Characterizing Positively Invariant Sets

Inductive and Topological Methods

by Khalil Ghorbal (Inria, Rennes, France)
on October 9, 2020

Positively Invariant Sets

» (Autonomous) Ordinary Differential Equations

Consider the system

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

* x_i' stands for $\frac{dx_i}{dt}$
* $f_i : \mathbb{R}^n \to \mathbb{R}$ continuous functions
* $f := (f_1, \ldots, f_n)$ define *a* vector field over $\mathbb{R}^n$
* $x := (x_1, \ldots, x_n)$
* the entire system is denoted by $x' = f(x)$

» Initial Value Problem

Assume that solutions always exist (at least locally) and are unique (e.g. local Lipschitz continuity of f is sufficient to guarantee this property).

* Let $\varphi(\cdot, x)$ denote the solution to $x' = f(x)$ for some $x \in \mathbb{R}^n$
* $\varphi(\cdot, x)$ is defined over I_x
* I_x is an open interval containing zero
* I_x is called the maximal interval of existence (for x)
* $t > 0$ (resp. $t \geq 0$) denotes $I_x \cap (0, +\infty)$ (resp. $I_x \cap [0, +\infty)$)

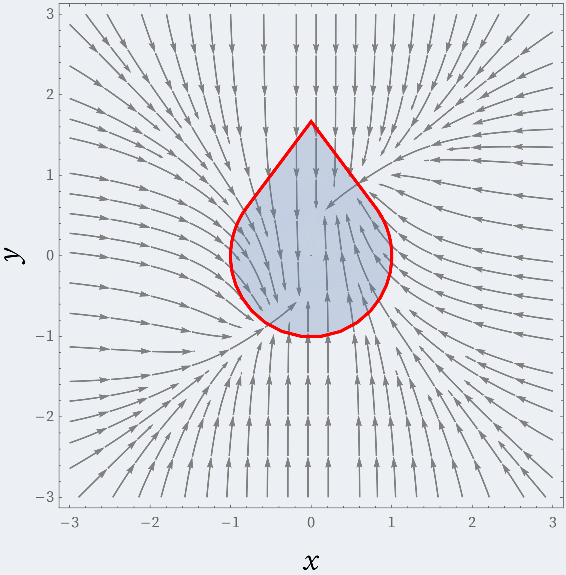
» Positively Invariant Sets

Given system of ODEs $x' = f(x)$, a set $S \subseteq \mathbb{R}^n$ is positively invariant if and only if no solution starting inside S can leave S in the future, i.e.

$$\forall\, x \in S.\ \forall\, t \geq 0.\ \varphi(t, x) \in S\,.$$

» Droplet

Is it positively invariant?



» Intuition

Nagumo's theorem

A closed set $S \subseteq \mathbb{R}^n$ is positively invariant for f **if and only if**:

The Nagumo Theorem (informally)

At each point on the **boundary** of S, the vector field f *"points into the interior of S or is tangent to S"*.

* M. Nagumo (1942) [in German]
* J. Yorke (1967),
* J-M. Bony (1969) [in French],
* H. Brezis (1970),
* P. Hartman, M. Crandall, R. Redheffer (1972)

» Smooth sub-level sets

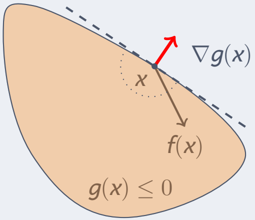
Nagumo's theorem

Suppose

- g is continuously differentiable, and
- $\nabla g(x) \neq 0$ for all x satisfying $g(x) = 0$

Then the sub-level set $\{x \mid g(x) \leq 0\}$ is positively invariant **iff**:

$$\forall x.\ (g(x) = 0 \Rightarrow \nabla g \cdot f(x) \leq 0)$$



» Beyond Practical Sets

* Important in control and engineering (Blanchini and Miani 2010)
* Formal verification using interactive and automated theorem proving (more recent)

* S might not be closed (nor open)
* S is often encoded as a semi-algebraic set
* The boundary of S might not be smooth

Real Induction

» Induction over non-negative reals

A predicate $P(t)$ holds true for *all* $t \geq 0$ **if and only if:**

1. $P(0)$,
2. $\forall\, t \geq 0.\ \neg P(t) \rightarrow \exists\, \varepsilon > 0.\ \forall\, T \in (t, t - \varepsilon).\ \neg P(T)$,
3. $\forall\, t \geq 0.\ P(t) \rightarrow \exists\, \varepsilon > 0.\ \forall\, T \in (t, t + \varepsilon).\ P(T)$.

