homogenized system is given by*

$$(y_0, y_1, \ldots, y_n) = \left(\frac{1}{\sqrt{1 + \|\boldsymbol{x}\|^2}}, \frac{x_1}{\sqrt{1 + \|\boldsymbol{x}\|^2}}, \ldots, \frac{x_n}{\sqrt{1 + \|\boldsymbol{x}\|^2}}\right). \qquad (8)$$

The dynamics of the homogenized systems can be obtained by taking derivative in the right-hand-side of Eq. (8). Hence, the safety verification problem of the original system Eq. (2) with sets $\mathcal{X}$, $\mathcal{I}$, and $\mathcal{U}$ can be translated into an equivalent problem for the homogenized system Eq. (8) with sets $\tilde{\mathcal{X}}$, $\tilde{\mathcal{I}}$, and $\tilde{\mathcal{U}}$. Furthermore, we show that a barrier certificate of the original system can be computed from a barrier certificate of the homogenized system.

Theorem 6. $B(y_0, \boldsymbol{y}) \in \mathcal{C}^1(\mathbb{R}^{n+1})$ *is a barrier certificate of the homogenized system if and only if* $B(\frac{1}{\sqrt{\|\boldsymbol{x}\|^2+1}}, \frac{\boldsymbol{x}}{\sqrt{\|\boldsymbol{x}\|^2+1}})$ *is a barrier certificate of the original system.*

Proof. Let $B(y_0, \boldsymbol{y})$ be a barrier certificate of the homogenized system. Denote $g(\boldsymbol{x}) \triangleq B(\frac{1}{\sqrt{\|\boldsymbol{x}\|^2+1}}, \frac{\boldsymbol{x}}{\sqrt{\|\boldsymbol{x}\|^2+1}})$, we show that $g(\boldsymbol{x})$ satisfies the conditions in

Theorem [2]. For $\boldsymbol{x} \in \mathcal{I}$, since $(y_0, \boldsymbol{y}) \in \tilde{\mathcal{I}}^b$ by Lem. [1] and Eq. (8), we have $g(\boldsymbol{x}) = B(y_0, \boldsymbol{y}) \leq 0$. Similarly, for $\boldsymbol{x} \in \mathcal{U}$, we have $g(\boldsymbol{x}) = B(y_0, \boldsymbol{y}) \geq \epsilon_e$. Finally, since

$$\mathfrak{L}_{\boldsymbol{f}} g(\boldsymbol{x}) = \sum_{i=1}^{n} \frac{\partial g(\boldsymbol{x})}{\partial x_i} f_i(\boldsymbol{x}) = \sum_{i=1}^{n} \left(\sum_{j=0}^{n} \frac{\partial B(y_0, \boldsymbol{y})}{\partial y_j} \frac{\partial y_j}{\partial x_i} \right) f_i(\boldsymbol{x})$$

$$= \sum_{j=0}^{n} \frac{\partial B(y_0, \boldsymbol{y})}{\partial y_j} \left(\sum_{i=1}^{n} \frac{\partial y_j}{\partial x_i} f_i(\boldsymbol{x}) \right) = \mathfrak{L}_{\boldsymbol{f}'} B(y_0, \boldsymbol{y}),$$

where $\boldsymbol{f}'$ is the dynamic of the homogenized system. For any $\boldsymbol{x} \in \mathcal{X}$ we have $\mathfrak{L}_{\boldsymbol{f}} g(\boldsymbol{x}) - \lambda g(\boldsymbol{x}) = \mathfrak{L}_{\boldsymbol{f}'} B(y_0, \boldsymbol{y}) - \lambda B(y_0, \boldsymbol{y}) \leq 0$. The other direction is similar. $\square$

