Vector Barrier Certificates and Comparison Systems*

Andrew Sogokon[1], Khalil Ghorbal[2], Yong Kiam Tan[1], and André Platzer[1]

[1] Computer Science Department, Carnegie Mellon University, Pittsburgh, USA
{asogokon | yongkiat | aplatzer}@cs.cmu.edu
[2] INRIA, Rennes, France
khalil.ghorbal@inria.fr

Abstract. Vector Lyapunov functions are a multi-dimensional extension of the more familiar (scalar) Lyapunov functions, commonly used to prove stability properties in systems of non-linear ordinary differential equations (ODEs). This paper explores an analogous vector extension for so-called *barrier certificates* used in safety verification. As with vector Lyapunov functions, the approach hinges on constructing appropriate *comparison systems*, i.e., related differential equation systems from which properties of the original system may be inferred. The paper presents an accessible development of the approach, demonstrates that most previous notions of barrier certificate are special cases of comparison systems, and discusses the potential applications of vector barrier certificates in safety verification and invariant synthesis.

Keywords: ordinary differential equations, safety verification, vector barrier certificates, comparison systems

1 Introduction

Over the past decade, *barrier certificates* have emerged as a rather popular Lyapunov-like technique for proving safety properties of continuous systems governed by ODEs, as well as hybrid dynamical systems, which combine continuous and discrete dynamics and provide models for modern control and embedded systems. Since the original formulation of barrier certificates [37], significant efforts have been directed at the problem of generalizing and relaxing the conditions that are required under this approach, so as to broaden its scope and applicability. A number of generalizations have been reported in the verification community (e.g. [22,11]). We demonstrate in this paper how *comparison systems* (a well-established concept in the theory of ODEs) fundamentally underlie these developments and provide a clean conceptual basis for understanding and further developing the method of barrier certificates. Following the seminal work of

* This work was supported by the National Science Foundation under NSF CPS Award CNS-1739629 and by the AFOSR under grant number FA9550-16-1-0288; the third author was supported by the National Science Scholarship from A*STAR, Singapore.

K. Havelund et al. (Eds.): FM 2018, LNCS 10951, pp. 418–437, 2018.
DOI: 10.1007/978-3-319-95582-7_25

R. E. Bellman, who first introduced *vector Lyapunov functions* [2] as a way of relaxing the standard (scalar) Lyapunov conditions for proving stability in ODEs, we will explore an extension of barrier certificates based on multi-dimensional (i.e. vector) comparison systems.

Structure of this paper. Mathematical preliminaries are reviewed in Section 2. Thereafter, the paper consists of two technical parts. The first part, in Section 3, reviews the method of barrier certificates and demonstrates how *convex* [37], *exponential-type* [22] and the more recent *general barrier certificates* [11] effectively amount to a straightforward application of the *comparison principle* and can be interpreted as special cases of this more general framework. The second part, in Section 4, uses multi-dimensional comparison systems to extend existing (scalar) notions of barrier certificates to what we term *vector barrier certificates*, analogously to vector Lyapunov functions known from control theory. Section 6 discusses related work and Section 7 concludes with a short summary.

2 Fundamental Definitions

We begin with an overview of some important concepts and definitions. In this paper we are concerned with studying systems of polynomial ODEs and will work under the assumption that functions are polynomials, unless stated otherwise.

2.1 Systems of Ordinary Differential Equations

An autonomous n-dimensional system of ODEs is of the form:

$$\begin{aligned} x_1' &= f_1(x_1, x_2, \ldots, x_n), \\ &\vdots \\ x_n' &= f_n(x_1, x_2, \ldots, x_n), \end{aligned}$$

where $f_i : \mathbb{R}^n \to \mathbb{R}$ is a real-valued (typically continuous) function for each $i \in \{1, \ldots, n\}$, and x_i' denotes the time derivative of x_i, i.e. $\frac{dx_i}{dt}$. In applications, constraints are often used to specify the states where the system is allowed to evolve, i.e. the system may only be allowed to evolve inside some given set $Q \subseteq \mathbb{R}^n$, which is known as the *evolution constraint* (or a *mode invariant* of some mode q in the context of hybrid automata). We can write down systems of constrained ODEs concisely by using vector notation, i.e. by writing $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x}),\ \boldsymbol{x} \in Q$. Here we have $\boldsymbol{x}' = (x_1', \ldots, x_n')$ and $\boldsymbol{f} : \mathbb{R}^n \to \mathbb{R}^n$ is a *vector field* generated by the system, i.e. $\boldsymbol{f}(\boldsymbol{x}) = (f_1(\boldsymbol{x}), \ldots, f_n(\boldsymbol{x}))$ for all $\boldsymbol{x} \in \mathbb{R}^n$. If no evolution constraint is given, Q is assumed to be the Euclidean space $\mathbb{R}^n$. The Lie derivative of a differentiable scalar function $g : \mathbb{R}^n \to \mathbb{R}$ in the state variables of such a system is denoted by g' and given by $\sum_{i=1}^{n} \frac{\partial g}{\partial x_i} f_i$.

A *solution* to the initial value problem (IVP) for the system of ODEs $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$ with initial value $\boldsymbol{x}_0 \in \mathbb{R}^n$ is a (differentiable) function $\boldsymbol{x} : (a, b) \to \mathbb{R}^n$

defined for all t in some open interval including zero, i.e. $t \in (a, b)$, where $a, b \in \mathbb{R} \cup \{\infty, -\infty\}$, $a < 0 < b$, and such that $\boldsymbol{x}(0) = \boldsymbol{x}_0$ and $\frac{d}{dt}\boldsymbol{x}(t) = \boldsymbol{f}(\boldsymbol{x}(t))$ for all $t \in (a, b)$. At time t, for solutions to IVPs with initial value $\boldsymbol{x}_0$, we shall write $\boldsymbol{x}(\boldsymbol{x}_0, t)$, or simply $\boldsymbol{x}(t)$ if the initial condition is understood from context. If the solution $\boldsymbol{x}(\boldsymbol{x}_0, t)$ is available in closed-form,[3] then one can study properties such as safety and liveness by analysing the closed-form expression. However, in non-linear ODEs it is in practice highly uncommon for solutions to exist explicitly in closed-form [20,3], and even if closed-form solutions can be found, transcendental functions in these expressions lead to undecidable arithmetic [41].

Remark 1. In this paper we employ a slight abuse of notation for sets and formulas characterizing those sets, i.e. Q denotes both a set $Q \subseteq \mathbb{R}^n$ and a formula Q of real arithmetic with free variables $x_1, \ldots, x_n$ which characterizes this set. In the case of sub-level sets, i.e. sets characterized by predicates of the form $B \leq 0$ where B is a real valued function in the (dependent) variables $x_1, \ldots, x_n$, we will write $B(\boldsymbol{x}) \leq 0$ to mean $B \leq 0$ is true in state $\boldsymbol{x} \in \mathbb{R}^n$, and will explicitly use the independent time variable t to write $B(\boldsymbol{x}(t)) \leq 0$ when we are interested in evaluating the predicate along a solution $\boldsymbol{x}(t)$ of a differential equation.

2.2 Safety Verification and Direct Methods

In continuous systems governed by ODEs, a common verification challenge lies in establishing *safety* in a given system, which requires showing that no state in some designated set of *unsafe* states is reachable by following the solutions to the system from some given set of initial configurations. More precisely:

Definition 1 (Safety in ODEs). *Given a system of ODEs* $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$ *with evolution constraint* $Q \subseteq \mathbb{R}^n$*, and the sets* Init $\subseteq \mathbb{R}^n$*,* Unsafe $\subseteq \mathbb{R}^n$ *of initial and unsafe states, respectively, the system is said to be* safe *if and only if:* $\forall\, \boldsymbol{x}_0 \in \text{Init}.\ \forall t \geq 0. \Big((\ \forall \tau \in [0, t].\ \boldsymbol{x}(\boldsymbol{x}_0, \tau)\ \in Q) \Rightarrow \boldsymbol{x}(\boldsymbol{x}_0, t) \notin \text{Unsafe} \Big)$.