» Induction over non-negative reals

A predicate $P(t)$ holds true for *all* $t \geq 0$ **if and only if**:

1. $P(0)$,
2. $\forall\, t \geq 0.\ \neg P(t) \to \exists\, \varepsilon > 0.\ \forall\, T \in (t, t - \varepsilon).\ \neg P(T)$,
3. $\forall\, t \geq 0.\ P(t) \to \exists\, \varepsilon > 0.\ \forall\, T \in (t, t + \varepsilon).\ P(T)$.

Proof.

"**if**" Consider (for contradiction) the time $t_* = \inf\{t \geq 0 \mid \neg P(t)\}$.
By 1. and 3. we have that $t_* \neq 0$, so t_* must be positive, but in this case $P(t)$ holds for all $t \in [0, t_*)$ (by definition). If $P(t_*)$, then t_* cannot be an infimum (by 3.), and if $\neg P(t_*)$ then (by 2.) we have that $\neg P(t)$ holds for all $t \in (t_* - \varepsilon, t_*)$ for some $\varepsilon > 0$; a contradiction.
"**only if**" is obvious. □

» Induction over non-negative reals

A predicate $P(t)$ holds true for all $t \geq 0$ **if and only if:**

1. $P(0)$,
2. $\forall\, t \geq 0.\ \neg P(t) \rightarrow \exists\, \varepsilon > 0.\ \forall\, T \in (t, t - \varepsilon).\ \neg P(T)$,
3. $\forall\, t \geq 0.\ P(t) \rightarrow \exists\, \varepsilon > 0.\ \forall\, T \in (t, t + \varepsilon).\ P(T)$.

Condition 2. can be replaced by a weaker condition

$$\forall\, t > 0.\ \neg P(t) \rightarrow \exists\, T \in [0, t).\ \neg P(T)\,,$$

or its contrapositive form

$$\forall\, t > 0.\ P(t) \leftarrow \big(\forall\, T \in [0, t).\ P(T)\big).$$

Pete L. Clark, *The Instructor's Guide to Real Induction*, **Mathematics Magazine 92(2)**, 2019.

» In Sets

Definition

Let $S \subseteq \mathbb{R}^n$. The In_f set of S is defined as

$$\mathsf{In}_f(S) \stackrel{\text{def}}{=} \{x \in \mathbb{R}^n \mid \exists\, \varepsilon > 0.\ \forall\, t \in (0, \varepsilon).\ \varphi(t, x) \in S\}$$

$\mathsf{In}_f(S)$ is the set of states, not necessarily in S, from which the system will evolve inside S for some non-trivial time interval "immediately in the future".

» Constructions

1. Reversing the flow

$$\mathsf{In}_{-f}(S) = \{x \in \mathbb{R}^n \mid \exists\, \varepsilon > 0.\, \forall\, t \in (0, \varepsilon).\, \varphi(-t, x) \in S\}$$

2. Complementing

$$\mathsf{In}_{f}(S)^c = \{x \in \mathbb{R}^n \mid \forall\, \varepsilon > 0.\, \exists\, t \in (0, \varepsilon).\, \varphi(t, x) \notin S\}$$

3. In set of the complement

$$\mathsf{In}_{f}(S^c) = \{x \in \mathbb{R}^n \mid \exists\, \varepsilon > 0.\, \forall\, t \in (0, \varepsilon).\, \varphi(t, x) \notin S\}$$

» Constructions

1. Reversing the flow

$$\mathrm{In}_{-f}(S) = \{x \in \mathbb{R}^n \mid \exists\, \varepsilon > 0.\ \forall\, t \in (0, \varepsilon).\ \varphi(-t, x) \in S\}$$

2. Complementing

$$\mathrm{In}_f(S)^c = \{x \in \mathbb{R}^n \mid \forall\, \varepsilon > 0.\ \exists\, t \in (0, \varepsilon).\ \varphi(t, x) \notin S\}$$

3. In set of the complement

$$\mathrm{In}_f(S^c) = \{x \in \mathbb{R}^n \mid \exists\, \varepsilon > 0.\ \forall\, t \in (0, \varepsilon).\ \varphi(t, x) \notin S\}$$

Thus, $\mathrm{In}_f(S^c) \subseteq \mathrm{In}_f(S)^c$ (the converse doesn't hold in general).