According to Stone-Weierstrass theorem [38], a continuous function in a compact space in $\mathbb{R}^{n+1}$ can be approximated by polynomials. This means that, if there exists $B(y_0, \boldsymbol{y}) \in \mathcal{C}^1(\mathbb{R}^{n+1})$ as a barrier certificate, one should be able to find a polynomial barrier certificate (of sufficient large degree) close to it. In fact, this is one of the reasons why we are primarily concerned with polynomial barrier certificates in the bounded case. By Theorem [6], if $B(y_0, \boldsymbol{y})$ is a polynomial of degree d, then we have

$$(\sqrt{\|\boldsymbol{x}\|^2 + 1})^d B\left(\frac{1}{\sqrt{\|\boldsymbol{x}\|^2 + 1}}, \frac{\boldsymbol{x}}{\sqrt{\|\boldsymbol{x}\|^2 + 1}}\right) = B_1(\boldsymbol{x}) + \sqrt{\|\boldsymbol{x}\|^2 + 1} \cdot B_2(\boldsymbol{x})$$

for some polynomials $B_1(\boldsymbol{x}), B_2(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$. From this expression, we can see that Theorem [5] is a special case when $B(y_0, \boldsymbol{y})$ itself is a homogeneous polynomial (i.e., all monomials are of the same degree) and $B_2(\boldsymbol{x}) = 0$.

Definition 3. *We say a barrier certificate $B(\boldsymbol{x})$ is* semialgebraic [1] *if it can be expressed as $B(\boldsymbol{x}) = B_1(\boldsymbol{x}) + \sqrt{\|\boldsymbol{x}\|^2 + 1} \cdot B_2(\boldsymbol{x})$ for some $B_1(\boldsymbol{x}), B_2(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$.*

The synthesis of semialgebraic barrier certificates is not straightforward, due to the existence of non-polynomial component $\sqrt{\|\boldsymbol{x}\|^2 + 1}$. To address this problem, we employ the technique in [22] to encode these non-polynomial expressions into polynomials with extra variables. To be concrete, we introduce two variables u and v, which stand for $\sqrt{\|\boldsymbol{x}\|^2 + 1}$ and $\frac{1}{\sqrt{\|\boldsymbol{x}\|^2+1}}$, respectively. Then, by Theorem [2], the conditions for a semialgebraic barrier certificate can be written as

$$\begin{aligned}
B_1(\boldsymbol{x}) + u B_2(\boldsymbol{x}) &\leq 0, &\text{for } \boldsymbol{x} \in \mathcal{I}, u^2 = \|\boldsymbol{x}\|^2 + 1, u \geq 0, \\
B_1(\boldsymbol{x}) + u B_2(\boldsymbol{x}) &\geq \epsilon_e, &\text{for } \boldsymbol{x} \in \mathcal{U}, u^2 = \|\boldsymbol{x}\|^2 + 1, u \geq 0, \\
G(\boldsymbol{x}, u, v) &\geq 0, &\text{for } \boldsymbol{x} \in \mathcal{X}, u^2 = \|\boldsymbol{x}\|^2 + 1, u \geq 0, uv = 1,
\end{aligned} \tag{9}$$

---

[1] A function $f(\boldsymbol{x})$ is called semialgebraic if its graph $\{(\boldsymbol{x}, f(\boldsymbol{x})) \mid \boldsymbol{x} \in \mathbb{R}^n\}$ is a semialgebraic set. Here, semialgebraic barrier certificates can only express a certain subclass of semialgebraic functions.

where $G(\boldsymbol{x}, u, v) \in \mathbb{R}[\boldsymbol{x}, u, v]$ is defined by

$$
\begin{aligned}
&\lambda \left(B_1(\boldsymbol{x}) + \sqrt{\|\boldsymbol{x}\|^2 + 1} \cdot B_2(\boldsymbol{x}) \right) - \mathfrak{L}_{\boldsymbol{f}} \left(B_1(\boldsymbol{x}) + \sqrt{\|\boldsymbol{x}\|^2 + 1} \cdot B_2(\boldsymbol{x}) \right) \\
&= \lambda \left(B_1(\boldsymbol{x}) + u \cdot B_2(\boldsymbol{x}) \right) - \mathfrak{L}_{\boldsymbol{f}} B_1(\boldsymbol{x}) - u \cdot \mathfrak{L}_{\boldsymbol{f}} B_2(\boldsymbol{x}) - v B_2(\boldsymbol{x}) \sum_{i=1}^{n} x_i f_i(\boldsymbol{x}) \\
&\hateq \ G(\boldsymbol{x}, u, v).
\end{aligned}
\tag{10}
$$

Similar to Theorems 3 and 5, we have the following characterization for semialgebraic barrier certificates. Without loss of generality, we assume that $B_1(\boldsymbol{x})$ and $B_2(\boldsymbol{x})$ are both of degree d.