The above is a *semantic* definition, since it explicitly involves the solutions $\boldsymbol{x}(t)$ of the system. The fact that exact solutions to non-linear ODEs are rarely available is a significant limitation, and was historically the principal driving force behind the development of the so-called *qualitative theory* of differential equations, which is concerned with proving properties about differential equations *directly*, i.e. without explicitly computing their solutions. Powerful methods, such as Lyapunov's *direct method* [26] for proving stability in ODEs, emerged out of this theory and have become standard tools in the field of dynamical systems and control (see e.g. [19,42,51]). The next section will give a comprehensive review of direct methods for solving the safety verification problem for continuous systems using existing notions of barrier certificates.

[3] i.e. as a *finite* expression in terms of polynomials and *elementary functions* that can be constructed using the usual arithmetic operations $+, -, \times, \div$, from $\exp, \sin, \cos$, and their inverses; this includes natural logarithms, nth roots, etc. (see [3, Ch. 4]).

3 Barrier Certificates

First introduced by Prajna and Jadbabaie [37], the method of barrier certificates works by exhibiting a real-valued *barrier* function B which serves to partition the state space into two disjoint regions, respectively containing the initial and the unsafe states of the system, and such that the trajectories of the system cannot leave the initial states into the region containing unsafe states. The most general principle was not elaborated explicitly in the original work [37], but is stated, e.g., in [11, §3] as the *principle of barrier certificates*. The semantic statement of this principle (reproduced below) is not in itself useful for verifying safety properties because it explicitly involves the solutions to the system of ODEs.

Lemma 1 (Safety with semantic barrier certificates). *Given a system of ODEs $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$, possibly with an evolution constraint $Q \subseteq \mathbb{R}^n$, a set of initial states* Init $\subseteq \mathbb{R}^n$*, and a set of unsafe states* Unsafe $\subseteq \mathbb{R}^n$*, if a differentiable (barrier) function $B : \mathbb{R}^n \to \mathbb{R}$ satisfies the following conditions, then safety of the system in the sense of Definition 1 follows trivially:*

1. $\forall\, \boldsymbol{x} \in \text{Unsafe}.\ B(\boldsymbol{x}) > 0$,
2. $\forall\, \boldsymbol{x}_0 \in \text{Init}.\ \forall\, t \geq 0.\Big(\, (\forall\, \tau \in [0,t].\ \boldsymbol{x}(\boldsymbol{x}_0, \tau) \in Q) \Rightarrow B(\boldsymbol{x}(\boldsymbol{x}_0, t)) \leq 0 \Big)$.

Fortunately, there are a number of ways in which one can establish whether or not a given function B has the properties required by the semantic principle stated in Lemma 1 *without* having to compute solutions. There are at present a number of different kinds of barrier certificates in the literature, which differ in the kinds of conditions they employ for ensuring the second requirement of the general principle in Lemma 1. We can broadly separate these into two classes: (**i**) those which essentially reduce to an application of the so-called *comparison principle*, and (**ii**) those explicitly based on reasoning about (positive) *invariant sets* [4]. In what follows, it is important to recall that *semi-definite programming* (SDP) and sum-of-squares (SOS) decomposition techniques (whose use to search for Lyapunov functions was pioneered by Parrilo [31]) provide a tractable search procedure only for certain kinds of barrier certificates.

3.1 Comparison System-based Barrier Certificates

Convex/weak. The original formulation in [37] is known as a *convex* [36,38] (also *weak* [45]) barrier certificate and imposes the following three formal requirements, which are sufficient to satisfy the conditions in Lemma 1 (we elide the $\boldsymbol{x}$-dependency in Unsafe, Init, Q, and B):

CBC 1. $\forall\, \boldsymbol{x} \in \mathbb{R}^n.\, (\text{Unsafe} \to B > 0)$,
CBC 2. $\forall\, \boldsymbol{x} \in \mathbb{R}^n.\, (\text{Init} \to B \leq 0)$,
CBC 3. $\forall\, \boldsymbol{x} \in \mathbb{R}^n.\, (Q \to B' \leq 0)$.

[4] i.e. sets of states that remain invariant under the flow of the system as time advances.

The above conditions ensure that the sub-level set $B \leq 0$ is a sound over-approximation of the set of states reachable from Init. If the evolution constraint Q, as well as Init and Unsafe, are all given by conjunctions of polynomial inequalities, one can formulate a search for polynomial $B \in \mathbb{R}[\boldsymbol{x}]$ as a semi-definite program by fixing some maximum degree for a symbolic polynomial *template* of B and using an SDP solver to obtain its monomial coefficients [37]. The convexity in the name refers to the set of functions B, since for any two functions $B, \tilde{B}$ that satisfy the requirements **CBC 1-3**, any convex combination $\alpha B + (1-\alpha)\tilde{B}$, where $\alpha \in [0,1]$, will also be a convex/weak barrier certificate satisfying the same requirements. It is precisely this convexity property which enables the use of SDP from convex optimization and makes barrier certificates of this kind interesting from a practical standpoint.

Exponential-type. So-called *exponential-type* barrier certificates [22] extend weak barrier certificates by generalizing the condition on the derivative of B in a way that maintains the convexity of the search space. These conditions are:

ETBC 1. $\forall \boldsymbol{x} \in \mathbb{R}^n.\, (\text{Unsafe} \rightarrow B > 0)$,
ETBC 2. $\forall \boldsymbol{x} \in \mathbb{R}^n.\, (\text{Init} \rightarrow B \leq 0)$,
ETBC 3. $\forall \boldsymbol{x} \in \mathbb{R}^n.\, (Q \rightarrow B' \leq \lambda B)$, for some fixed $\lambda \in \mathbb{R}$.

Since these conditions also define a convex set, one can search for barrier certificates of this kind using semi-definite programming for fixed $\lambda \in \mathbb{R}$ and bounded degree polynomial templates of B, analogously to the weak/convex barrier certificates. To use this method, one is required to supply a value for λ: with $\lambda = 0$ one recovers the conditions for convex barrier certificates; the choice of $\lambda > 0$ or $\lambda < 0$ was observed to have significant practical impact on the barrier functions that one can generate using semi-definite programming [22, §3.1].

General. More recently, so-called *general* barrier certificates were reported in [11] and generalize the condition used in exponential-type barrier certificates yet further by allowing the right-hand side of the differential inequality to be a (potentially non-linear) univariate *function* of the barrier function itself. The conditions are as follows:

GBC 1. $\forall \boldsymbol{x} \in \mathbb{R}^n.\, (\text{Unsafe} \rightarrow B > 0)$,
GBC 2. $\forall \boldsymbol{x} \in \mathbb{R}^n.\, (\text{Init} \rightarrow B \leq 0)$,
GBC 3. $\forall \boldsymbol{x} \in \mathbb{R}^n.\, (Q \rightarrow B' \leq \omega(B))$,
GBC 4. $\forall t \geq 0.\ b(\boldsymbol{x}(t)) \leq 0$, where $b(\boldsymbol{x}(t)) : \mathbb{R} \rightarrow \mathbb{R}$ is some continuously differentiable function such that: (**i**) $b(\boldsymbol{x}(0)) \leq 0$, and (**ii**) $b' = \omega(b)$.

Barrier certificates satisfying the above requirements will *not* form a convex set. To use this method of verification in practice, one is first required to supply some *fixed* univariate function ω, e.g. one could take $\omega(b) = -b + b^2$, and make sure that the solutions $b(t)$ to the differential equation $b' = \omega(b)$ exist and remain non-positive for all time, i.e. $\forall t \geq 0.\ b(t) \leq 0$, from the initial conditions (at which b is required to be non-positive). One may be forgiven for thinking these conditions obscure and unmotivated at first; in the next section we will elucidate how these conditions in fact amount to a simple exercise in applying the comparison principle in the theory of ODEs to safety verification.

3.2 Comparison Systems

Informally, one may think of a *comparison system* for a given system of ODEs as being another system of ODEs that (**i**) is in some sense simpler to analyse and (**ii**) enables one to establish properties of the original system of ODEs. The idea behind the *comparison principle* is that by establishing some desired property of the comparison system (which is hopefully not as difficult), one is able to draw the conclusion that this property also holds in the original system.

Remark 2. A comparison system may be described as a certain *abstraction* of a system of ODEs by another system.

