Characterization and Automated Computation of Invariant Algebraic Sets for Algebraic Differential Equations

Khalil Ghorbal

Carnegie Mellon University

KIT, Karlsruhe, Germany
September 10th, 2014

Context: Hybrid Systems Model

`Sensing`: `read data from sensors`

Context: Hybrid Systems Model

Sensing: read data from sensors
Control: actuate

Context: Hybrid Systems Model

`Sensing`: `read data from sensors`

`Control`: `actuate`

`Plant`: `evolve`

Context: Hybrid Systems Model

```
(
Sensing: read data from sensors
Control: actuate
Plant: evolve
)*
```

Context: Hybrid Systems Model

Init

$\longrightarrow$

(

Sensing: `read data from sensors`

Control: `actuate`

Plant: `evolve`

$)^*$

Safety

Context: Hybrid Systems Model

Init

$\longrightarrow$

[

(

Sensing: read data from sensors

Control: actuate

Plant: evolve

$)^*$

]

Safety

Context: Hybrid Systems Model

Init

$\longrightarrow$

[

(

Sensing: read data from sensors

Control: actuate

Plant: evolve ◀ ◀ ◀ ◀ ◀

$)^*$

]

Safety

Evolution

- Continuous time
- Ordinary Differential Equations (ODE)

Related work: Handling the continuous part

- Solutions are hard to compute symbolically
- No closed form solution exists in general
- Alternatives
  - Local approximations (Taylor series) [Lanotte et al. 2005]
  - Inductive (differential) Invariants [Maths, ThPhy 1870-] [Control 1900-] [FM 2001-]
- Limitations
  - Linear differential equations [Tiwari et al. 2003-]
  - Restrictive subclasses of Invariants [Sankaranarayanan et al 2006-, Matringe et al. 2009-, Platzer 2010]
  - Expensive procedure [Liu et al. 2011]

Related work: Handling the continuous part

- Solutions are hard to compute symbolically
- No closed form solution exists in general
- Alternatives
  - Local approximations (Taylor series) [Lanotte et al. 2005]
  - Inductive (differential) Invariants [Maths, ThPhy 1870-] [Control 1900-] [FM 2001-]
- Limitations
  - Linear differential equations [Tiwari et al. 2003-]
  - Restrictive subclasses of Invariants [Sankaranarayanan et al 2006-, Matringe et al. 2009-, Platzer 2010]
  - Expensive procedure [Liu et al. 2011]

Related work: Handling the continuous part

- Solutions are hard to compute symbolically
- No closed form solution exists in general
- Alternatives
  - Local approximations (Taylor series) [Lanotte et al. 2005]
  - Inductive (differential) Invariants [Maths, ThPhy 1870-] [Control 1900-] [FM 2001-]
- Limitations
  - Linear differential equations [Tiwari et al. 2003-]
  - Restrictive subclasses of Invariants [Sankaranarayanan et al 2006-, Matringe et al. 2009-, Platzer 2010]
  - Expensive procedure [Liu et al. 2011]

Related work: Handling the continuous part

- Solutions are hard to compute symbolically
- No closed form solution exists in general
- Alternatives
  - Local approximations (Taylor series) [Lanotte et al. 2005]
  - Inductive (differential) Invariants [Maths, ThPhy 1870-] [Control 1900-] [FM 2001-]
- Limitations
  - Linear differential equations [Tiwari et al. 2003-]
  - Restrictive subclasses of Invariants [Sankaranarayanan et al 2006-, Matringe et al. 2009-, Platzer 2010]
  - Expensive procedure [Liu et al. 2011]

Related work: Handling the continuous part

- Solutions are hard to compute symbolically
- No closed form solution exists in general
- Alternatives
  - Local approximations (Taylor series) [Lanotte et al. 2005]
  - Inductive (differential) Invariants [Maths, ThPhy 1870-] [Control 1900-] [FM 2001-]
- Limitations

This talk

  - Linear differential equations [Tiwari et al. 2003-]
  - Restrictive subclasses of Invariants [Sankaranarayanan et al 2006-, Matringe et al. 2009-, Platzer 2010]
  - Expensive procedure [Liu et al. 2011]

Related work: Handling the continuous part

- Solutions are hard to compute symbolically
- No closed form solution exists in general
- Alternatives
  - Local approximations (Taylor series) [Lanotte et al. 2005]
  - Inductive (differential) Invariants [Maths, ThPhy 1870-] [Control 1900-] [FM 2001-]
- Limitations

This talk

  - Linear differential equations [Tiwari et al. 2003-]

Polynomial

  - Restrictive subclasses of Invariants [Sankaranarayanan et al 2006-, Matringe et al. 2009-, Platzer 2010]
  - Expensive procedure [Liu et al. 2011]