Theorem 7. *Assume that $\mathcal{I}$, $\mathcal{U}$, and $\mathcal{X}$ are all closed at infinity. Given $\lambda \in \mathbb{R}$ and $\epsilon_e \in \mathbb{R}_{>0}$, consider the following constraints with parameter ϵ,*

$$
\begin{aligned}
&B(\boldsymbol{x}, u) = B_1(\boldsymbol{x}) + u \cdot B_2(\boldsymbol{x}) \\
&- \tilde{B}(x_0, \boldsymbol{x}, u) + \epsilon = \sigma_0^{\mathcal{I}} + \sum_{i=1}^{m_i+4} \sigma_i^{\mathcal{I}} \tilde{g}_i^{\mathcal{I}} \\
&\tilde{B}(x_0, \boldsymbol{x}, u) - \epsilon_e x_0^{d+1} + \epsilon = \sigma_0^{\mathcal{U}} + \sum_{i=1}^{m_u+4} \sigma_i^{\mathcal{U}} \tilde{g}_i^{\mathcal{U}} \\
&\tilde{G}(x_0, \boldsymbol{x}, u, v) + \epsilon = \sigma_0^{\mathcal{X}} + \sum_{i=1}^{m_x+5} \sigma_i^{\mathcal{X}} \tilde{g}_i^{\mathcal{X}} \\
&\sigma_0^{\mathcal{I}}, \ldots, \sigma_{m_i+2}^{\mathcal{I}}, \sigma_0^{\mathcal{U}}, \ldots, \sigma_{m_u+2}^{\mathcal{U}} \in \Sigma[x_0, \boldsymbol{x}, u], \\
&\sigma_0^{\mathcal{X}}, \ldots, \sigma_{m_x+2}^{\mathcal{X}} \in \Sigma[x_0, \boldsymbol{x}, u, v], \\
&\sigma_{m_i+3}^{\mathcal{I}}, \sigma_{m_i+4}^{\mathcal{I}}, \sigma_{m_u+3}^{\mathcal{U}}, \sigma_{m_u+4}^{\mathcal{U}} \in \mathbb{R}[x_0, \boldsymbol{x}, u] \\
&\sigma_{m_x+3}^{\mathcal{X}}, \sigma_{m_x+4}^{\mathcal{X}}, \sigma_{m_x+5}^{\mathcal{X}} \in \mathbb{R}[x_0, \boldsymbol{x}, u, v],
\end{aligned}
\tag{11}
$$

where $G(\boldsymbol{x}, u, v)$ is as defined in Eq. (10), $\tilde{g}_{m_i+1}^{\mathcal{I}} = \tilde{g}_{m_u+1}^{\mathcal{U}} = \tilde{g}_{m_x+1}^{\mathcal{X}} = x_0$, $\tilde{g}_{m_i+2}^{\mathcal{I}} = \tilde{g}_{m_u+2}^{\mathcal{U}} = \tilde{g}_{m_x+2}^{\mathcal{X}} = u$, $\tilde{g}_{m_i+3}^{\mathcal{I}} = \tilde{g}_{m_u+3}^{\mathcal{U}} = \tilde{g}_{m_x+3}^{\mathcal{X}} = u^2 - x_0^2 - \|\boldsymbol{x}\|^2$, $\tilde{g}_{m_i+4}^{\mathcal{I}} = \tilde{g}_{m_u+4}^{\mathcal{U}} = x_0^2 + \|\boldsymbol{x}\|^2 + u^2 - 1$, $\tilde{g}_{m_x+4}^{\mathcal{X}} = uv - x_0^2$, and $\tilde{g}_{m_x+5}^{\mathcal{X}} = x_0^2 + \|\boldsymbol{x}\|^2 + u^2 + v^2 - 1$. When $\epsilon = 0$, Eq. (11) gives a sound characterization for semialgebraic barrier certificates, i.e., any pair of solutions $B_1(\boldsymbol{x}), B_2(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ to the above constraints makes $B(\boldsymbol{x})$ a barrier certificate. When $\epsilon > 0$, Eq. (11) gives a complete characterization for semialgebraic barrier certificates, i.e., any semialgebraic barrier certificate with $B_1(\boldsymbol{x}), B_2(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ of degree d satisfies the above constraints.