The comparison principle emerged as a coherent technique in the theory of ODEs and applied mathematics in the middle of the twentieth century. It was employed by numerous authors, e.g. by Conti [10] to study existence of solutions of ODEs, and by Brauer [6] to study stability using comparison systems as a way of generalizing the classic requirement $V' \leq 0$ on the derivative of Lyapunov functions V. For demonstrating stability of some n-dimensional system of ODEs $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$, if one has a *positive definite* function $V : \mathbb{R}^n \to \mathbb{R}$ that satisfies a more general differential inequality

$$V' \leq \omega(V)\,,$$

where $\omega : \mathbb{R} \to \mathbb{R}$ is an appropriately chosen scalar function, one can construct a (scalar) comparison system by introducing a fresh variable (e.g. v; really a function of time $v(t)$) and replacing the inequality by an equality, thus obtaining a *one-dimensional* first order system of ODEs, i.e. the differential *equation*

$$v' = \omega(v)\,.$$

The comparison principle relates properties of the solutions $v(t)$ of this one-dimensional system to properties of the solutions $\boldsymbol{x}(t)$ of the original n-dimensional system $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$ by using solutions $V(t)$, i.e. $V(\boldsymbol{x}(t))$, to the differential inequality. For example, one use of the comparison principle in the theory of ODEs is to infer stability of the original system by establishing stability of the one-dimensional comparison system (see e.g. Brauer [7], Habets and Peiffer [18, §2]).[5] The comparison principle hinges on an appropriate *comparison theorem*, which establishes the relationship between the solutions of the one-dimensional system to the solutions of the differential inequality. Below we state a particularly useful comparison theorem (a corollary to the comparison theorem in Walter [49, Ch. II, §IX]) which we shall use in later sections.

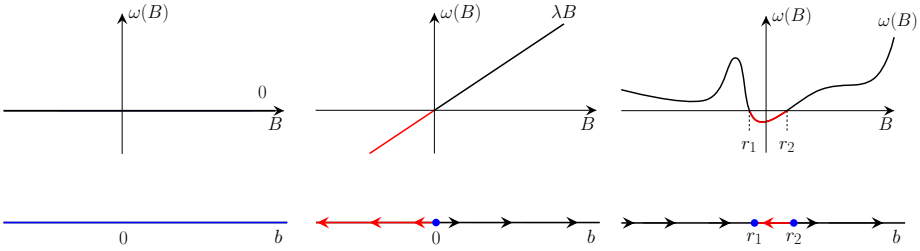
Theorem 1 (Scalar comparison theorem). *Let $B(t)$ and $b(t)$ be real valued functions differentiable on some real interval $[0, T]$. If $B' \leq \omega(B)$ and $b' = \omega(b)$ holds on $[0, T]$ for some locally Lipschitz continuous function ω and if $B(0) = b(0)$, then for all $t \in [0, T]$ one has $B(t) \leq b(t)$.*

[5] The comparison principle is described in some detail in [48], and also in a number of textbooks, e.g. in [42, Ch. II §3, Ch. IX], [51, §1.4], [19, Theorem 4.16].

The comparison theorem above ensures that the solutions $b(t)$ to the comparison system of *ODEs* act as upper bounds on the solutions $B(t)$ to the corresponding system of differential *inequalities*. We note in passing that the above theorem also holds more generally for ω with explicit time-dependence, i.e. $\omega(t, B)$.

3.3 Comparison Principle Interpretation of Barrier Certificates

The original formulation of convex barrier certificates in [37] can be interpreted using the comparison principle viewpoint as the trivial case in which the differential inequality $B' \leq 0$ (i.e. ω being the constant function 0) leads to the comparison system given by $b' = 0$, in which there is no motion. The initial states in the comparison system are defined as $b_{\text{Init}} = \{k \in \mathbb{R} \mid B(\boldsymbol{x}) = k, \boldsymbol{x} \in \text{Init}\}$; analogously, the unsafe states are $b_{\text{Unsafe}} = \{k \in \mathbb{R} \mid B(\boldsymbol{x}) = k, \boldsymbol{x} \in \text{Unsafe}\}$. Since the value of B at unsafe states is required to be greater than its values at initial states by conditions **CBC 1-2**, the safety property follows because the solutions of the comparison system $b(t)$ bound the solutions $B(t)$ from above and cannot increase. Figure 1a illustrates this comparison system. Since every point is an equilibrium and $b(0) \leq 0$ is required for all initial states in b_{Init}, and $b(t) = b(0) \leq 0$ will hold for all $t \geq 0$, the comparison system cannot evolve into a potentially unsafe state $b(\tau) > 0$ (i.e. $b(\tau) \in b_{\text{Unsafe}}$) for any $\tau > 0$. As a consequence, $B(\boldsymbol{x}(t)) \leq 0$ will hold for all $\boldsymbol{x}(0) \in \text{Init}$ for *as long as solutions are defined in the original system*, by Theorem 1, satisfying the requirements in Lemma 1.



(a) Constant (zero) **(b)** Linear **(c)** Non-linear

Fig. 1: Right-hand sides of differential inequalities $B' \leq \omega(B)$ shown above. Their corresponding scalar comparison systems $b' = \omega(b)$ are shown below as vector fields on the real line. The motion in these comparison systems is directed "to the right" whenever ω is above zero, and "to the left" when it is below; equilibria are those points where ω evaluates to zero, i.e. the real roots of ω.

The *exponential-type* [22] and *general* [11] barrier certificates can also be easily understood as special instances of applying the comparison principle. With the former, one has a *linear* differential inequality $B' \leq \lambda B$, for some $\lambda \in \mathbb{R}$, which leads to the simple linear comparison system $b' = \lambda b$ (i.e. $\omega(b) = \lambda b$) defined on the real line (illustrated in Fig. 1b.) As before, by showing unreachability of unsafe states b_{Unsafe} from the initial states b_{Init} in the comparison

system, Theorem 1 allows one to soundly conclude the safety property in the original system provided that $B(\boldsymbol{x}) \leq 0$ for all initial states and $B(\boldsymbol{x}) > 0$ for all unsafe states, as required by **ETBC 1-2** (cf. Section 3.1). We note also that the solutions $b(t)$ in the comparison system are defined for all $t \geq 0$, since the system is linear, and the bounding property stated in the comparison theorem will hold for as long as solutions are defined in the original system.

The general barrier certificates reported in [11] simply allow for a *non-linear* function ω of B in the right-hand side of the differential inequality, i.e. $B' \leq \omega(B)$. This leads to a non-linear scalar comparison system $b' = \omega(b)$ which can exhibit more interesting flows on the real line (as shown in Fig. 1c.) The principle, however, is exactly the same: the unreachability of the unsafe states from the initial states *in the comparison system* (e.g. the one-dimensional flow shown in Fig. 1c) implies the safety property in the original system. However, since ω can be non-linear, it also becomes important to ensure that solutions from the initial states in the comparison systems do not escape to infinity before they do in the original system. Thus, the last requirement of general barrier certificates **GBC 4** is essentially requiring one to explicitly supply an appropriate comparison system.[6]

3.4 Invariant Set-based Barrier Certificates

An alternative way of ensuring condition (*2.*) in Lemma 1 is by directly requiring the *continuous invariance* property of the entire sub-level set of the barrier function, i.e. $B \leq 0$, and explicitly requiring that all initial states lie inside this sub-level set, i.e. $\forall\, \boldsymbol{x} \in \text{Init}.\ B(\boldsymbol{x}) \leq 0$. The set $\{\boldsymbol{x} \in \mathbb{R}^n \mid B(\boldsymbol{x}) \leq 0\}$ is a *continuous invariant* under constraint Q if the system cannot continuously evolve from a state $\boldsymbol{x} \in \mathbb{R}^n$ satisfying $B(\boldsymbol{x}) \leq 0$ into a state $\boldsymbol{x}(t)$ satisfying $B(\boldsymbol{x}(t)) > 0$, while respecting the constraint Q. Semantically, this amounts to showing that the following holds:

$$\forall \boldsymbol{x}_0 \in \mathbb{R}^n.\, (B(\boldsymbol{x}_0) \leq 0 \Rightarrow (\forall t \geq 0.\, (\forall\, \tau \in [0,t].\boldsymbol{x}(\boldsymbol{x}_0, \tau) \in Q) \Rightarrow B(\boldsymbol{x}(\boldsymbol{x}_0, t)) \leq 0))$$

Notice the subtle difference of this requirement to that in Lemma 1, which does *not* require the sub-level set $B \leq 0$ to be a continuous invariant.