» Characterizing positively invariant sets via real induction

Theorem (Liu et al. 2011)

A set $S \subseteq \mathbb{R}^n$ is positively invariant under the flow of the system $x' = f(x)$ **if and only if**

$$S \subseteq \mathrm{In}_f(S) \quad \text{and} \quad S^c \subseteq \mathrm{In}_{-f}(S^c)\,.$$

Proof.

Take "$\varphi(t, x) \in S$" as the predicate $P(t)$. □

» Distributive properties

$$\mathrm{In}_f(S_1 \cap S_2) = \mathrm{In}_f(S_1) \cap \mathrm{In}_f(S_2)$$

$$\mathrm{In}_f(S_1 \cup S_2) \supseteq \mathrm{In}_f(S_1) \cup \mathrm{In}_f(S_2)$$

» Distributive properties

$$\text{In}_f(S_1 \cap S_2) = \text{In}_f(S_1) \cap \text{In}_f(S_2)$$

$$\text{In}_f(S_1 \cup S_2) \supseteq \text{In}_f(S_1) \cup \text{In}_f(S_2)$$

Counterexample

$x' = 1$ and $S = \{x \in \mathbb{R} \mid x \leq 0 \vee (x > 0 \wedge \sin(x^{-1}) = 0)\}$.

- $0 \notin \text{In}_f(S)$
- Therefore $0 \in \text{In}_f(S)^c$
- $0 \notin \text{In}_f(S^c)$

Thus: $\text{In}_f(S \cup S^c) = \text{In}_f(\mathbb{R}^n) = \mathbb{R}^n \neq \text{In}_f(S) \cup \text{In}_f(S^c)$.

» In set of equalities

Let g be analytic.

$$g' = \sum_{i=1}^{n} \frac{\partial g}{\partial x_i} f_i = \nabla g \cdot f$$

$$\boxed{g(\varphi(t,x)) = g(x) + g'(x)t + g''(x)\frac{t^2}{2!} + \cdots}$$

» In set of equalities

Let g be analytic.

$$g' = \sum_{i=1}^{n} \frac{\partial g}{\partial x_i} f_i = \nabla g \cdot f$$

$$\boxed{g(\varphi(t,x)) = g(x) + g'(x)t + g''(x)\frac{t^2}{2!} + \cdots}$$

$$\mathrm{In}_f(g = 0) \quad \equiv \quad g = 0 \cap g' = 0 \cap g'' = 0 \cap g''' = 0 \cap \cdots$$

» In set of equalities

Let g be analytic.

$$g' = \sum_{i=1}^{n} \frac{\partial g}{\partial x_i} f_i = \nabla g \cdot f$$

$$\boxed{g(\varphi(t,x)) = g(x) + g'(x)t + g''(x)\frac{t^2}{2!} + \cdots}$$

$$\mathrm{In}_f(g=0) \quad \equiv \quad g=0 \cap g'=0 \cap g''=0 \cap g'''=0 \cap \cdots$$

which can be described by an "infinite formula":

$$\text{“} \quad \mathrm{In}_f(g=0) \quad \equiv \quad g=0 \wedge g'=0 \wedge g''=0 \wedge g'''=0 \wedge \cdots \quad \text{”}.$$

» In set of inequalities

$$g(\varphi(t,x)) = g(x) + g'(x)t + g''(x)\frac{t^2}{2!} + \cdots$$

The situation with inequalities $g < 0$ is similar:

$$\text{“}\quad \mathrm{In}_f(g<0) \equiv g<0$$
$$\vee\ (g=0 \wedge \dot{g}<0)$$
$$\vee\ (g=0 \wedge \dot{g}=0 \wedge \ddot{g}<0)$$
$$\vee\ (g=0 \wedge \dot{g}=0 \wedge \ddot{g}=0 \wedge \dddot{g}<0)$$
$$\vdots$$
$$\text{”}$$

» In set of inequalities

$$g(\varphi(t,x)) = g(x) + g'(x)t + g''(x)\frac{t^2}{2!} + \cdots$$

The situation with inequalities $g < 0$ is similar:

$$\text{“}\quad \mathrm{In}_f(g<0) \equiv g < 0$$
$$\vee\ (g = 0 \wedge \dot{g} < 0)$$
$$\vee\ (g = 0 \wedge \dot{g} = 0 \wedge \ddot{g} < 0)$$
$$\vee\ (g = 0 \wedge \dot{g} = 0 \wedge \ddot{g} = 0 \wedge \dddot{g} < 0)$$
$$\vdots$$
$$\text{”}$$

What happens when g and f are polynomials?