Proof. By applying Theorem 4 to Eq. (9). Similar to the proof of Theorem 5. □

6 Experiments

Implementation. We implemented the barrier certificate synthesis procedures in Julia programming language, interfaced with TSSOS [40] for formulating SOS
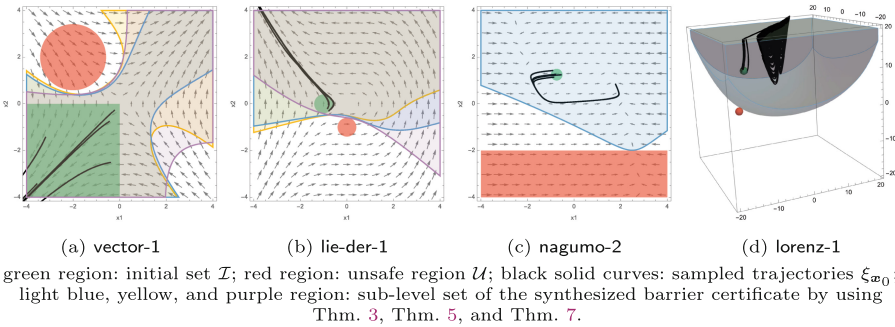
relaxations and MOSEK solver [5] for solving the underlying SDP. All experiments were performed on a Mac lap-top with Apple M2 chip and 8GB memory. The code and benchmarks are publicly available online . In the following, we use the corresponding theorems to refer to different approaches/characterizations.

Experiment Settings. The goal of our experiments was to compare the differences between employing characterizations Theorems 3, 5, and 7 to synthesize exponential-type barrier certificates over unbounded domains. To this end, we collected a set of dynamical systems of dimension 2 and 3 from the literature. For each benchmark system, we designed two problem instances. In the first instance, we only let the domain $\mathcal{X} = \mathbb{R}^n$ be unbounded, while in the second instance, we further let the initial set $\mathcal{I}$ and/or the unsafe region $\mathcal{U}$ be unbounded (not necessarily containing the original bounded counterparts).

In practical computation, we set $\lambda = -1$, $\epsilon_e = 10^{-5}$ in the definition of barrier certificates and $\epsilon = 0$ in the sum-of-squares characterizations. As discussed after Theorem 3, the $\epsilon = 0$ case can be viewed as both sound and complete in most practical situations. We manually verified that the sets $\mathcal{I}, \mathcal{U}$, and $\mathcal{X}$ are closed at infinity.

For Theorems 3 and 5, we searched for polynomial barrier certificates $B(\boldsymbol{x})$ up to degree 6. For Theorem 7, due to the $\sqrt{\|\boldsymbol{x}\|^2 + 1}$ term, we searched for semi-algebraic barrier certificates with $B_1(\boldsymbol{x})$ and $B_2(\boldsymbol{x})$ up to degree 4. When the target degree d is fixed, by restricting the highest degree of involved polynomials to be the smallest even number larger than d, the sum-of-squares characterizations can be solved as SDPs [7]. For each solution returned by SDP solver, we utilized MATHEMATICA to symbolically verify that the numerical solution $B(\boldsymbol{x})$ satisfies the barrier certificate conditions. The timeout for verifying each barrier certificate candidate was set to be 10 min. We report the total time for solving SDP constraints and verifying the results.

Empirical Observations. Table 1 reports the experimental results, and Fig. 1 portraits selected examples. We mainly compare the results from two aspects.

(a) vector-1   (b) lie-der-1   (c) nagumo-2   (d) lorenz-1

green region: initial set $\mathcal{I}$; red region: unsafe region $\mathcal{U}$; black solid curves: sampled trajectories $\xi_{\boldsymbol{x}_0}$; light blue, yellow, and purple region: sub-level set of the synthesized barrier certificate by using Thm. 3, Thm. 5, and Thm. 7.

Fig. 1. Portraits of four selected examples.

