Vector Barrier Certificates and Comparison Systems

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

1 - Carnegie Mellon University, Pittsburgh, USA

2 - Inria, Rennes, France

16 July 2018, FM 2018, Oxford, UK

Preliminaries: Systems of ODEs

An autonomous n-dimensional system of ODEs has the general form:

$$x_1' = f_1(x_1, \ldots, x_n),$$
$$\vdots$$
$$x_n' = f_n(x_1, \ldots, x_n),$$

where x_i' denotes the time derivative $\frac{dx_i}{dt}$ and f_i are continuous functions.

Preliminaries: Systems of ODEs

An autonomous n-dimensional system of ODEs has the general form:

$$x_1' = f_1(x_1, \ldots, x_n),$$
$$\vdots$$
$$x_n' = f_n(x_1, \ldots, x_n),$$

where x_i' denotes the time derivative $\frac{dx_i}{dt}$ and f_i are continuous functions.

We write $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$. The **vector field** $\boldsymbol{f} : \mathbb{R}^n \to \mathbb{R}^n$ gives the direction of motion at each point in space.

Preliminaries: Systems of ODEs

An autonomous n-dimensional system of ODEs has the general form:

$$x_1' = f_1(x_1, \ldots, x_n),$$
$$\vdots$$
$$x_n' = f_n(x_1, \ldots, x_n),$$

where x_i' denotes the time derivative $\frac{dx_i}{dt}$ and f_i are continuous functions.

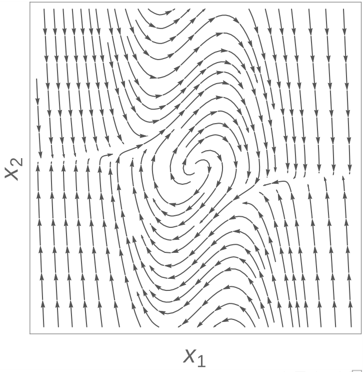
We write $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$. The **vector field** $\boldsymbol{f} : \mathbb{R}^n \to \mathbb{R}^n$ gives the direction of motion at each point in space.

A **solution** $\boldsymbol{x}(\boldsymbol{x}_0, t) : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n$ **exactly describes the motion** of a particle $\boldsymbol{x}_0$ under the influence of the vector field.

Example: Van der Pol oscillator

The Van der Pol system oscillator evolves according to the following ODEs:

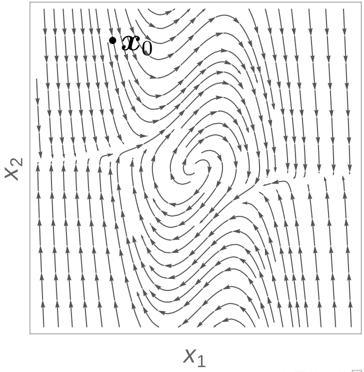
$$x_1' = x_2,$$
$$x_2' = (1 - x_1^2)x_2 - x_1$$



Example: Van der Pol oscillator

The Van der Pol system oscillator evolves according to the following ODEs:

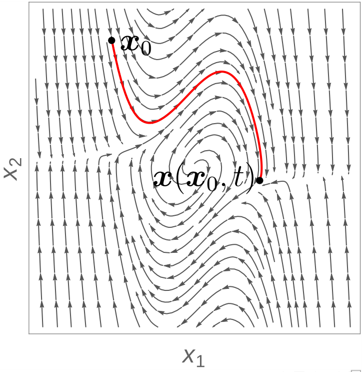
$$x_1' = x_2,$$
$$x_2' = (1 - x_1^2)x_2 - x_1$$



Example: Van der Pol oscillator

The Van der Pol system oscillator evolves according to the following ODEs:

$$x_1' = x_2,$$
$$x_2' = (1 - x_1^2)x_2 - x_1$$



Barrier certificates

Lyapunov-like safety verification method, due to Prajna & Jadbabaie (2004).