» Ascending chain condition

- $\mathbb{R}[x_1, \ldots, x_n]$ is **Noetherian** (Hilbert basis theorem)
- Assuming a polynomial vector field $f_i \in \mathbb{R}[x_1, \ldots, x_n]$

» Ascending chain condition

* $\mathbb{R}[x_1, \ldots, x_n]$ is **Noetherian** (Hilbert basis theorem)
* Assuming a polynomial vector field $f_i \in \mathbb{R}[x_1, \ldots, x_n]$

Let $p \in \mathbb{R}[x_1, \ldots, x_n]$, then the ascending chain of ideals

$$\langle p \rangle \subseteq \langle p, p' \rangle \subseteq \langle p, p', p'' \rangle \subseteq \cdots$$

is finite, i.e. there exists a $k \in \mathbb{N}$ such that $\langle p, p', \ldots, p^{(k)} \rangle = \langle p, p', \ldots, p^{(K)} \rangle$ for all $K \geq k$.

» Ascending chain condition

- $\mathbb{R}[x_1, \ldots, x_n]$ is **Noetherian** (Hilbert basis theorem)
- Assuming a polynomial vector field $f_i \in \mathbb{R}[x_1, \ldots, x_n]$

Let $p \in \mathbb{R}[x_1, \ldots, x_n]$, then the ascending chain of ideals

$$\langle p \rangle \subseteq \langle p, p' \rangle \subseteq \langle p, p', p'' \rangle \subseteq \cdots$$

is finite, i.e. there exists a $k \in \mathbb{N}$ such that $\langle p, p', \ldots, p^{(k)} \rangle = \langle p, p', \ldots, p^{(K)} \rangle$ for all $K \geq k$.

- k is the order of p w.r.t. to f, denoted $\mathrm{ord}_f(p)$
- $\mathrm{ord}_f(p)$ is computable using Gröbner bases

» In set of **polynomial** equalities

Let g be analytic.

$$g' = \sum_{i=1}^{n} \frac{\partial g}{\partial x_i} f_i = \nabla g \cdot f$$

$$\boxed{g(\varphi(t,x)) = g(x) + g'(x)t + g''(x)\frac{t^2}{2!} + \cdots}$$

$$\mathrm{In}_f(g=0) \quad \equiv \quad g=0 \cap g'=0 \cap g''=0 \cap g'''=0 \cap \cdots$$

which can be described by an “infinite formula”:

$$\text{“} \quad \mathrm{In}_f(g=0) \quad \equiv \quad g=0 \wedge g'=0 \wedge g''=0 \wedge g'''=0 \wedge \cdots \quad \text{”}.$$

» In set of **polynomial** inequalities

$$g(\varphi(t,x)) = g(x) + g'(x)t + g''(x)\frac{t^2}{2!} + \cdots$$

The situation with inequalities $g < 0$ is similar:

$$\text{“} \quad \text{In}_f(g < 0) \equiv g < 0 \\ \vee\ (g = 0 \wedge \dot{g} < 0) \\ \vee\ (g = 0 \wedge \dot{g} = 0 \wedge \ddot{g} < 0) \\ \vee\ (g = 0 \wedge \dot{g} = 0 \wedge \ddot{g} = 0 \wedge \dddot{g} < 0) \\ \vdots \quad \text{”}$$

» Semi-algebraic sets

$$\mathrm{In}_f(S_1 \cap S_2) = \mathrm{In}_f(S_1) \cap \mathrm{In}_f(S_2)$$

$$\mathrm{In}_f(S_1 \cup S_2) \supseteq \mathrm{In}_f(S_1) \cup \mathrm{In}_f(S_2)$$

Counterexample

$x' = 1$ and $S = \{x \in \mathbb{R} \mid x \leq 0 \vee (x > 0 \wedge \sin(x^{-1}) = 0)\}$.

* $0 \notin \mathrm{In}_f(S)$
* Therefore $0 \in \mathrm{In}_f(S)^c$
* $0 \notin \mathrm{In}_f(S^c)$

Thus: $\mathrm{In}_f(S \cup S^c) = \mathrm{In}_f(\mathbb{R}^n) = \mathbb{R}^n \neq \mathrm{In}_f(S) \cup \mathrm{In}_f(S^c)$.