Table 1. Experimental results for synthesizing exponential type barrier certificates.

system	dim	unbounded	Thm. 3 [21]			Our Thm. 5			Our Thm. 7		
			deg	succ	time(s)	deg	succ	time(s)	deg	succ	time(s)
vector[37]	2	$\mathcal{X}$	4	✓	0.58	3	✓	0.03	**2**	✓	0.83
		$\mathcal{I},\mathcal{U},\mathcal{X}$	> 6	✗	0.39	4	✓	0.16	**2**	✓	0.72
barrier[29]	2	$\mathcal{X}$	> 6	✗	2.40	> 6	✗	2.73	>4	✗	22.98
		$\mathcal{I},\mathcal{U},\mathcal{X}$	> 6	✗	0.78	3	✓	0.04	**2**	✓	3.12
lie-der[24]	2	$\mathcal{X}$	3	✓	0.19	3	✓	0.14	1	✓	0.75
		$\mathcal{I},\mathcal{U},\mathcal{X}$	**3**	✓	0.14	**3**	✓	0.19	3	✓	5.04
arch1[36]	2	$\mathcal{X}$	**4**	✓	0.40	**4**	✓	0.54	> 4	✗	117.61
		$\mathcal{I},\mathcal{U},\mathcal{X}$	**1**	✓	0.09	**1**	✓	0.04	2	✓	20.92
arch2[36]	2	$\mathcal{X}$	**3**	✓	0.20	**3**	✓	0.21	3	✓	5.53
		$\mathcal{I},\mathcal{U},\mathcal{X}$	3	✓	0.18	3	✓	0.18	2	✓	1.59
arch3[36]	2	$\mathcal{X}$	**2**	✓	0.12	**2**	✓	0.13	**2**	✓	3.45
		$\mathcal{I},\mathcal{U},\mathcal{X}$	> 6	✗	0.84	> 6	✗	1.30	1	✓	0.34
arch4[36]	2	$\mathcal{X}$	> 6	✗	0.11	5	✓	0.74	**3**	✓	5.69
		$\mathcal{U},\mathcal{X}$	> 6	✗	1.02	**6**	✓	1.21	> 4	✗	7.74
nagumo[34]	2	$\mathcal{X}$	**2**	✓	0.13	**2**	✓	0.14	**2**	✓	3.50
		$\mathcal{U},\mathcal{X}$	> 6	✗	1.02	**3**	✓	0.17	> 4	✗	23.73
lorenz[10]	3	$\mathcal{X}$	6	?	TO	4	✓	72.13	2	?	TO
		$\mathcal{U},\mathcal{X}$	5	✓	248.88	6	?	TO	2	?	TO
lotka[14]	3	$\mathcal{X}$	> 6	✗	88.97	> 6	✗	27.8	3	?	TO
		$\mathcal{U},\mathcal{X}$	> 6	✗	0.27	> 6	✗	438.54	3	?	TO

dim: system dimension; **unbounded**: the unbounded region(s); **deg**: degree of polynomial barrier certificates or polynomial components in semialgebraic barrier certificates; **succ**: whether our algorithm succeeds in finding a valid barrier certificate. ✓ means valid solution, ✗ means no solution or invalid solution (within the search range), and ? means unverified; TO: verification takes more than 10 min in MATHEMATICA; **time**: total time for SDP solving and verification.

Expressiveness : For problems with unbounded domains, both our complete characterizations Theorems 5 and 7 are more expressive than the incomplete characterization Theorem 3, as they succeeds in synthesizing barrier certificates in more problem instances. The two complete characterizations offer distinct advantages: Thm. 5 exhibits broader applicability, demonstrably successful for problem instances like arch4-2 and nagumo-2. In contrast, Theorem 7 excels at synthesizing lower-degree barrier certificates, as exemplified by vector-1,2 and barrier-1,2 problem instances. The experimental results also demonstrate that, while Theorem 7 theoretically subsumes Theorem 5, its characterization presents significantly greater complexity and hinders its ability to identify solutions, due to inherent numerical issues in SDP solvers.

Efficiency : For most benchmarks, the time overhead for employing Theorem 5 is comparable to Theorem 3, while Theorem 7 is evidently slower than the other two. This should be attributed to the introduction of fresh variables in SOS characterizations in the complete characterizations (one for Theorem 5 and two for Theorem 7). Hence, the computation cost of both SDP solving and posterior verification increases, mildly for Theorem 5 (e.g., lie-der-2 and arch1-1) but severely for Theorem 7 (e.g., barrier-1 and arch1-1). We also want to emphasize that, for 3-dimensional systems with higher-degree templates, posterior verification time increases significantly, meaning that we can not verify the validity of the barrier certificate candidates within a reasonable amount of time.