MAIN IDEA: Find a differentiable function $B : \mathbb{R}^n \to \mathbb{R}$ such that

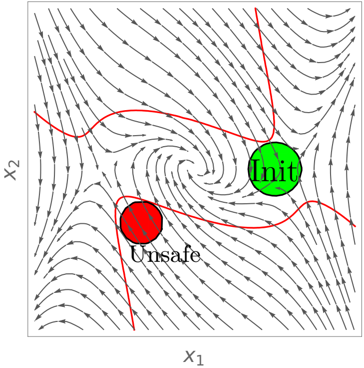
- $B(\boldsymbol{x}) > 0$ holds for every $\boldsymbol{x} \in \text{Unsafe}$,
- For all $\boldsymbol{x}_0 \in \text{Init}$, $B(\boldsymbol{x}(\boldsymbol{x}_0, t)) \leq 0$ holds for all future t.

Barrier certificates

Lyapunov-like safety verification method, due to Prajna & Jadbabaie (2004).

<u>MAIN IDEA</u>: Find a differentiable function $B : \mathbb{R}^n \to \mathbb{R}$ such that

- $B(\boldsymbol{x}) > 0$ holds for every $\boldsymbol{x} \in$ Unsafe,
- For all $\boldsymbol{x}_0 \in$ Init, $B(\boldsymbol{x}(\boldsymbol{x}_0, t)) \leq 0$ holds for all future t.

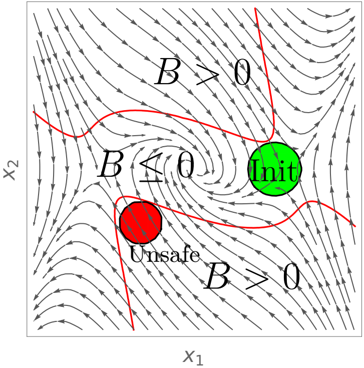


Barrier certificates

Lyapunov-like safety verification method, due to Prajna & Jadbabaie (2004).

MAIN IDEA: Find a differentiable function $B : \mathbb{R}^n \to \mathbb{R}$ such that

- $B(\boldsymbol{x}) > 0$ holds for every $\boldsymbol{x} \in$ Unsafe,
- For all $\boldsymbol{x}_0 \in$ Init, $B(\boldsymbol{x}(\boldsymbol{x}_0, t)) \leq 0$ holds for all future t.



Barrier certificates (more formally)

Lemma (Safety with semantic barrier certificates)

Given :

- *a system of n first-order ODEs $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$,*

Barrier certificates (more formally)

Lemma (Safety with semantic barrier certificates)

Given :

- *a system of* n *first-order ODEs* $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$,
- *possibly an evolution constraint* $Q \subseteq \mathbb{R}^n$,

Barrier certificates (more formally)

Lemma (Safety with semantic barrier certificates)

Given :

- *a system of* n *first-order ODEs* $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$,
- *possibly an evolution constraint* $Q \subseteq \mathbb{R}^n$,
- *a set of initial states* $\mathrm{Init} \subseteq \mathbb{R}^n$,

Barrier certificates (more formally)

Lemma (Safety with semantic barrier certificates)

Given :

- *a system of* n *first-order ODEs* $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$*,*
- *possibly an evolution constraint* $Q \subseteq \mathbb{R}^n$*,*
- *a set of initial states* $\mathrm{Init} \subseteq \mathbb{R}^n$*,*
- *and a set of unsafe states* $\mathrm{Unsafe} \subseteq \mathbb{R}^n$*,*

Barrier certificates (more formally)

Lemma (Safety with semantic barrier certificates)

Given :

- *a system of n first-order ODEs* $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$,
- *possibly an evolution constraint* $Q \subseteq \mathbb{R}^n$,
- *a set of initial states* $\mathrm{Init} \subseteq \mathbb{R}^n$,
- *and a set of unsafe states* $\mathrm{Unsafe} \subseteq \mathbb{R}^n$,

if a differentiable (barrier) function $B : \mathbb{R}^n \to \mathbb{R}$ *satisfies the following conditions, then the system is* ***safe****:*

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

Kinds of barrier certificates

Recall the (semantic) conditions:

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

Kinds of barrier certificates

Recall the (semantic) conditions:

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

Several *direct* sufficient conditions have been proposed to ensure the last requirement. Observe that the solutions $\boldsymbol{x}(\boldsymbol{x}_0, t)$ are not explicit.