Related work: Handling the continuous part

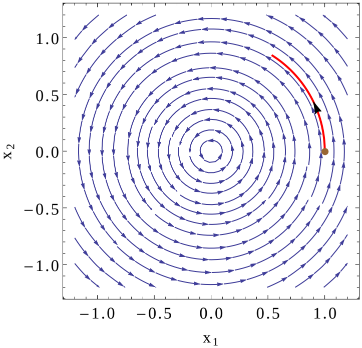
- Solutions are hard to compute symbolically
- No closed form solution exists in general
- Alternatives
  - Local approximations (Taylor series) [Lanotte et al. 2005]
  - Inductive (differential) Invariants [Maths, ThPhy 1870-] [Control 1900-] [FM 2001-]
- Limitations — This talk
  - Linear differential equations [Tiwari et al. 2003-] — **Polynomial**
  - Restrictive subclasses of Invariants — **All Algebraic Sets** [Sankaranarayanan et al 2006-, Matringe et al. 2009-, Platzer 2010]
  - Expensive procedure [Liu et al. 2011]

Related work: Handling the continuous part

- Solutions are hard to compute symbolically
- No closed form solution exists in general
- Alternatives
  - Local approximations (Taylor series) [Lanotte et al. 2005]
  - Inductive (differential) Invariants [Maths, ThPhy 1870-] [Control 1900-] [FM 2001-]
- Limitations — This talk
  - Linear differential equations [Tiwari et al. 2003-] — **Polynomial**
  - Restrictive subclasses of Invariants [Sankaranarayanan et al 2006-, Matringe et al. 2009-, Platzer 2010] — **All Algebraic Sets**
  - Expensive procedure [Liu et al. 2011] — **Efficient**

Algebraic Invariant Equations

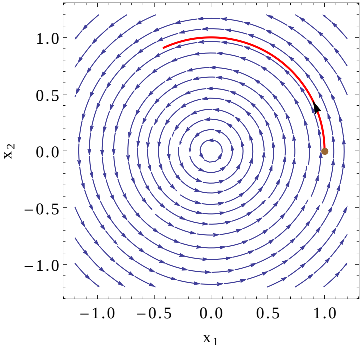
$$(\dot{x}_1, \dot{x}_2) = (-x_2, x_1)$$



The solution for $\mathbf{x}_0 = (1, 0)$ for $t = [0, 1]$

Algebraic Invariant Equations

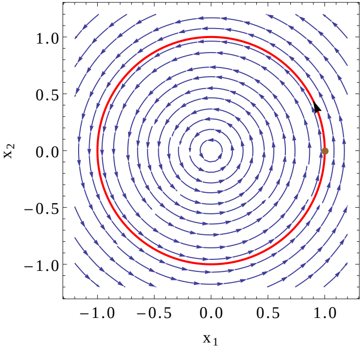
$$(\dot{x}_1, \dot{x}_2) = (-x_2, x_1)$$



The solution for $\mathbf{x}_0 = (1, 0)$ for $t = [0, 2]$

Algebraic Invariant Equations

$$(\dot{x}_1, \dot{x}_2) = (-x_2, x_1)$$

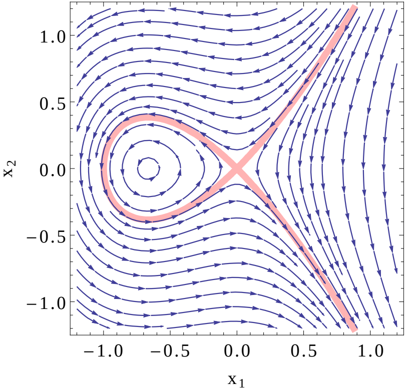


Algebraic Invariant Equation

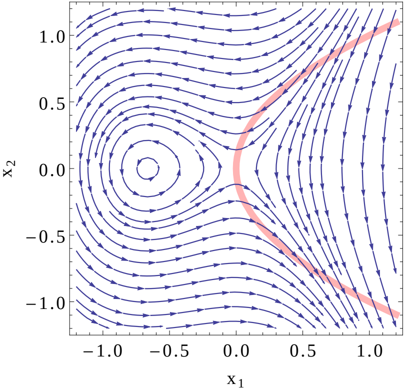
The solution for $\mathbf{x}_0 = (1, 0)$ respects $\boxed{x_1(t)^2 + x_2(t)^2 - 1 = 0}$ $\forall t$

Problem I. *Checking the invariance of Algebraic Equations*

Given $\dot{\mathbf{x}} = \mathbf{p}$, and $\mathbf{x}_0$ such that $h(\mathbf{x}_0) = 0$, is $h(\mathbf{x}(t)) = 0$ for all t ?