» In set of semi-algebraic sets

$$S \equiv \bigvee_{i=1}^{l} \left(\bigwedge_{j=1}^{m_i} p_{ij} < 0 \;\wedge \bigwedge_{j=m_i+1}^{M_i} p_{ij} = 0 \right)$$

$$\mathrm{In}_f(S) \equiv \bigvee_{i=1}^{l} \left(\bigwedge_{j=1}^{m_i} \mathrm{In}_f(p_{ij} < 0) \;\wedge \bigwedge_{j=m_i+1}^{M_i} \mathrm{In}_f(p_{ij} = 0) \right)$$

» LZZ Decision procedure

Checking problem

Given a semi-algebraic set S and a polynomial vector field f, check whether S is positively invariant for f.

1. Construct $\mathrm{In}_f(S)$
2. Construct $\mathrm{In}_{-f}(S^c)$ (using the reversed flow $-f$).
3. Check the semi-algebraic set inclusions $S \subseteq \mathrm{In}_f(S)$ and $S^c \subseteq \mathrm{In}_{-f}(S^c)$ using e.g. the CAD algorithm (Collins and Hong 1991).

» LZZ Decision procedure

Checking problem

Given a semi-algebraic set S and a polynomial vector field f, check whether S is positively invariant for f.

1. Construct $\mathrm{In}_f(S)$
2. Construct $\mathrm{In}_{-f}(S^c)$ (using the reversed flow $-f$).
3. Check the semi-algebraic set inclusions $S \subseteq \mathrm{In}_f(S)$ and $S^c \subseteq \mathrm{In}_{-f}(S^c)$ using e.g. the CAD algorithm (Collins and Hong 1991).

In practice, checking the inclusions **never** terminates!

Exit Sets

» Exit sets

Exit Set (Conley 78)

The exit set of $S \subseteq \mathbb{R}^n$ with respect to the local flow induced by $x' = f(x)$ is defined as follows:

$$\mathrm{Exit}_f(S) \stackrel{\text{def}}{=} \{x \in S \mid \forall\, t > 0.\ \exists\, s \in (0,t).\ \varphi(s,x) \notin S\}\,.$$

$\mathrm{Exit}_f(S)$ is the set of points in S from which the flow leaves S "immediately in the futur".

» Exit sets

Exit Set (Conley 78)

The exit set of $S \subseteq \mathbb{R}^n$ with respect to the local flow induced by $x' = f(x)$ is defined as follows:

$$\mathrm{Exit}_f(S) \overset{\text{def}}{=} \{x \in S \mid \forall\, t > 0.\ \exists\, s \in (0, t).\ \varphi(s, x) \notin S\}.$$

$\mathrm{Exit}_f(S)$ is the set of points in S from which the flow leaves S "immediately in the futur".

* $\mathrm{Exit}_f(S)$ and $\mathrm{Exit}_{-f}(S)$ are not necessarily disjoint
* neither do they cover the intersection $S \cap \partial S$

» Constructions

1. Reversing the flow

$$\mathrm{Exit}\_{-f}(S) = \{x \in S \mid \forall\, t > 0.\ \exists\, s \in (0,t).\ \varphi(-s,x) \notin S\}$$

2. Complementing

$$\mathrm{Exit}_f(S)^c = S^c \cup \{x \in S \mid \exists\, t > 0.\ \forall\, s \in (0,t).\ \varphi(s,x) \in S\}$$

3. Exit set of the complement

$$\mathrm{Exit}_f(S^c) = \{x \in S^c \mid \forall\, t > 0.\ \exists\, s \in (0,t).\ \varphi(s,x) \in S\}$$

» Characterizing positively invariant sets via exit sets

A set $S \subseteq \mathbb{R}^n$ is positively invariant if and only if both $\mathrm{Exit}_f(S)$ and $\mathrm{Exit}_{-f}(S^c)$ are empty.

Proof.

For any set $S \subseteq \mathbb{R}^n$, $\mathrm{Exit}_f(S) = \mathrm{In}_f(S)^c \cap S$.

$$\emptyset = \underbrace{\mathrm{In}_f(S)^c \cap S}_{\mathrm{Exit}_f(S)} \iff S \subseteq \mathrm{In}_f(S)\,,$$

$$\emptyset = \underbrace{\mathrm{In}_{-f}(S^c)^c \cap S^c}_{\mathrm{Exit}_{-f}(S^c)} \iff S^c \subseteq \mathrm{In}_{-f}(S^c)\,.$$