Remark 3. Continuous invariance is a generalization of the notion of *positive invariance* used in control (e.g. see [4]); its greater generality is due to an appropriate handling of evolution constraints. We note that the problem of checking whether a given *semi-algebraic set* (i.e. a set described by a finite Boolean combination of polynomial equations and inequalities) defines a continuous invariant

[6] For the interested reader, we note that in [11, Theorem 1], the barrier function B is denoted by φ, the function ω is denoted ψ, and the variable b of the comparison system denoted by θ. Indeed, the final condition (5) in [11, Theorem 1] simply requires that the solution of the comparison system $b' = \omega(b)$ (i.e. $\theta' = \psi(\theta)$ using notation employed in the article) does not become positive as time (denoted by ξ) advances. No reference to the comparison principle is made in that work.

under the flow of a polynomial first-order system of ODEs is decidable (a remarkable result due to Liu, Zhan and Zhao [25]). However, *searching* for continuous invariants – even those of restricted form, such as sub-level sets of polynomial functions – using tools such as real quantifier elimination is impractical due to the time complexity of existing algorithms (e.g. partial CAD [9]).

An example of barrier certificate conditions based on continuous invariance is the so-called *strict* [45] (also known as *non-convex* [36,38]) barrier certificate, which imposes the following formal requirements:

SBC 1. $\forall \boldsymbol{x} \in \mathbb{R}^n.\, (\text{Unsafe} \rightarrow B > 0)$,
SBC 2. $\forall \boldsymbol{x} \in \mathbb{R}^n.\, (\text{Init} \rightarrow B \leq 0)$,
SBC 3. $\forall \boldsymbol{x} \in \mathbb{R}^n.\, (Q \wedge B = 0 \rightarrow B' < 0)$.

In the last condition, the strict inequality $B'(\boldsymbol{x}) < 0$ is only required to hold at the roots of the function B, i.e. for all $\boldsymbol{x} \in Q$ such that $B(\boldsymbol{x}) = 0$. This condition[7] is in practice less conservative than that used in convex barrier certificates, since it does not impose a requirement on the derivative everywhere in the evolution constraint Q. However, the set of functions B satisfying this condition is no longer convex and as a result one may no longer directly apply semi-definite programming to search for this type of barrier functions. An alternative *iterative* search method for strict barrier certificates was explored in [37,36] and was also used to search for (likewise non-convex) general barrier certificates [11, §4].

We note that continuous invariance is the main principle underlying safety verification problems. In fact, scalar comparison systems are essentially means of generating sufficient continuous invariants to solve the problem at hand. For example, in a one-dimensional comparison system $b' = \omega(b)$, obtained from the differential inequality $B' \leq \omega(B)$, for any $k \in \mathbb{R}$ such that $\omega(k) < 0$ it is guaranteed that $B'(\boldsymbol{x}) < 0$ holds at all states $\boldsymbol{x}$ satisfying $B(\boldsymbol{x}) = k$.[8] This property is sufficient to conclude that the sub-level set $B \leq k$ is a continuous invariant in the original n-dimensional system. For example, in the non-linear system $b' = \omega(b)$ illustrated in Fig. 1c, any $k \in (r_1, r_2)$ can be used to extract such an invariant; for the linear example in Fig. 1b one may take any $k < 0$.

4 From Scalar to Vector Comparison Systems

A multi-dimensional version of Lyapunov functions, known as vector Lyapunov functions, was first introduced in 1962 by Bellman [2], using the more general *vector* comparison principle.[9] Below we briefly review this development.

[7] Note that the inequality needs to be *strict*; the original formulation of non-convex barrier certificates in [37] featured a non-strict inequality $B' \leq 0$, which leads to *unsoundness* in certain degenerate cases. A finite number of inequalities involving higher-order derivatives of B can be used instead to soundly establish continuous invariance of the sub-level set $B \leq 0$, following the result reported in [25].

[8] Each point k on the real line in a scalar comparison system $b' = \omega(b)$ corresponds to $\{\boldsymbol{x} \in \mathbb{R}^n \mid B(\boldsymbol{x}) = k\}$ in the original state space.

[9] The technique itself was also independently developed by V. M. Matrosov [27], who also published his research in 1962, shortly after Bellman.

4.1 Vector Lyapunov Functions

The main idea behind vector Lyapunov functions is as follows: instead of searching for a single Lyapunov function $V : \mathbb{R}^n \to \mathbb{R}$, one searches for a *vector* function $\boldsymbol{V} : \mathbb{R}^n \to \mathbb{R}^m$, where $\boldsymbol{V}(\boldsymbol{x})$ is a vector $(V_1(\boldsymbol{x}), \ldots, V_m(\boldsymbol{x}))$ and $V_1, \ldots, V_m$ are scalar functions, such that for each $i = 1, \ldots, m$ one has $V_i' \leq \omega_i(V_1, \ldots, V_m)$, where $\omega_i : \mathbb{R}^m \to \mathbb{R}$. In the classic (scalar) Lyapunov case, i.e. the special case where $m = 1$, if one had $V' \leq \omega(V)$, with positive definite V and some appropriate scalar function ω, one could use the comparison principle to infer stability by showing this property in the scalar comparison system $v' = \omega(v)$ (e.g. see Brauer [7]). With vector Lyapunov functions one is instead interested in analysing the *vector* comparison system $\boldsymbol{v}' = \boldsymbol{\omega}(\boldsymbol{v})$, obtained from a *system* of differential inequalities $\boldsymbol{V}' \leq \boldsymbol{\omega}(\boldsymbol{V})$, where $\boldsymbol{\omega} : \mathbb{R}^m \to \mathbb{R}^m$. There is, however, an (unpleasant) extra requirement: in order to conclude stability of the original system from the stability of the vector comparison system, the vector function $\boldsymbol{\omega}$ needs to be *quasi-monotone increasing*.

Definition 2. *A function $\boldsymbol{\omega} : \mathbb{R}^m \to \mathbb{R}^m$ is said to be* quasi-monotone increasing *on a set $U \subseteq \mathbb{R}^m$ if $\omega_i(\boldsymbol{x}) \leq \omega_i(\boldsymbol{y})$ for all $i = 1, \ldots, m$ and all $\boldsymbol{x}, \boldsymbol{y} \in U$ such that $x_i = y_i$, and $x_k \leq y_k$ for all $k \neq i$.*

In particular, univariate functions (case $m = 1$) are always quasi-monotone increasing by definition since the required inequality holds trivially ($x = y$ implies $\omega(x) \leq \omega(y)$). In the vector case, a linear multivariate function $\boldsymbol{\omega}(\boldsymbol{x}) = A\boldsymbol{x}$ is quasi-monotone increasing if and only if all the off-diagonal entries of the $m \times m$ real matrix A are non-negative (e.g. see [48]). Such a matrix is said to be *essentially non-negative*, *quasi-positive*, or a *Metzler matrix*.

Remark 4. Clearly, vector comparison systems are only interesting in practice insofar as they are easier to analyse than the original system. For stability analysis with vector Lyapunov functions, linear vector comparison systems of the form $\boldsymbol{v}' = \omega(\boldsymbol{v}) = A\boldsymbol{v}$, where A is an appropriate essentially non-negative $m \times m$ real matrix, are easier to work with than non-linear vector comparison systems. One may easily create linear quasi-monotone increasing vector comparison systems $\boldsymbol{v}' = A\boldsymbol{v}$ that are stable *a priori* and then search for vector Lyapunov functions that satisfy the corresponding system of differential inequalities $\boldsymbol{V}' \leq A\boldsymbol{V}$; see [17]. Indeed, Bellman's approach [2] only focused on linear vector comparison systems. The general method of vector Lyapunov functions has been applied extensively to study stability of non-linear systems; the interested reader is invited to consult [28,24], and [19, §4.11] for a more thorough overview.