Summary. For practical applications, we recommend employing Theorem 5 to synthesize polynomial barrier certificates for unbounded problems. This approach achieves a high level of expressiveness while maintaining efficiency comparable to Theorem 3. Moreover, we believe that the performance of Theorem 7 can be improved by exploiting algebraic structures of the constraints. For example, the variables u, v only occur linearly or quadratically in constraints, which can be utilized in restrict the templates of unknown sum-of-squares polynomials.

Remark 1. In our experiments, we did *not* consider different parameter settings (such as the selection of λ discussed in [21]) and constraint formulations (such as techniques for taming numerical errors discussed in [32]), which may impact the synthesized barrier certificates but are not the focus of the current paper.

7   Conclusion

This paper addresses the problem of synthesizing barrier certificates over unbounded domains. Previous SDP-based approaches to this problem are incomplete, because Putinar's Positivstellensatz is only applicable in bounded cases. We fill this gap by proposing the first complete sum-of-squares characterization for polynomial barrier certificates, achieved through the utilization of the homogenization approach derived from optimization theory. Furthermore, we introduce the notions of homogenized systems and semialgebraic barrier certificates, which are induced from polynomial barrier certificates of the homogenized systems. For such non-polynomial barrier certificates, we also provide a complete characterization. Experimental results substantiate the efficacy of both of our approaches, demonstrating their enhanced expressiveness and ability to synthesize more barrier certificates in comparison to existing methods.

While our paper primarily focuses on synthesizing barrier certificates for differential dynamical systems, it is crucial to note that our method can be readily extended to other types of systems, including hybrid systems and systems with control, disturbance, or stochastic dynamics. Furthermore, our method can also be utilized in related verification problems such as Lyapunov function synthesis, program invariant generation, and so on.

Data Availability Statement. The experimental results of this paper may be reproduced using the artifact on Figshare https://doi.org/10.6084/m9.figshare.26085853, or via GitHub link https://github.com/EcstasyH/BCunbounded.

References

1. Abate, A., Ahmed, D., Edwards, A., Giacobbe, M., Peruffo, A.: FOSSIL: a software tool for the formal synthesis of Lyapunov functions and barrier certificates using neural networks. In: 24th ACM International Conference on Hybrid Systems: Computation and Control, HSCC 2021, pp. 1–11. ACM (2021)
2. Ames, A.D., Xu, X., Grizzle, J.W., Tabuada, P.: Control barrier function based quadratic programs for safety critical systems. IEEE Trans. Autom. Control **62**(8), 3861–3876 (2017)
3. Anand, M., Murali, V., Trivedi, A., Zamani, M.: Safety verification of dynamical systems via k-inductive barrier certificates. In: 2021 60th IEEE Conference on Decision and Control CDC 2021, pp. 1314–1320. IEEE (2021)
4. Anand, M., Murali, V., Trivedi, A., Zamani, M.: k-inductive barrier certificates for stochastic systems. In: Hybrid Systems: Computation and Control, 25th ACM International Conference, pp. 1–11. ACM (2022)
5. ApS, M.: MOSEK Optimizer API for Julia. Version 10.1.13. (2019). https://docs.mosek.com/latest/juliaapi/index.html
6. Bak, S.: t-barrier certificates: a continuous analogy to k-induction. In: 6th IFAC Conference on Analysis and Design of Hybrid Systems, ADHS 2018. IFAC-PapersOnLine, vol. 51, pp. 145–150. Elsevier (2018)
7. Blekherman, G., Parrilo, P.A., Thomas, R.R.: Semidefinite Optimization and Convex Algebraic Geometry. SIAM (2012)
8. Dai, L., Gan, T., Xia, B., Zhan, N.: Barrier certificates revisited. J. Symb. Comput. **80**, 62–86 (2017)
9. Davenport, J.H., Heintz, J.: Real quantifier elimination is doubly exponential. J. Symb. Comput. **5**(1–2), 29–35 (1988)
10. Djaballah, A., Chapoutot, A., Kieffer, M., Bouissou, O.: Construction of parametric barrier functions for dynamical systems using interval analysis. Automatica **78**, 287–296 (2017)
11. Feng, S., Chen, M., Xue, B., Sankaranarayanan, S., Zhan, N.: Unbounded-time safety verification of stochastic differential dynamics. In: Lahiri, S.K., Wang, C. (eds.) CAV 2020. LNCS, vol. 12225, pp. 327–348. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-53291-8_18
12. Gao, S., Avigad, J., Clarke, E.M.: δ-complete decision procedures for satisfiability over the reals. In: Gramlich, B., Miller, D., Sattler, U. (eds.) IJCAR 2012. LNCS (LNAI), vol. 7364, pp. 286–300. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-31365-3_23