Convex (Prajna & Jadbabaie, 2004)	**Exponential-type** (Kong et al., 2013)	**'General'** (Dai et al., 2017)
$Q \to B' \leq 0.$	$Q \to B' \leq \lambda B.$	$Q \to B' \leq \omega(B)$, $\forall t \geq 0.\ b(t) \leq 0$, b is the solution to $b' = \omega(b)$.

Kinds of barrier certificates

Recall the (semantic) conditions:

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

Several *direct* sufficient conditions have been proposed to ensure the last requirement. Observe that the solutions $\boldsymbol{x}(\boldsymbol{x}_0, t)$ are not explicit.

Convex
(Prajna & Jadbabaie, 2004)

$Q \to B' \leq 0.$

Exponential-type
(Kong et al., 2013)

$Q \to B' \leq \lambda B.$

'General'
(Dai et al., 2017)

$Q \to B' \leq \omega(B)$,
$\forall t \geq 0.\ b(t) \leq 0$,
b is the solution to $b' = \omega(b)$.

All these conditions are instantiations of the *comparison principle*.

Comparison principle

Used by R. Conti (1956), F. Brauer, C. Corduneanu (1960s), many others.
Not a new idea in applied mathematics; used in stability theory.

Comparison principle

Used by R. Conti (1956), F. Brauer, C. Corduneanu (1960s), many others.
Not a new idea in applied mathematics; used in stability theory.

MAIN IDEA: Given $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$, if a positive definite differentiable function $V : \mathbb{R}^n \to \mathbb{R}$ satisfies the differential inequality

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

where $\omega : \mathbb{R} \to \mathbb{R}$ is an appropriate *scalar* function, **one may infer the stability of $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$ from the stability of the one-dimensional system**

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

Comparison principle

Used by R. Conti (1956), F. Brauer, C. Corduneanu (1960s), many others. **Not a new idea** in applied mathematics; used in stability theory.

MAIN IDEA: Given $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$, if a positive definite differentiable function $V : \mathbb{R}^n \to \mathbb{R}$ satisfies the differential inequality

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

where $\omega : \mathbb{R} \to \mathbb{R}$ is an appropriate *scalar* function, **one may infer the stability of $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$ from the stability of the one-dimensional system**

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

One obtains an *abstraction* of the system by another *one-dimensional* system.

Comparison theorem (scalar majorization)

The comparison principle hinges on an appropriate *comparison theorem*.

Theorem (Scalar comparison theorem)

Let $V(t)$ and $v(t)$ be real valued functions differentiable on $[0, T]$. If

$$V' \le \omega(V) \quad \text{and} \quad v' = \omega(v)$$

holds on $[0, T]$ for some locally Lipschitz continuous function ω and if $V(0) = v(0)$, then for all $t \in [0, T]$ one has

$$V(t) \le v(t).$$

Informally, Solutions to the ODE $v' = \omega(v)$ act as upper bounds (i.e. *majorize*) solutions to $V' \le \omega(V)$.

Comparison principle

1. Introduce a fresh variable v (really a function of time $v(t)$),

Comparison principle

1. Introduce a fresh variable v (really a function of time $v(t)$),
2. Replace the scalar differential inequality $V' \leq \omega(V)$ by an equality.

Comparison principle

1. Introduce a fresh variable v (really a function of time $v(t)$),
2. Replace the scalar differential inequality $V' \leq \omega(V)$ by an equality.