4.2 Vector Comparison Principle

Quasi-monotonicity of the right-hand side in the comparison system $\boldsymbol{b}' = \boldsymbol{\omega}(\boldsymbol{b})$ ensures that its solutions $\boldsymbol{b}(t)$ majorize (bound above component-by-component) the solutions $\boldsymbol{B}(t)$ to the system of differential inequalities $\boldsymbol{B}' \leq \boldsymbol{\omega}(\boldsymbol{B})$, analogously to the scalar comparison case in Theorem 1. Following [2], we state (in

Theorem 2) a vector comparison theorem which enables one to employ the *vector comparison principle* for the practically interesting case where $\boldsymbol{\omega}$ is *linear* (for a proof, see e.g. [1, Ch. 4, §6, Theorem 4]).

Theorem 2 (Linear vector comparison theorem). *For a given system of ODEs $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$ and an essentially non-negative matrix, $A \in \mathbb{R}^{m\times m}$, if $\boldsymbol{B} = (B_1, B_2, \ldots, B_m)$ satisfies the system of differential inequalities $\boldsymbol{B}' \leq A\boldsymbol{B}$, then for all $t \geq 0$ the inequality $\boldsymbol{B}(t) \leq \boldsymbol{b}(t)$ holds component-wise, where $\boldsymbol{b}(t)$ is the solution to the comparison system $\boldsymbol{b}' = A\boldsymbol{b}$, $\boldsymbol{B}(t)$ is any solution to the system of differential inequalities, and $\boldsymbol{b}(0) = \boldsymbol{B}(0)$.*

The above vector comparison theorem can be generalized to the non-linear case where $\boldsymbol{B}' \leq \boldsymbol{\omega}(\boldsymbol{B})$ and $\boldsymbol{b}' = \boldsymbol{\omega}(\boldsymbol{b})$, provided that the non-linear vector function $\boldsymbol{\omega} : \mathbb{R}^m \to \mathbb{R}^m$ is quasi-monotone increasing. For a precise statement and proof see e.g. [19, §4.13], [49, Ch III, §XII], [23, §4.1].

4.3 Safety with Vector Barrier Certificates

The main interest in pursuing the vector comparison approach is to relax the conditions on each individual function component of the vector. The hope is that it is easier to search for functions that satisfy less rigid criteria. It is natural to ask whether one might profitably apply vector comparison systems to safety verification. We begin by stating a useful lemma.

Lemma 2. *If $A \in \mathbb{R}^{m\times m}$ is an essentially non-negative matrix, then for any initial value $\boldsymbol{b}_0 \leq \boldsymbol{0}$, the solution $\boldsymbol{b}(t)$ to the linear system $\boldsymbol{b}' = A\boldsymbol{b}$ is such that $\boldsymbol{b}(t) \leq \boldsymbol{0}$ for all $t \geq 0$.*

Proof. This follows from the fact that solutions to the linear system $\boldsymbol{b}' = A\boldsymbol{b}$ from an initial value $\boldsymbol{b}_0 \leq \boldsymbol{0}$ are given by $\boldsymbol{b}(t) = e^{At}\boldsymbol{b}_0$, and all the elements of the matrix exponential e^{At} are non-negative for all $t \geq 0$ if and only if A is essentially non-negative (e.g. see proof of Theorem 4 in [1, Ch. 4, §6]). □

Theorem 3. *Given $\boldsymbol{x}' = f(\boldsymbol{x})$, Q,* Init*, and* Unsafe *as before, an m-vector of continuously differentiable functions $\boldsymbol{B} = (B_1, B_2, \ldots, B_m)$ and some essentially non-negative $m \times m$ matrix A, if the following conditions hold, then the safety property of the system is guaranteed:*

VBC$_\wedge$1. $\forall\, \boldsymbol{x} \in \mathbb{R}^n.\, (\text{Init} \to \bigwedge_{i=1}^m B_i \leq 0)$,
VBC$_\wedge$2. $\forall\, \boldsymbol{x} \in \mathbb{R}^n.\, (\text{Unsafe} \to \bigvee_{i=1}^m B_i > 0)$,
VBC$_\wedge$3. $\forall\, \boldsymbol{x} \in \mathbb{R}^n.\, (Q \to \boldsymbol{B}' \leq A\boldsymbol{B})$.

Proof. Elementary, since the states satisfying $\bigwedge_{i=1}^m B_i(\boldsymbol{x}) \leq 0$ include all the initial states, no unsafe states, and majorizing solutions $\boldsymbol{b}(t)$ of the comparison system $\boldsymbol{b}' = A\boldsymbol{b}$ cannot take on positive values in any component for any time $t \geq 0$ (by Lemma 2). Thus, $\boldsymbol{B}(t) \leq \boldsymbol{0}$ for all $t \geq 0$ (by Theorem 2). □

For any given matrix $A \in \mathbb{R}^{m\times m}$ if the m-vectors $\boldsymbol{B} = (B_1, B_2, \ldots, B_m)$ and $\tilde{\boldsymbol{B}} = (\tilde{B}_1, \tilde{B}_2, \ldots, \tilde{B}_m)$ satisfy conditions $\mathbf{VBC}_\wedge\mathbf{1}$ and $\mathbf{VBC}_\wedge\mathbf{3}$, then so does their convex combination $\widehat{\boldsymbol{B}} = \alpha\boldsymbol{B} + (1-\alpha)\tilde{\boldsymbol{B}}$, where $\alpha \in [0,1]$. The latter holds since $\widehat{\boldsymbol{B}}' = \alpha\boldsymbol{B}' + (1-\alpha)\tilde{\boldsymbol{B}}' \leq \alpha A\boldsymbol{B} + (1-\alpha)A\tilde{\boldsymbol{B}} = A\widehat{\boldsymbol{B}}$. Unfortunately, the condition $\mathbf{VBC}_\wedge\mathbf{2}$, while intuitive and desirable, leads to non-convexity. To recover convexity one may write down a stronger condition as follows.[10]

Corollary 1. *Given $\boldsymbol{x}' = f(\boldsymbol{x})$, Q,* Init*,* Unsafe*, $\boldsymbol{B}$ and A as before, if for some $i^* \in \{1,\ldots,m\}$ the following conditions hold, then the safety property of the system is guaranteed:*

VBC 1. $\forall\, \boldsymbol{x} \in \mathbb{R}^n.\, (\text{Init} \rightarrow \bigwedge_{i=1}^{m} B_i \leq 0)$,
VBC 2. $\forall\, \boldsymbol{x} \in \mathbb{R}^n.\, (\text{Unsafe} \rightarrow B_{i^*} > 0)$,
VBC 3. $\forall\, \boldsymbol{x} \in \mathbb{R}^n.\, (Q \rightarrow \boldsymbol{B}' \leq A\boldsymbol{B})$.

Notice that a barrier function B_{i^*} satisfying the conditions **VBC 1-3** satisfies the requirement of the semantic principle in Lemma 1, but its sub-level set $B_{i^*} \leq 0$ need *not* be a continuous invariant (unlike in scalar barrier certificates).

Remark 5. Vector barrier certificates can also be defined using a non-linear vector differential inequality $\boldsymbol{B}' \leq \boldsymbol{\omega}(\boldsymbol{B})$, where $\boldsymbol{\omega}$ is some non-linear quasi-monotone increasing function. This, however, would lead to the convexity property being lost and would also require the solutions to the comparison system to be of sufficient duration in order to ensure soundness. This approach does not appear to be at all promising from a practical standpoint, but provides the most general notion for vector barrier certificates.