13. Gao, S., Kong, S., Clarke, E.M.: dReal: an smt solver for nonlinear theories over the reals. In: Bonacina, M.P. (ed.) CADE 2013. LNCS (LNAI), vol. 7898, pp. 208–214. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38574-2_14

14. Goubault, E., Jourdan, J., Putot, S., Sankaranarayanan, S.: Finding non-polynomial positive invariants and lyapunov functions for polynomial systems through darboux polynomials. In: American Control Conference, ACC 2014, pp. 3571–3578. IEEE (2014)

15. Guo, F., Wang, L., Zhou, G.: Minimizing rational functions by exact jacobian SDP relaxation applicable to finite singularities. J. Global Optim. **58**(2), 261–284 (2014)

16. Henzinger, T.A., Kopke, P.W., Puri, A., Varaiya, P.: What's decidable about hybrid automata? In: Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing, STOC 1995, pp. 373–382. ACM (1995)

17. Hoare, C.A.R.: An axiomatic basis for computer programming. Commun. ACM **12**(10), 576–580 (1969)

18. Huang, C., Chen, X., Lin, W., Yang, Z., Li, X.: Probabilistic safety verification of stochastic hybrid systems using barrier certificates. ACM Trans. Embed. Comput. Syst. **16**(5s), 1–19 (2017)

19. Huang, L., Nie, J., Yuan, Y.: Homogenization for polynomial optimization with unbounded sets. Math. Program. **200**(1), 105–145 (2023)

20. Jagtap, P., Soudjani, S., Zamani, M.: Formal synthesis of stochastic systems via control barrier certificates. IEEE Trans. Autom. Control **66**(7), 3097–3110 (2021)

21. Kong, H., He, F., Song, X., Hung, W.N.N., Gu, M.: Exponential-condition-based barrier certificate generation for safety verification of hybrid systems. In: Sharygina, N., Veith, H. (eds.) CAV 2013. LNCS, vol. 8044, pp. 242–257. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39799-8_17

22. Lasserre, J.B., Putinar, M.: Positivity and optimization: beyond polynomials. In: Anjos, M.F., Lasserre, J.B. (eds.) Handbook on Semidefinite, Conic and Polynomial Optimization. International Series in Operations Research & Management Science, vol. 166, pp. 407–434. Springer, New York, NY (2012). https://doi.org/10.1007/978-1-4614-0769-0_14

23. Lasserre, J.B.: Moments, Positive Polynomials and their Applications, vol. 1. World Scientific (2009)

24. Liu, J., Zhan, N., Zhao, H.: Computing semi-algebraic invariants for polynomial dynamical systems. In: Proceedings of the 11th International Conference on Embedded Software, EMSOFT 2011, pp. 97–106. ACM (2011)

25. Murali, V., Trivedi, A., Zamani, M.: Closure certificates. In: HSCC 2024: Proceedings of the 27th ACM International Conference on Hybrid Systems: Computation and Control, pp. 1–11 (2024)

26. Nie, J.: Discriminants and nonnegative polynomials. J. Symb. Comput. **47**(2), 167–191 (2012)

27. Peruffo, A., Ahmed, D., Abate, A.: Automated and formal synthesis of neural barrier certificates for dynamical models. In: TACAS 2021. LNCS, vol. 12651, pp. 370–388. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-72016-2_20

28. Platzer, A., Clarke, E.M.: Computing differential invariants of hybrid systems as fixedpoints. In: Gupta, A., Malik, S. (eds.) CAV 2008. LNCS, vol. 5123, pp. 176–189. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-70545-1_17

29. Prajna, S., Jadbabaie, A.: Safety verification of hybrid systems using barrier certificates. In: Alur, R., Pappas, G.J. (eds.) HSCC 2004. LNCS, vol. 2993, pp. 477–492. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24743-2_32