□

Distributive properties

$$\mathrm{Exit}_f(S_1 \cap S_2) = (\mathrm{Exit}_f(S_1) \cap S_2) \cup (S_1 \cap \mathrm{Exit}_f(S_2))$$

$$\mathrm{Exit}_f(S_1 \cup S_2) \subseteq \left(\mathrm{Exit}_f(S_1) \cap \mathrm{In}_f(S_2)^c\right) \cup \left(\mathrm{In}_f(S_1)^c \cap \mathrm{Exit}_f(S_2)\right)$$

» Distributive properties

$$\mathrm{Exit}_f(S_1 \cap S_2) = (\mathrm{Exit}_f(S_1) \cap S_2) \cup (S_1 \cap \mathrm{Exit}_f(S_2))$$

$$\mathrm{Exit}_f(S_1 \cup S_2) \subseteq \left(\mathrm{Exit}_f(S_1) \cap \mathrm{In}_f(S_2)^c\right) \cup \left(\mathrm{In}_f(S_1)^c \cap \mathrm{Exit}_f(S_2)\right)$$

Counterexample

$x' = 1$ and the sets

$$S_1 = \{0\} \cup \left\{x \in \mathbb{R} \mid x > 0 \wedge \sin\left(x^{-1}\right) = 0\right\},$$
$$S_2 = \{0\} \cup \left\{x \in \mathbb{R} \mid x > 0 \wedge \sin\left(x^{-1}\right) \neq 0\right\}.$$

* $0 \in \mathrm{Exit}_f(S_1)$ and $0 \in \mathrm{Exit}_f(S_2)$
* $0 \notin \mathrm{In}_f(S_1)$ and $0 \notin \mathrm{In}_f(S_2)$
* $0 \notin \mathrm{Exit}_f(S_1 \cup S_2)$ ($x \geq 0$ is a positively invariant set)

» Exit set of polynomial equalities

$$
\begin{aligned}
\mathrm{Exit}_f(p = 0) \equiv \big(\, & p = 0 \land p' \neq 0 \\
\lor\, & p = 0 \land p' = 0 \land p'' \neq 0 \\
& \vdots \\
\lor\, & p = 0 \land p' = 0 \land p'' = 0 \land \cdots \land p^{(\mathrm{ord}_f(p))} \neq 0 \big) \,.
\end{aligned}
$$

» Exit set of polynomial equalities

$$
\begin{aligned}
\mathrm{Exit}_f(p = 0) \equiv \big(\, & p = 0 \wedge p' \neq 0 \\
\vee\, & p = 0 \wedge p' = 0 \wedge p'' \neq 0 \\
& \vdots \\
\vee\, & p = 0 \wedge p' = 0 \wedge p'' = 0 \wedge \cdots \wedge p^{(\mathrm{ord}_f(p))} \neq 0 \big) .
\end{aligned}
$$

The exit set of open sets is empty. In particular

$$\mathrm{Exit}_f(p < 0) \equiv \mathsf{F}$$

» Decision procedure

Coarse granularity

Checking problem

Given a semi-algebraic set S and a polynomial vector field f, check whether S is positively invariant for f.

1. Construct $\mathrm{Exit}_f(S)$
2. Construct $\mathrm{Exit}_{-f}(S^c)$ (using the reversed flow $-f$).
3. Check the emptiness of $\mathrm{Exit}_f(S)$ and $\mathrm{Exit}_{-f}(S^c)$ using e.g. the CAD algorithm (Collins and Hong 1991).

» Decision procedure

Coarse granularity

Checking problem

Given a semi-algebraic set S and a polynomial vector field f, check whether S is positively invariant for f.

1. Construct $\mathrm{Exit}_f(S)$
2. Construct $\mathrm{Exit}_{-f}(S^c)$ (using the reversed flow $-f$).
3. Check the emptiness of $\mathrm{Exit}_f(S)$ and $\mathrm{Exit}_{-f}(S^c)$ using e.g. the CAD algorithm (Collins and Hong 1991).

But then we hit the same wall!

» Decomposition to basic semi-algebraic sets

Fine granularity

- S semi-algebraic set encoded in a normal form $\bigwedge_{i=1}^{k} \bigvee_{j=1}^{m_i} (p_{ij} \bowtie_{ij} 0)$ (CNF)
- $p_{ij} \in \mathbb{R}[x_1, \ldots, x_n]$
- $m = \max_i m_i$
- $d = \max_{i,j} \deg(p_{ij})$
- $\rho = \max_{i,j} \mathrm{ord}_f(p_{ij})$

Then $\mathrm{Exit}_f(S) \vee \mathrm{Exit}_{-f}(\neg S)$ is a union of at most $k\rho m^k(\rho+1)^{k-1}$ basic semi-algebraic sets

$$q_1 \bowtie_1 0 \wedge \ldots \wedge q_s \bowtie_s 0\,,$$

where $s \leq m - 1 + k(\rho + 1)$ and $\deg(q_j) \leq d + \rho(\deg(f) - 1)$.