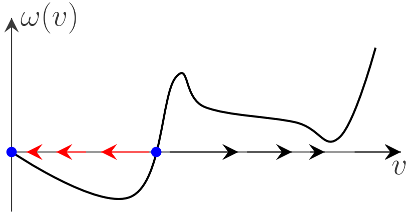
$$V' \leq \omega(V) \longrightarrow v' = \omega(v)$$

Comparison principle

1. Introduce a fresh variable v (really a function of time $v(t)$),
2. Replace the scalar differential inequality $V' \leq \omega(V)$ by an equality.

$$V' \leq \omega(V) \longrightarrow v' = \omega(v)$$

Obtain one-dimensional abstraction; 1-d systems are easy to study.



Kinds of barrier certificates

Recall the (semantic) conditions:

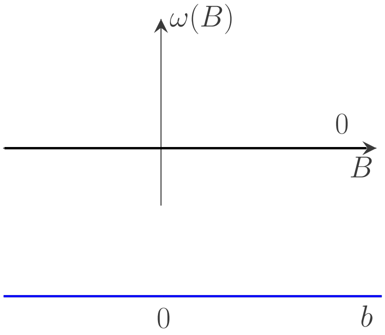
1. $\forall\, \boldsymbol{x} \in \text{Unsafe}.\ B(\boldsymbol{x}) > 0,$
2. $\forall\, \boldsymbol{x}_0 \in \text{Init}.\ \forall\, t \geq 0. \Big((\forall\, \tau \in [0, t].\ \boldsymbol{x}(\boldsymbol{x}_0, \tau) \in Q) \Rightarrow B(\boldsymbol{x}(\boldsymbol{x}_0, t)) \leq 0 \Big).$

Several *direct* sufficient conditions have been proposed to ensure the last requirement. Observe that the solutions $\boldsymbol{x}(\boldsymbol{x}_0, t)$ are not explicit.

Convex (Prajna & Jadbabaie, 2004)	**Exponential-type** (Kong et al., 2013)	**'General'** (Dai et al., 2017)
$Q \to B' \leq 0.$	$Q \to B' \leq \lambda B.$	$Q \to B' \leq \omega(B)$, $\forall t \geq 0.\ b(t) \leq 0$, b is the solution to $b' = \omega(b)$.

All these conditions are instantiations of the *comparison principle*.

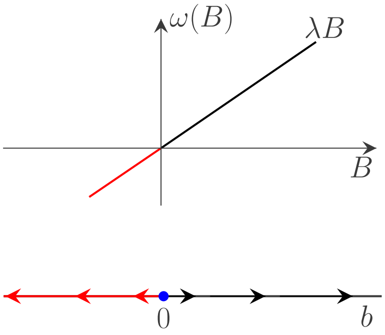
Convex barrier certificates (Prajna & Jadbabaie, 2004)



Differential inequality $B' \leq 0$

Comparison system $b' = 0$

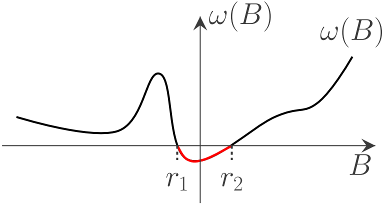
Exponential-type barrier certificates (Kong et al., 2013)



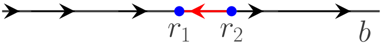
Differential inequality $B' \leq \lambda B$

Comparison system $b' = \lambda b$

General barrier certificates (Dai, et al., 2017)