Theorem 4 (Deductive power). *Every polynomial convex or 'exponential-type' barrier certificate is (trivially) a vector barrier certificate satisfying the conditions* $\mathbf{VBC}_\wedge$**1-3** *(or* **VBC 1-3***). The converse is false, i.e. there exist polynomial vector barrier certificates sufficient for proving certain safety properties where a scalar barrier certificate does not exist.*

Proof. For the non-trivial part, consider the system $x_1' = x_2,\ x_2' = x_1$. Suppose that the initial states in this system satisfy the formula $x_1 \leq 0 \wedge x_2 \leq 0$ and the unsafe states satisfy $x_1 > 0$. If we take $B_1 = x_1$ and $B_2 = x_2$ then, since $B_1' = x_1'$ and $B_2' = x_2'$, the following system of differential inequalities is satisfied: $B_1' \leq B_2,\ B_2' \leq B_1$, which is equivalently written down as a linear system of differential inequalities with an essentially non-negative matrix: $\begin{pmatrix} B_1' \\ B_2' \end{pmatrix} \leq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$. The vector (B_1, B_2) satisfies all the conditions in Theorem 3 and Corollary 1 with $i^* = 1$ (note that the comparison system is in this case equivalent to the original essentially non-negative system in the new variables b_1, b_2). However, there is *no* polynomial function B that can act as a scalar barrier certificate. For contradiction, assume there is such a (continuous) B. The verification problem requires that $B(x_1, x_2)$ evaluates to 0 whenever $x_1 = 0 \wedge x_2 \leq 0$

[10] Naturally, for the vectorial formulation to be interesting, *none* of the functions $B_1, \ldots, B_m$ should be (scalar) barrier certificates in their own right.

holds, therefore the univariate polynomial $B(0, x_2)$ has infinitely many real roots and is therefore the zero polynomial, from which we conclude that $B(x_1, x_2)$ has real roots on the entire line $x_1 = 0$. The set $B(x_1, x_2) \leq 0$ thus cannot be a continuous invariant (and B is therefore not a convex or an 'exponential-type' barrier certificate) because any trajectory initialized from $x_1 = 0 \wedge x_2 > 0$ enters the unsafe set where the function B is required to be positive. □

Vector barrier certificates can also exist with lower polynomial degrees than is possible with scalar barrier certificates. To take an example, consider the verification problem (with $x_1' = x_2, x_2' = x_1$, as that in the above proof) illustrated in Fig. 2, where the initial states are represented by the green rectangle $[-7, -\frac{1}{2}] \times [-4, -\frac{3}{2}]$ and the unsafe states by the red circle of radius $\sqrt{2}$ centred at $(-3, 2)$. The vector barrier certificate $(B_1, B_2) = (x_1, x_2)$ is *linear* in each component (i.e. has polynomial degree 1) and satisfies all the conditions required by Theorem 3 and Corollary 1. However, there is no *linear/affine* function that is a *scalar* barrier certificate for this problem because there is no half-plane that includes all the initial states, no unsafe states, and is invariant under the dynamics (i.e. such that trajectories cannot escape). This holds because any line separating the two sets cannot have slope 1 or -1, which are the only possible values for slope of a linear function defining an invariant half-plane in this system.

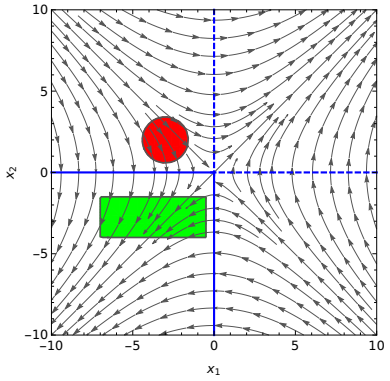


Fig. 2: Vector barrier certificate $(B_1, B_2) = (x_1, x_2)$.

As with barrier certificates based on scalar comparison systems, one is able to extract invariant sets from the vector generalization; the class of invariants one can extract is, in fact, richer. For example, given a vector differential inequality $\boldsymbol{B}' \leq A\boldsymbol{B}$, where A is essentially non-negative, one may extract a *conjunctive* invariant $\bigwedge_{i=1}^{m} B_i \leq 0$. Furthermore, the constituent conjuncts $B_i \leq 0$ of such a conjunction need not define invariant sets in their own right.

4.4 Generating Vector Barrier Certificates using SDP

Generation of vector barrier certificates based on Corollary 1 using sum-of-squares optimization can be performed with a straightforward generalization of corresponding techniques for scalar barrier certificates [37]. Let us assume that the sets $\mathrm{Init}, \mathrm{Unsafe}, Q$ are characterized by the conjunctions: $\bigwedge_{i=1}^{a} I_i \geq 0$, $\bigwedge_{i=1}^{b} U_i \geq 0$, and $\bigwedge_{i=1}^{c} Q_i \geq 0$ respectively, where I_i, U_i, Q_i are polynomials. Fix a small, positive constant $\epsilon > 0$, and fix an essentially non-negative $m \times m$ matrix A. Let B_i be template polynomials, and $\sigma_{I_{i,j}}, \sigma_{U_j}, \sigma_{Q_{i,j}}$ be sum-of-squares template polynomials.[11] The following is a sum-of-squares optimization problem

[11] Template polynomials are polynomials of fixed degree, but with symbolic coefficients. Sum-of-squares optimization searches for appropriate values for these coefficients.

for size m vector barrier certificates $B_1, B_2, \ldots, B_m$, with $i^* \in \{1, \ldots, m\}$:

$$-B_i - \Sigma_{j=1}^{a} \sigma_{I_{i,j}} I_j \geq 0 \text{ for all } i = 1, 2, \ldots, m \qquad (\textbf{VBC 1})$$

$$B_{i^*} - \Sigma_{j=1}^{b} \sigma_{U_j} U_j - \epsilon \geq 0 \qquad (\textbf{VBC 2})$$

$$\Sigma_{j=1}^{m} A_{ij} B_j - B_i' - \Sigma_{j=1}^{c} \sigma_{Q_{i,j}} Q_j \geq 0 \text{ for all } i = 1, 2, \ldots, m \qquad (\textbf{VBC 3})$$

The three optimization constraints ensure that the corresponding **VBC** condition holds for the resulting B_i. We show an example of barrier certificates that can be generated by this method.

Example 1 (Linear barriers). Consider the following 3-dimensional system:

$$\begin{aligned} x_1' &= 2x_1 + x_2 + 2x_3 - x_1^2 + x_1 x_3 - x_3^2, \\ x_2' &= -2 + x_1 - x_2 - x_2^2, \\ x_3' &= -2 - x_2 - x_3 + x_1^2 - x_1 x_3, \end{aligned}$$

where Init is defined by $\bigwedge_{i=1}^{3} -x_i \geq 0$, Unsafe by $x_1 + x_2 + x_3 \geq 1$, and there is no evolution constraint. Using the matrix $A = \left(\begin{smallmatrix} 0 & 1 & 2 \\ 1 & -1 & 0 \\ 1 & 0 & 1 \end{smallmatrix}\right)$, $i^* = 1$, and the sum-of-squares solver SOSTOOLS [30], we obtain the following *true* vector barrier certificate by manually tweaking the floating-point coefficients returned by the solver. [12] Observe that neither $B_1 \leq 0$ nor $B_2 \leq 0$ define invariant sets.

$$\begin{aligned} B_1 &= (365x_1 + 365x_2 + 365x_3 - 60)/100, \\ B_2 &= (175x_1 + 180x_2 + 100x_3 - 160)/100, \\ B_3 &= (460x_1 + 155x_2 + 270x_3 - 250)/100. \end{aligned}$$

Alternatives to SDP There exist a number of alternatives to semi-definite programming which can be employed to generate vector barrier certificates. For example, constraint programming techniques for solving inequality constraints over the reals were studied by Ratschan [39] and applied to search for Lyapunov-like functions [40]. Computation of strict barrier certificates using interval constraint satisfaction techniques was later investigated by Bouissou [5], Djaballah, et al. [12]. Another intriguing alternative studied by Sankaranarayanan et al. [44] (and later Yang et al. [50]) is the linear relaxation approach based on so-called Handelman representations [21] (which allow the use of linear programming to establish the positive semi-definite property of a polynomial over a compact convex polyhedron); this technique was observed to be much less prone to numerical errors than methods based on interior-point solvers. These approaches, however, are limited to problems with bounded domains.

[12] Numerical inaccuracies plague SOS-based approaches to generating all types of barrier certificates and render most generated barrier certificates subtly incorrect. Mitigating this issue is an important, but orthogonal, question that has been investigated elsewhere [32,43].