» Recursive procedure

Divide and conquer

Let S and R be two semi-algebraic sets. We define $\mathrm{NonEmpty}_f(S, R)$ recursively on the Boolean structure of S:
$\mathrm{NonEmpty}_f(S, R)$ returns False if and only if $\mathrm{Exit}_f(S) \cap R$ is empty.

$$
\begin{aligned}
\mathrm{NonEmpty}_f(A,\ R) &:= \mathrm{Reduce}\left(\exists x_1. \dots \exists x_n.\ \mathrm{Exit}_f(A) \wedge R\right)\ , \\
\mathrm{NonEmpty}_f(S_1 \wedge S_2,\ R) &:= \mathrm{NonEmpty}_f(S_1,\ S_2 \wedge R) \\
&\quad \vee \mathrm{NonEmpty}_f(S_2,\ S_1 \wedge R)\ , \\
\mathrm{NonEmpty}_f(S_1 \vee S_2,\ R) &:= \mathrm{NonEmpty}_f(S_1, \neg \mathrm{In}_f(S_2) \wedge R) \\
&\quad \vee \mathrm{NonEmpty}_f(S_2,\ \neg \mathrm{In}_f(S_1) \wedge R)\ , \\
\mathrm{NonEmpty}_f(\neg S,\ R) &:= \mathrm{NonEmpty}_f(\mathrm{Neg}(S),\ R)\ .
\end{aligned}
$$

» ES decision procedure

Theorem

A semi-algebraic set S is positively invariant for a system of polynomial ODEs $x' = f(x)$ if and only if

$$\neg\left(\mathrm{NonEmpty}_f(S, \mathrm{T}) \ \vee\ \mathrm{NonEmpty}_{-f}(\neg S, \mathrm{T})\right) \quad .$$

» ES decision procedure

Theorem

A semi-algebraic set S is positively invariant for a system of polynomial ODEs $x' = f(x)$ if and only if

$$\neg\left(\mathrm{NonEmpty}_f(S, \mathrm{T}) \;\vee\; \mathrm{NonEmpty}_{-f}(\neg S, \mathrm{T})\right) \quad .$$

Trade-ff

ES proposes a natural trade-off between the fine and coarse granularities suggested by the Boolean structure of the candidate S.

» Complexity analysis

Normal forms

* S in in disjunctive normal form (DNF) $\bigvee_{i=1}^{k} \bigwedge_{j=1}^{m_i} A_{ij}$
* A_{ij} are atomic formulas
* $m = \mathsf{max}_i\, m_i$

* The recursion depth of $\mathsf{NonEmpty}_f(S, \mathsf{T})$ is bounded by $k + m$
* The number of calls to Reduce is $\sum_{i=1}^{k} m_i \leq km$
* Each call has the form $\mathsf{Reduce}\, \exists x_1 \ldots \exists x_n . \mathsf{Exit}_f(A_{rs}) \wedge R_{rs}$, where

$$R_{rs} \equiv \bigwedge_{j=1, j \neq s}^{m_r} A_{rj} \wedge \neg \mathsf{In}_f \left(\bigvee_{i=1, i \neq s}^{k} \bigwedge_{j=1}^{m_i} A_{ij} \right) .$$

A similar statement holds for conjunctive normal forms (CNF).

» DNF example

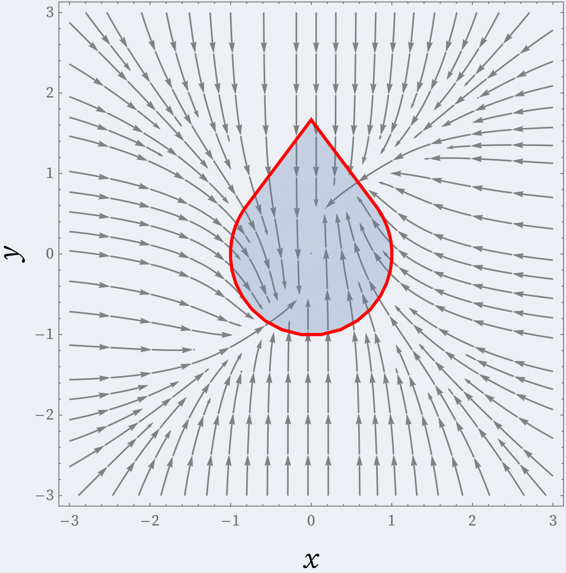
$$S \equiv (A_{11} \wedge A_{12}) \vee A_{21} \vee A_{31} \; (k = 3,\ m = m_1 = 2,\ m_2 = m_3 = 1).$$