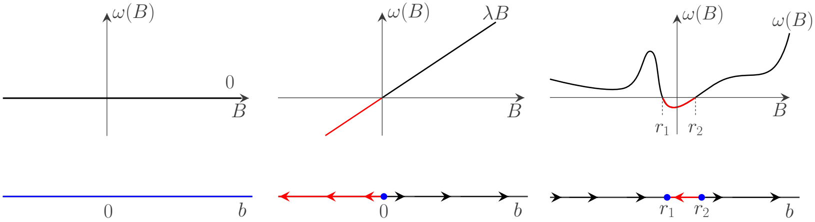


Differential inequality $B' \leq \omega(B)$



Comparison system $b' = \omega(b)$

Scalar barrier certificates as comparison systems

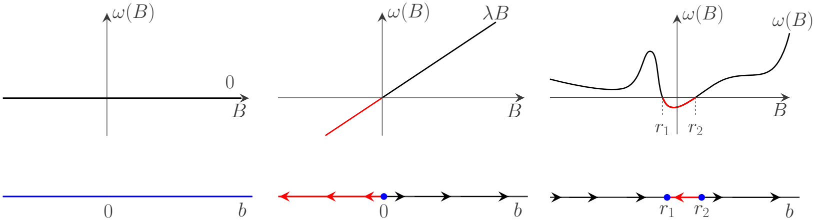


(a) Constant (zero)
Convex

(b) Linear
Exponential

(c) Non-linear
General

Scalar barrier certificates as comparison systems



(a) Constant (zero)
Convex

(b) Linear
Exponential

(c) Non-linear
General

Can we leverage the comparison principle to go beyond the scalar case?

Vector comparison systems

R.E. Bellman introduced **vector Lyapunov functions** in 1962.

Vector comparison systems

R.E. Bellman introduced **vector Lyapunov functions** in 1962.

<u>MAIN IDEA</u>: Given $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$, if a positive definite differentiable function $V : \mathbb{R}^n \to \mathbb{R}^m$ satisfies the differential inequality

$$\boldsymbol{V}' \leq \boldsymbol{\omega}(\boldsymbol{V}),$$

where $\boldsymbol{\omega} : \mathbb{R}^m \to \mathbb{R}^m$ is an appropriate *vector* function, **one may infer the stability of $x' = \boldsymbol{f}(x)$ from the stability of the m-dimensional system**

$$\boldsymbol{v}' = \boldsymbol{\omega}(\boldsymbol{v}).$$

Vector comparison systems

R.E. Bellman introduced **vector Lyapunov functions** in 1962.

MAIN IDEA: Given $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$, if a positive definite differentiable function $V : \mathbb{R}^n \to \mathbb{R}^m$ satisfies the differential inequality

$$\boldsymbol{V}' \leq \boldsymbol{\omega}(\boldsymbol{V}),$$

where $\boldsymbol{\omega} : \mathbb{R}^m \to \mathbb{R}^m$ is an appropriate *vector* function, **one may infer the stability of $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$ from the stability of the m-dimensional system**

$$\boldsymbol{v}' = \boldsymbol{\omega}(\boldsymbol{v}).$$

One obtains an *abstraction* of the system by another *m-dimensional* system.

Vector comparison systems

R.E. Bellman introduced **vector Lyapunov functions** in 1962.

MAIN IDEA: Given $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$, if a positive definite differentiable function $V : \mathbb{R}^n \to \mathbb{R}^m$ satisfies the differential inequality

$$\boldsymbol{V}' \leq \boldsymbol{\omega}(\boldsymbol{V}),$$

where $\boldsymbol{\omega} : \mathbb{R}^m \to \mathbb{R}^m$ is an appropriate *vector* function, **one may infer the stability of $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$ from the stability of the m-dimensional system**

$$\boldsymbol{v}' = \boldsymbol{\omega}(\boldsymbol{v}).$$

One obtains an *abstraction* of the system by another *m-dimensional* system.

!!! CAVEAT: The vector function $\boldsymbol{\omega}$ needs to be *quasi-monotone increasing*.

Quasi-monotone increasing functions

Definition

A function $\boldsymbol{\omega} : \mathbb{R}^m \to \mathbb{R}^m$ *is said to be quasi-monotone increasing if*

$$\omega_i(\boldsymbol{x}) \leq \omega_i(\boldsymbol{y})$$

for all $i = 1, \ldots, m$ *and all* $\boldsymbol{x}, \boldsymbol{y}$ *such that* $x_i = y_i$*, and* $x_k \leq y_k$ *for all* $k \neq i$.

Quasi-monotone increasing functions

Definition

A function $\boldsymbol{\omega} : \mathbb{R}^m \to \mathbb{R}^m$ is said to be quasi-monotone increasing if

$$\omega_i(\boldsymbol{x}) \leq \omega_i(\boldsymbol{y})$$

for all $i = 1, \ldots, m$ and all $\boldsymbol{x}, \boldsymbol{y}$ such that $x_i = y_i$, and $x_k \leq y_k$ for all $k \neq i$.