30. Prajna, S., Jadbabaie, A., Pappas, G.J.: A framework for worst-case and stochastic safety verification using barrier certificates. IEEE Trans. Autom. Control **52**(8), 1415–1428 (2007)
31. Putinar, M.: Positive polynomials on compact semi-algebraic sets. Indiana Univ. Math. J. **42**(3), 969–984 (1993)
32. Roux, P., Voronin, Y., Sankaranarayanan, S.: Validating numerical semidefinite programming solvers for polynomial invariants. Formal Methods Syst. Des. **53**(2), 286–312 (2018)
33. Salamati, A., Zamani, M.: Data-driven safety verification of stochastic systems via barrier certificates: a wait-and-judge approach. In: Learning for Dynamics and Control Conference, L4DC 2022. Proceedings of Machine Learning Research, vol. 168, pp. 441–452. PMLR (2022)
34. Sassi, M.A.B., Girard, A., Sankaranarayanan, S.: Iterative computation of polyhedral invariants sets for polynomial dynamical systems. In: 53rd IEEE Conference on Decision and Control, CDC 2014, pp. 6348–6353. IEEE (2014)
35. Sassi, M.A.B., Sankaranarayanan, S., Chen, X., Ábrahám, E.: Linear relaxations of polynomial positivity for polynomial Lyapunov function synthesis. IMA J. Math. Control. Inf. **33**(3), 723–756 (2016)
36. Sogokon, A., Ghorbal, K., Johnson, T.T.: Non-linear continuous systems for safety verification. In: ARCH@CPSWeek 2016, 3rd International Workshop on Applied Verification for Continuous and Hybrid Systems. EPiC Series in Computing, vol. 43, pp. 42–51. EasyChair (2016)
37. Sogokon, A., Ghorbal, K., Tan, Y.K., Platzer, A.: Vector barrier certificates and comparison systems. In: Havelund, K., Peleska, J., Roscoe, B., de Vink, E. (eds.) FM 2018. LNCS, vol. 10951, pp. 418–437. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-95582-7_25
38. Stone, M.H.: The generalized weierstrass approximation theorem. Math. Mag. **21**(5), 237–254 (1948). http://www.jstor.org/stable/3029337
39. Tarski, A.: A Decision Method for Elementary Algebra and Geometry. University of California Press, Berkeley (May (1951)
40. Wang, J., Magron, V., Lasserre, J.: TSSOS: a moment-SOS hierarchy that exploits term sparsity. SIAM J. Optim. **31**(1), 30–58 (2021)
41. Wang, Q., Chen, M., Xue, B., Zhan, N., Katoen, J.: Encoding inductive invariants as barrier certificates: synthesis via difference-of-convex programming. Inf. Comput. **289**(Part), 104965 (2022)
42. Wang, Q., Li, Y., Xia, B., Zhan, N.: Generating semi-algebraic invariants for non-autonomous polynomial hybrid systems. J. Syst. Sci. Complexity **30**(1), 234–252 (2017)
43. Wongpiromsarn, T., Topcu, U., Lamperski, A.: Automata theory meets barrier certificates: temporal logic verification of nonlinear systems. IEEE Trans. Autom. Control **61**(11), 3344–3355 (2016)
44. Xu, X., Tabuada, P., Grizzle, J.W., Ames, A.D.: Robustness of control barrier functions for safety critical control. In: 5th IFAC Conference on Analysis and Design of Hybrid Systems, ADHS 2015. IFAC-PapersOnLine, vol. 48, pp. 54–61. Elsevier (2015)
45. Zeng, X., Lin, W., Yang, Z., Chen, X., Wang, L.: Darboux-type barrier certificates for safety verification of nonlinear hybrid systems. In: International Conference on Embedded Software, 2016, pp. 1–10. ACM (2016)
46. Zhao, H., Qi, N., Dehbi, L., Zeng, X., Yang, Z.: Formal synthesis of neural barrier certificates for continuous systems via counterexample guided learning. ACM Trans. Embed. Comput. Syst. **22**(5s), 1–21 (2023)

47. Zhao, H., Zeng, X., Chen, T., Liu, Z.: Synthesizing barrier certificates using neural networks. In: HSCC 2020: 23rd ACM International Conference on Hybrid Systems: Computation and Control, Sydney, New South Wales, Australia, April 21–24, 2020, pp. 1–11. ACM (2020)