5 Limitations and Outlook

The trade-off in employing the vector comparison principle comes down to the following: the relaxation of requirements on each individual component of the vector function comes at the price of increased complexity (due to increased dimension) of the comparison system. Already in the scalar ($m = 1$) special case corresponding to the 'exponential-type' barrier certificate, the choice of the single coefficient λ in the comparison system $b' = \lambda b$ was observed to impact the results [22]. Our approach provides more flexibility but also requires more choices in the essentially non-negative matrix A. While we do not yet have general heuristics, a possible strategy for picking alternative matrices A when the initial choice fails is to change the values of the matrix in a way that changes the qualitative behaviour of the trajectories of the comparison system $\boldsymbol{b}' = A\boldsymbol{b}$ (i.e. changes the structure of the *phase portrait*; see e.g. [3, Ch. 5, pp. 147–149]). It is clear that in practice one should always attempt to find a scalar barrier certificate ($m = 1$) first and proceed to increase the dimension m of the comparison system if the search was unsuccessful (for example due to numerical inaccuracies when polynomials of high degree are involved [11]). Vector barrier certificates could alleviate some of these problems because they allow us to reduce the polynomial degree of the barriers. An empirical study of this trade-off (and indeed of existing scalar notions of barrier certificates) falls outside of the scope of this work and would require a large set of verification benchmarks to be objective, but presents an interesting direction for further investigation.

We remark, however, that scalar comparison systems, even when they are insufficient to prove the safety property at hand, may reveal structure in the dynamics which could help in constructing an appropriate comparison system for vector barrier certificates. The proposition below is a direct consequence of a property of essentially non-negative (Metzler) matrices, akin to the Perron-Frobenius theorem for non-negative matrices which establishes the existence of an eigenvector in the non-negative orthant (e.g. see [46, Proposition 1]).

Proposition 1. *For a given system of ODEs $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$ and an essentially non-negative matrix, $A \in \mathbb{R}^{m\times m}$, if $\boldsymbol{B} = (B_1, B_2, \ldots, B_m)$ satisfies the system of differential inequalities $\boldsymbol{B}' \leq A\boldsymbol{B}$, then there exists a scalar function g and a scalar μ such that $g' \leq \mu g$.*

Proof. Since A is Metzler, then its transpose, A^T, is also a Metzler matrix. Let $\boldsymbol{u}$ be an eigenvector of A^T in the non-negative orthant with eigenvalue μ, i.e. $A^T\boldsymbol{u} = \mu\boldsymbol{u}$. Then, the scalar product $g := \boldsymbol{u} \cdot \boldsymbol{B}$ satisfies the scalar comparison inequality: $g' = \boldsymbol{u} \cdot \boldsymbol{B}' \leq \boldsymbol{u} \cdot (A\boldsymbol{B}) = (A^T\boldsymbol{u}) \cdot \boldsymbol{B} = (\mu\boldsymbol{u}) \cdot \boldsymbol{B} = \mu g$. The inequality is justified since all the components of the vector $\boldsymbol{u}$ are non-negative. □

The (real) eigenvalue μ is in fact the *dominant eigenvalue* (also called the *spectral abscissa*) of A: it is the maximum of the real parts of all the eigenvalues of A which coincides with the Perron-Frobenius root of A if A is non-negative. As a consequence, if a linear scalar comparison system cannot be found for a given scalar λ, one can rule out Metzler matrices with dominant eigenvalue below λ.

6 Related Work

In [11], Dai *et al.* explored an approach for combining more than one barrier certificate in order to prove safety in examples where a single barrier certificate could not be found (see [11, Lemmas 3 and 4]). However, these so-called *combined barrier certificates* only use the scalar variant of the comparison principle, i.e. for each barrier function B_i, a differential inequality of the form $B_i' \leq \omega_i(B_i)$ is considered, where $\omega_i : \mathbb{R} \to \mathbb{R}$ is a *univariate* analytic function, rather than a *multivariate* quasi-monotone increasing function, as we do in the vector barrier certificate framework. The way combined barrier certificates are constructed in [11] is closely related to the principle of *differential cuts* (DC), which was explored previously [33,15]. Platzer and Clarke [34] investigated ways of automatically generating *differential invariants*, which lift convex/weak barrier certificates from defining invariant sub-level sets of differentiable functions to formulas which can feature Boolean combinations of equalities and inequalities and thus describe a richer class of continuous invariants. In this paper we pursued a fundamentally different generalization; however, we remark that purely conjunctive differential invariants (of the form $\bigwedge_{i=1}^{m} B_i \leq 0$) in [34] reduce to the special case of vector barrier certificates where the matrix A is the zero matrix. Besides the method of barrier certificates, a number of other complementary methods are available for safety verification of continuous and hybrid systems, e.g. [13,8,14,29,47,35] (an overview of some techniques may be found in [16]).[13]

7 Conclusion

The comparison principle used in control theory and applied mathematics offers a powerful mechanism for creating abstractions of ODEs. In the domain of safety verification this principle can – in a very natural way – provide a theoretically satisfying foundation for understanding existing (scalar) notions of barrier certificates reported in [37,22,11]. Adopting the comparison principle viewpoint leads naturally to consider existing generalizations of this principle. In this vein, a multi-dimensional generalization of the method of barrier certificates (vector barrier certificates) has been formulated, in which the conditions on the derivative of barrier functions are relaxed in a way analogous to vector Lyapunov functions [2]. In the linear special case of this multidimensional extension (Corollary 1), the convexity of the search space can be preserved, allowing the use of tractable semi-definite programming techniques to search for more general classes of barrier certificates satisfying the semantic principle (Lemma 1) than was previously possible.

Acknowledgements. The authors would like to thank the FM 2018 reviewers for their feedback, constructive criticisms and suggestions, and extend special thanks to Dr Stefan Mitsch and Brandon Bohrer at Carnegie Mellon University for their detailed comments and scrutiny.

[13] Note, however, that the article [16] reproduces the unsound version of non-convex barrier certificates from [37], i.e. using the condition $\forall \boldsymbol{x} \in \mathbb{R}^n.(Q \wedge B = 0 \to B' \leq 0)$.

References

1. Beckenbach, E.F., Bellman, R.E.: Inequalities, Ergeb. Math. Grenzgeb., vol. 30. Springer (1961)
2. Bellman, R.: Vector Lyapunov functions. SIAM J. Control Optim. 1(1), 32–34 (1962)
3. Birkhoff, G., Rota, G.C.: Ordinary Differential Equations. John Wiley & Sons (1989)
4. Blanchini, F.: Set invariance in control. Automatica 35(11), 1747–1767 (1999)
5. Bouissou, O., Chapoutot, A., Djaballah, A., Kieffer, M.: Computation of parametric barrier functions for dynamical systems using interval analysis. In: 53rd IEEE Conference on Decision and Control, CDC 2014, Los Angeles, CA, USA, December 15-17, 2014. pp. 753–758. IEEE (2014)
6. Brauer, F.: Global behavior of solutions of ordinary differential equations. J. Math. Anal. Appl. 2(1), 145–158 (1961)
7. Brauer, F.: Some refinements of Lyapunov's second method. Canad. J. Math 17, 811–819 (1965)
8. Chen, X., Ábrahám, E., Sankaranarayanan, S.: Taylor model flowpipe construction for non-linear hybrid systems. In: Proceedings of the 33rd IEEE Real-Time Systems Symposium, RTSS 2012, San Juan, PR, USA, December 4-7, 2012. pp. 183–192. IEEE Computer Society (2012)
9. Collins, G.E., Hong, H.: Partial cylindrical algebraic decomposition for quantifier elimination. J. Symb. Comput. 12(3), 299–328 (1991)
10. Conti, R.: Sulla prolungabilità delle soluzioni di un sistema di equazioni differenziali ordinarie. Bollettino dell'Unione Matematica Italiana 11(4), 510–514 (12 1956)
11. Dai, L., Gan, T., Xia, B., Zhan, N.: Barrier certificates revisited. J. Symb. Comput. 80(1), 62–86 (2017)
12. Djaballah, A., Chapoutot, A., Kieffer, M., Bouissou, O.: Construction of parametric barrier functions for dynamical systems using interval analysis. Automatica 78, 287 – 296 (2017)
13. Fan, C., Kapinski, J., Jin, X., Mitra, S.: Locally optimal reach set overapproximation for nonlinear systems. In: 2016 International Conference on Embedded Software, EMSOFT 2016, Pittsburgh, Pennsylvania, USA, October 1-7, 2016. pp. 6:1–6:10. ACM (2016)
14. Frehse, G., Guernic, C.L., Donzé, A., Cotton, S., Ray, R., Lebeltel, O., Ripado, R., Girard, A., Dang, T., Maler, O.: SpaceEx: Scalable verification of hybrid systems. In: Gopalakrishnan, G., Qadeer, S. (eds.) Computer Aided Verification - 23rd International Conference, CAV 2011, Snowbird, UT, USA, July 14-20, 2011. Proceedings. LNCS, vol. 6806, pp. 379–395. Springer (2011)
15. Ghorbal, K., Sogokon, A., Platzer, A.: A hierarchy of proof rules for checking positive invariance of algebraic and semi-algebraic sets. Computer Languages, Systems & Structures 47, 19–43 (2017)
16. Guéguen, H., Lefebvre, M., Zaytoon, J., Nasri, O.: Safety verification and reachability analysis for hybrid systems. Annual Reviews in Control 33(1), 25–36 (2009)
17. Gunderson, R.W.: A stability condition for linear comparison systems. Quart. Appl. Math. 29(2), 327–328 (1971)
18. Habets, P., Peiffer, K.: Classification of stability-like concepts and their study using vector Lyapunov functions. J. Math. Anal. Appl. 43(2), 537–570 (1973)
19. Haddad, W.M., Chellaboina, V.: Nonlinear Dynamical Systems and Control, a Lyapunov-based approach. Princeton University Press (2008)