The procedure $\mathrm{NonEmpty}_f(S, \mathrm{T})$ calls Reduce 4 times:

$$\mathrm{Reduce}\ \exists x_1 \ldots \exists x_n.\ \mathrm{Exit}_f(A_{11}) \wedge A_{12} \wedge \neg \mathrm{In}_f(A_{21} \vee A_{31})$$
$$\mathrm{Reduce}\ \exists x_1 \ldots \exists x_n.\ \mathrm{Exit}_f(A_{12}) \wedge A_{11} \wedge \neg \mathrm{In}_f(A_{21} \vee A_{31})$$
$$\mathrm{Reduce}\ \exists x_1 \ldots \exists x_n.\ \mathrm{Exit}_f(A_{21}) \wedge \neg \mathrm{In}_f((A_{11} \wedge A_{12}) \vee A_{31})$$
$$\mathrm{Reduce}\ \exists x_1 \ldots \exists x_n.\ \mathrm{Exit}_f(A_{31}) \wedge \neg \mathrm{In}_f((A_{11} \wedge A_{12}) \vee A_{21})$$

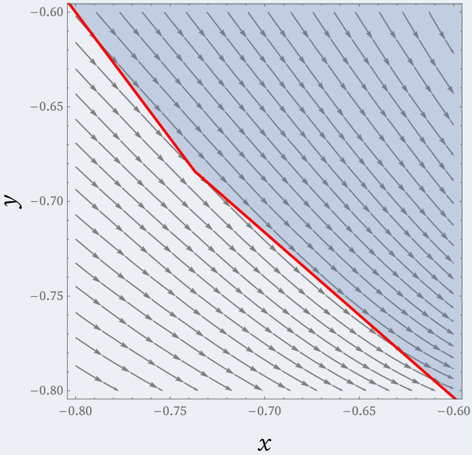
Examples

» The droplet ...



» ... is leaking!

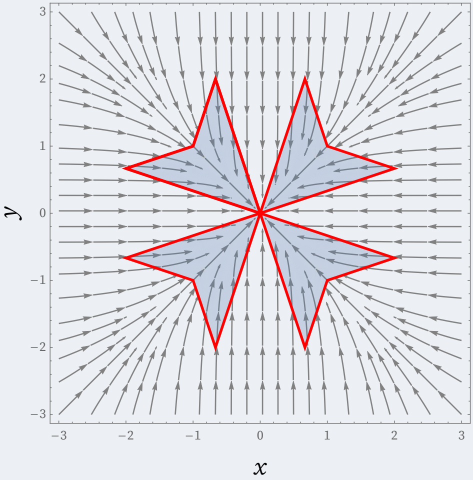
ES took 0.3s to prove falsity while **LZZ** gave no answer (> 4h)



» Maltese cross

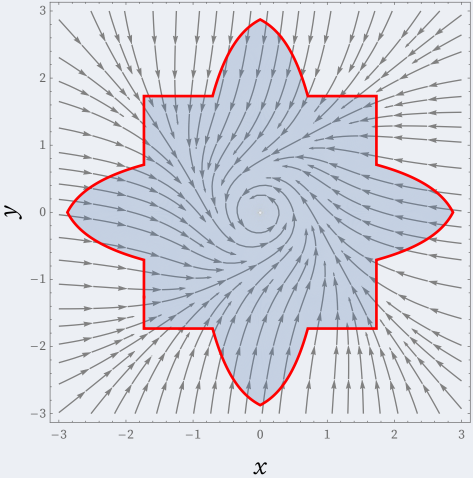
semi-linear invariant

ES proved invariance in 164s while **LZZ** gave no answer (> 4h)



» Semi-algebraic invariant

ES proved invariance in 7s and **LZZ** in 30mn



» Ongoing/Future work

- Experiment with RAGLib
- What is the best encoding for S?
- What are the topological spaces for which $\mathrm{In}_f(S_1 \cup S_2) = \mathrm{In}_f(S_1) \cup \mathrm{In}_f(S_2)$?

Thanks for attending!

More details available here
`https://arxiv.org/abs/2009.09797`