Every scalar function is (trivially) quasi-monotone increasing.

Quasi-monotone increasing functions

Definition

A function $\boldsymbol{\omega} : \mathbb{R}^m \to \mathbb{R}^m$ is said to be quasi-monotone increasing if

$$\omega_i(\boldsymbol{x}) \leq \omega_i(\boldsymbol{y})$$

for all $i = 1, \ldots, m$ and all $\boldsymbol{x}, \boldsymbol{y}$ such that $x_i = y_i$, and $x_k \leq y_k$ for all $k \neq i$.

Every scalar function is (trivially) quasi-monotone increasing.

A linear function $\boldsymbol{\omega}(\boldsymbol{x}) = A\boldsymbol{x}$ is quasi-monotone increasing if and only if A is *essentially non-negative*, i.e. all off-diagonal entries of A are non-negative.

Quasi-monotone increasing functions

Definition

A function $\boldsymbol{\omega} : \mathbb{R}^m \to \mathbb{R}^m$ *is said to be quasi-monotone increasing if*

$$\omega_i(\boldsymbol{x}) \leq \omega_i(\boldsymbol{y})$$

for all $i = 1, \dots, m$ *and all* $\boldsymbol{x}, \boldsymbol{y}$ *such that* $x_i = y_i$*, and* $x_k \leq y_k$ *for all* $k \neq i$*.*

Every scalar function is (trivially) quasi-monotone increasing.

A linear function $\boldsymbol{\omega}(\boldsymbol{x}) = A\boldsymbol{x}$ is quasi-monotone increasing if and only if A is *essentially non-negative*, i.e. all off-diagonal entries of A are non-negative.

Matrices with this property are also known as *Metzler matrices*.

Vector comparison principle

1. Introduce a fresh *vector* of variables $\boldsymbol{v}$ (*vector* function of time $\boldsymbol{v}(t)$),

Vector comparison principle

1. Introduce a fresh *vector* of variables $\boldsymbol{v}$ (*vector* function of time $\boldsymbol{v}(t)$),
2. Replace the vector differential inequality $\boldsymbol{V}' \leq \boldsymbol{\omega}(\boldsymbol{V})$ by an equality.

Vector comparison principle

1. Introduce a fresh *vector* of variables $\boldsymbol{v}$ (*vector* function of time $\boldsymbol{v}(t)$),
2. Replace the vector differential inequality $\boldsymbol{V}' \leq \boldsymbol{\omega}(\boldsymbol{V})$ by an equality.

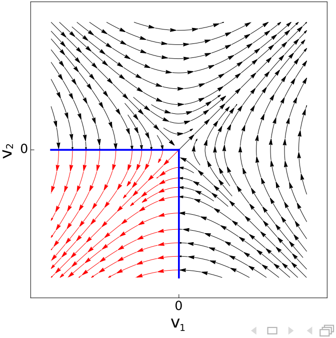
$$\boldsymbol{V}' \leq \boldsymbol{\omega}(\boldsymbol{V}) \quad \longrightarrow \quad \boldsymbol{v}' = \boldsymbol{\omega}(\boldsymbol{v})$$

Vector comparison principle

1. Introduce a fresh *vector* of variables $\boldsymbol{v}$ (*vector* function of time $\boldsymbol{v}(t)$),
2. Replace the vector differential inequality $\boldsymbol{V}' \leq \boldsymbol{\omega}(\boldsymbol{V})$ by an equality.

$$\boldsymbol{V}' \leq \boldsymbol{\omega}(\boldsymbol{V}) \longrightarrow \boldsymbol{v}' = \boldsymbol{\omega}(\boldsymbol{v})$$

Obtain an m-dimensional abstraction. More general than the scalar principle.