20. Hale, J.K., LaSalle, J.P.: Differential equations: Linearity vs. nonlinearity. SIAM Review 5(3), 249–272 (Jul 1963)
21. Handelman, D.: Representing polynomials by positive linear functions on compact convex polyhedra. Pacific J. Math. 132(1), 35–62 (1988)
22. 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.) Computer Aided Verification - 25th International Conference, CAV 2013, July 13-19, 2013. Proceedings. LNCS, vol. 8044, pp. 242–257. Springer (2013)
23. Lakshmikantham, V., Leela, S.: Differential and Integral Inequalities: Theory and Applications. Volume I: Ordinary Differential Equations. Academic Press (1969)
24. Lakshmikantham, V., Matrosov, V.M., Sivasundaram, S.: Vector Lyapunov Functions and Stability Analysis of Nonlinear Systems, Math. Appl., vol. 63. Springer (1991)
25. Liu, J., Zhan, N., Zhao, H.: Computing semi-algebraic invariants for polynomial dynamical systems. In: Chakraborty, S., Jerraya, A., Baruah, S.K., Fischmeister, S. (eds.) Ninth ACM International Conference on Embedded Software, October 9–14, 2011. Proceedings. pp. 97–106. EMSOFT'11, ACM (2011)
26. Lyapunov, A.M.: The general problem of stability of motion. Comm. Math. Soc. Kharkov (1892), English translation, Int. J. Control, vol. 55, pp. 531-773 (1992)
27. Matrosov, V.M.: On the theory of stability of motion. Prikl. Mat. Mekh. 26(6), 1506 – 1522 (1962), English translation (1962)
28. Michel, A.N., Miller, R.K.: Qualitative Analysis of Large Scale Dynamical Systems, Math. Sci. Engrg., vol. 134. Academic Press (1977)
29. Mitchell, I., Tomlin, C.: Level set methods for computation in hybrid systems. In: Lynch, N.A., Krogh, B.H. (eds.) Hybrid Systems: Computation and Control, Third International Workshop, HSCC 2000, Pittsburgh, PA, USA, March 23-25, 2000, Proceedings. LNCS, vol. 1790, pp. 310–323. Springer (2000)
30. Papachristodoulou, A., Anderson, J., Valmorbida, G., Prajna, S., Seiler, P., Parrilo, P.A.: SOSTOOLS version 3.00 sum of squares optimization toolbox for MATLAB. CoRR abs/1310.4716 (2013)
31. Parrilo, P.A.: Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization. Ph.D. thesis, California Institute of Technology (May 2000)
32. Peyrl, H., Parrilo, P.A.: Computing sum of squares decompositions with rational coefficients. Theor. Comput. Sci. 409(2), 269–281 (2008)
33. Platzer, A.: The structure of differential invariants and differential cut elimination. Log. Methods Comput. Sci. 8(4), 1–38 (2012)
34. Platzer, A., Clarke, E.M.: Computing differential invariants of hybrid systems as fixedpoints. Formal Methods in System Design 35(1), 98–120 (2009)
35. Platzer, A., Tan, Y.K.: Differential equation axiomatization: The impressive power of differential ghosts. In: Dawar, A., Grädel, E. (eds.) LICS. ACM, New York (2018)
36. Prajna, S.: Optimization-Based Methods for Nonlinear and Hybrid Systems Verification. Ph.D. thesis, California Institute of Technology (January 2005)
37. Prajna, S., Jadbabaie, A.: Safety verification of hybrid systems using barrier certificates. In: Alur, R., Pappas, G.J. (eds.) Hybrid Systems: Computation and Control, 7th International Workshop, HSCC 2004, March 25-27, 2004. Proceedings. LNCS, vol. 2993, pp. 477–492. Springer (2004)
38. 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)

39. Ratschan, S.: Efficient solving of quantified inequality constraints over the real numbers. ACM Trans. Comput. Log. 7(4), 723–748 (2006)
40. Ratschan, S., She, Z.: Providing a basin of attraction to a target region of polynomial systems by computation of Lyapunov-like functions. SIAM J. Control Optim. 48(7), 4377–4394 (Jul 2010)
41. Richardson, D.: Some undecidable problems involving elementary functions of a real variable. J. Symbolic Logic 33(4), 514–520 (1968)
42. Rouche, N., Habets, P., Laloy, M.: Stability Theory by Liapunov's Direct Method, Appl. Math. Sci., vol. 22. Springer (1977)
43. Roux, P., Voronin, Y., Sankaranarayanan, S.: Validating numerical semidefinite programming solvers for polynomial invariants. In: Rival, X. (ed.) Static Analysis - 23rd International Symposium, SAS 2016, Edinburgh, UK, September 8-10, 2016, Proceedings. LNCS, vol. 9837, pp. 424–446. Springer (2016)
44. Sankaranarayanan, S., Chen, X., Ábrahám, E.: Lyapunov function synthesis using Handelman representations. In: Tarbouriech, S., Krstic, M. (eds.) 9th IFAC Symposium on Nonlinear Control Systems, NOLCOS 2013, Toulouse, France, September 4-6, 2013. pp. 576–581. International Federation of Automatic Control (2013)
45. Sloth, C., Pappas, G.J., Wiśniewski, R.: Compositional safety analysis using barrier certificates. In: Dang, T., Mitchell, I.M. (eds.) Hybrid Systems: Computation and Control, HSCC'12, April 17-19, 2012. Proceedings. pp. 15–24. ACM (2012)
46. Son, N.K., Hinrichsen, D.: Robust stability of positive continuous time systems. Numer. Funct. Anal. Optim. 17(5-6), 649–659 (1996)
47. Tiwari, A.: Abstractions for hybrid systems. Formal Methods in System Design 32(1), 57–83 (2008)
48. Walter, W.: Differential inequalities and maximum principles: theory, new methods and applications. Nonlinear Analysis: Theory, Methods & Applications 30(8), 4695–4711 (1997), proceedings of the Second World Congress of Nonlinear Analysts
49. Walter, W.: Ordinary Differential Equations. Graduate Texts in Mathematics, Springer (1998)
50. Yang, Z., Huang, C., Chen, X., Lin, W., Liu, Z.: A linear programming relaxation based approach for generating barrier certificates of hybrid systems. In: Fitzgerald, J.S., Heitmeyer, C.L., Gnesi, S., Philippou, A. (eds.) FM 2016: Formal Methods - 21st International Symposium, November 9-11, 2016. Proceedings. LNCS, vol. 9995, pp. 721–738 (2016)
51. Yoshizawa, T.: Stability Theory by Liapunov's Second Method, Publications of the Mathematical Society of Japan, vol. 9. Math. Soc. Japan (1966)