Vector comparison principle

Theorem (Linear vector comparison theorem)

For a given system of ODEs $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$ *and a Metzler matrix,* $A \in \mathbb{R}^{m \times m}$*, if* $\boldsymbol{V} = (V_1, V_2, \ldots, V_m)$ *satisfies the system of differential inequalities*

$$\boldsymbol{V}' \leq A\boldsymbol{V},$$

then for all $t \geq 0$ *the inequality* $\boldsymbol{V}(t) \leq \boldsymbol{v}(t)$ *holds component-wise, where* $\boldsymbol{v}(t)$ *is the solution to the comparison system* $\boldsymbol{v}' = A\boldsymbol{v}$*, and* $\boldsymbol{v}(0) = \boldsymbol{V}(0)$.

Vector comparison principle

Theorem (Linear vector comparison theorem)

For a given system of ODEs $\boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x})$ *and a Metzler matrix,* $A \in \mathbb{R}^{m\times m}$*, if* $\boldsymbol{V} = (V_1, V_2, \ldots, V_m)$ *satisfies the system of differential inequalities*

$$\boldsymbol{V}' \leq A\boldsymbol{V},$$

then for all $t \geq 0$ *the inequality* $\boldsymbol{V}(t) \leq \boldsymbol{v}(t)$ *holds component-wise, where* $\boldsymbol{v}(t)$ *is the solution to the comparison system* $\boldsymbol{v}' = A\boldsymbol{v}$*, and* $\boldsymbol{v}(0) = \boldsymbol{V}(0)$*.*

Metzler matrices have another important property:

Lemma

If $A \in \mathbb{R}^{m\times m}$ *is a Metzler matrix, then for any* $\boldsymbol{v}_0 \leq \boldsymbol{0}$*, the solution* $\boldsymbol{v}(t)$ *to the linear system* $\boldsymbol{v}' = A\boldsymbol{v}$ *is such that* $\boldsymbol{v}(t) \leq \boldsymbol{0}$ *for all* $t \geq 0$*.*

Vector barrier certificates

Theorem

Given an m-vector of 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 system is safe:

VBC$_\wedge$1. $\forall \boldsymbol{x} \in \mathbb{R}^n. (\text{Init} \rightarrow \bigwedge_{i=1}^{m} B_i \leq 0)$,

VBC$_\wedge$2. $\forall \boldsymbol{x} \in \mathbb{R}^n. (\text{Unsafe} \rightarrow \bigvee_{i=1}^{m} B_i > 0)$,

VBC$_\wedge$3. $\forall \boldsymbol{x} \in \mathbb{R}^n. (Q \rightarrow \boldsymbol{B}' \leq A\boldsymbol{B})$.

Vector barrier certificates

Theorem

Given an m-vector of 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 system is safe:

VBC$_\wedge$1. $\forall \boldsymbol{x} \in \mathbb{R}^n. (\text{Init} \rightarrow \bigwedge_{i=1}^{m} B_i \leq 0)$,

VBC$_\wedge$2. $\forall \boldsymbol{x} \in \mathbb{R}^n. (\text{Unsafe} \rightarrow \bigvee_{i=1}^{m} B_i > 0)$,

VBC$_\wedge$3. $\forall \boldsymbol{x} \in \mathbb{R}^n. (Q \rightarrow \boldsymbol{B}' \leq A\boldsymbol{B})$.

Generation?

Vector barrier certificates

Theorem

Given an m-vector of 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 system is safe:

VBC$_\wedge$1. $\forall \boldsymbol{x} \in \mathbb{R}^n. (\text{Init} \rightarrow \bigwedge_{i=1}^{m} B_i \leq 0)$,

VBC$_\wedge$2. $\forall \boldsymbol{x} \in \mathbb{R}^n. (\text{Unsafe} \rightarrow \bigvee_{i=1}^{m} B_i > 0)$,

VBC$_\wedge$3. $\forall \boldsymbol{x} \in \mathbb{R}^n. (Q \rightarrow \boldsymbol{B}' \leq A\boldsymbol{B})$.

Generation?

- Unfortunately **VBC$_\wedge$2** leads to non-convexity.
- Convexity enables the use of efficient **semidefinite solvers**.

Vector barrier certificate (convex)

Theorem

Given an m-vector of functions $\boldsymbol{B} = (B_1, B_2, \ldots, B_m)$ and some essentially non-negative $m \times m$ matrix A, if for some $i^* \in \{1, \ldots, m\}$ the following conditions hold, then the system is safe:

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. $\forall \boldsymbol{x} \in \mathbb{R}^n. (Q \rightarrow \boldsymbol{B}' \leq A\boldsymbol{B})$.

The above conditions define a **convex set**.

Generating vector barrier certificates using SDP

Solve a sum-of-squares optimization problem for size m vector barrier certificates $B_1, B_2, \ldots, B_m$, with $i^* \in \{1, \ldots, m\}$:

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

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

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

Possible using e.g. SOSTOOLS toolbox in Matlab, together with a semidefinite solve (e.g. SeDuMi).

Vector barrier certificates (deductive power)

Theorem

Polynomial convex or 'exponential-type' barrier certificates (trivially) satisfy the conditions $\textbf{\textit{VBC}}_{\wedge}\textbf{\textit{1-3}}$ *(or* ***VBC 1-3****). The converse is false.*

Vector barrier certificates (deductive power)

Theorem

*Polynomial convex or 'exponential-type' barrier certificates (trivially) satisfy the conditions **VBC$_\wedge$1-3** (or **VBC 1-3**). The converse is false.*

There are vector barrier certificates for some safety properties where scalar barrier certificates do not exist.

Vector barrier certificates (deductive power)

Theorem

Polynomial convex or 'exponential-type' barrier certificates (trivially) satisfy the conditions $\textbf{\textit{VBC}}_\wedge$ ***1-3*** (*or* ***VBC 1-3***)*. The converse is false.*

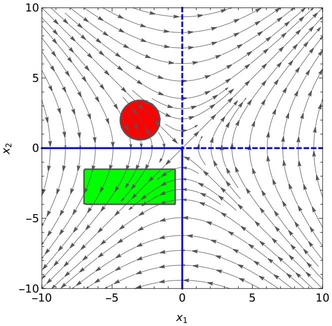
There are vector barrier certificates for some safety properties where scalar barrier certificates do not exist.

Vector barrier certificates can also exist with *lower polynomial degrees* than is possible with scalar barrier certificates!

Vector barrier certificates (example)

$$x_1' = x_2,$$
$$x_2' = x_1,$$

Vector barrier certificate $(B_1, B_2) = (x_1, x_2)$ satisfies $\begin{pmatrix} B_1' \\ B_2' \end{pmatrix} \leq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$ and has polynomial degree 1. No scalar barrier certificate of degree 1 exists.



Summary

- The comparison principle is a powerful and fundamental abstraction mechanism for ODEs.

Summary

- The comparison principle is a powerful and fundamental abstraction mechanism for ODEs.
- Existing (scalar) notions of barrier certificates follow easily from this principle.

Summary

- The comparison principle is a powerful and fundamental abstraction mechanism for ODEs.
- Existing (scalar) notions of barrier certificates follow easily from this principle.
- A generalization of existing notions of barrier certificates is achieved, following Bellman's use of the vector comparison principle.

Summary

- The comparison principle is a powerful and fundamental abstraction mechanism for ODEs.
- Existing (scalar) notions of barrier certificates follow easily from this principle.
- A generalization of existing notions of barrier certificates is achieved, following Bellman's use of the vector comparison principle.
- Also possible to use time-dependent Metzler matrices, i.e. $A(t)$. Work on this ongoing.

Limitations

- Choosing an appropriate Metzler matrix A for the comparison system is generally non-trivial.

Limitations

- Choosing an appropriate Metzler matrix A for the comparison system is generally non-trivial.
- Numerical inaccuracies in the results (to be expected with existing solvers).

Limitations

- Choosing an appropriate Metzler matrix A for the comparison system is generally non-trivial.
- Numerical inaccuracies in the results (to be expected with existing solvers).
- Trade-off: dimension of the comparison system vs degree of the barrier functions.

End

Questions?

Acknowledgments

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.