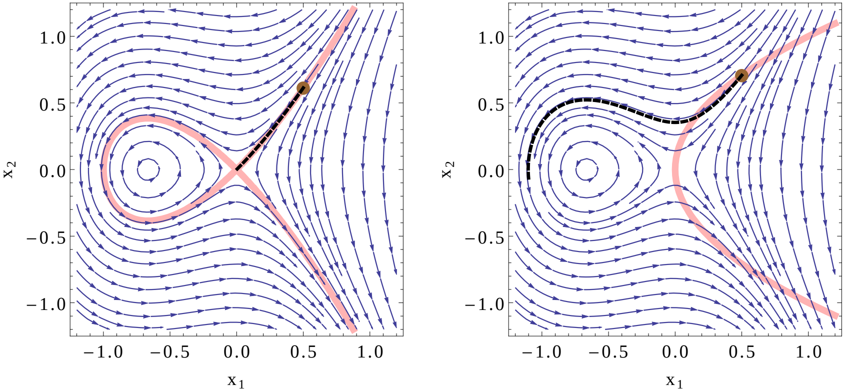
$h(x_1, x_2) = x_1^2 + x_1^3 - x_2^2$



$h(x_1, x_2) = x_1 - x_2^2$

Problem I. *Checking the invariance of Algebraic Equations*

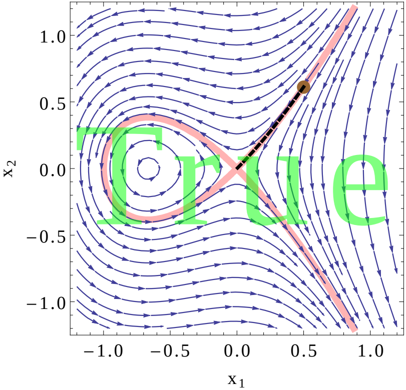
Given $\dot{\mathbf{x}} = \mathbf{p}$, and $\mathbf{x}_0$ such that $h(\mathbf{x}_0) = 0$, is $h(\mathbf{x}(t)) = 0$ for all t ?



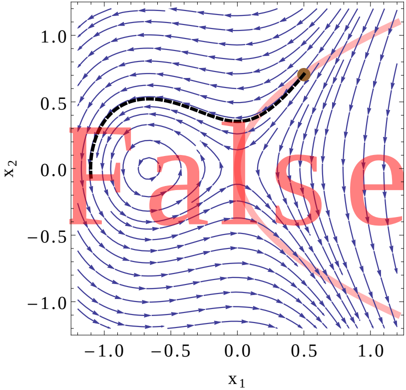
$$h(x_1, x_2) = x_1^2 + x_1^3 - x_2^2 \qquad h(x_1, x_2) = x_1 - x_2^2$$

Problem I. *Checking the invariance of Algebraic Equations*

Given $\dot{\mathbf{x}} = \mathbf{p}$, and $\mathbf{x}_0$ such that $h(\mathbf{x}_0) = 0$, is $h(\mathbf{x}(t)) = 0$ for all t ?

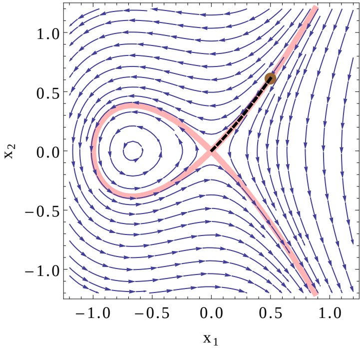


$$h(x_1, x_2) = x_1^2 + x_1^3 - x_2^2$$



$$h(x_1, x_2) = x_1 - x_2^2$$

Abstracting Orbits Using Algebraic Sets



Concrete Domain

The trajectory of the solution of an Initial Value Problem ($\dot{\mathbf{x}} = \mathbf{f}$, $\mathbf{x}_0$).

Abstract Domain

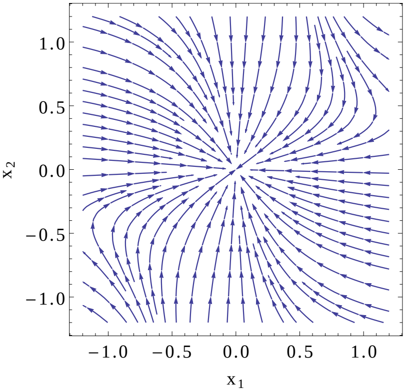
Algebraic Sets.

Problem: Checking soundness

Checking the soundness of the abstraction: does a given algebraic set overapproximate the trajectory of the solution ?

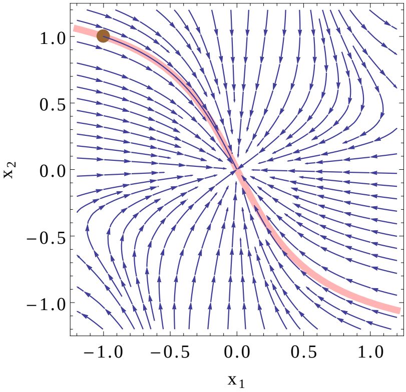
Problem II. *Generate Algebraic Invariant Equations*

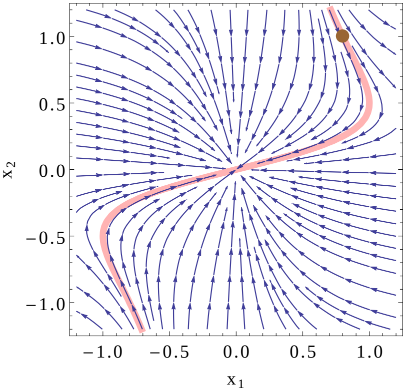
Given $\dot{\mathbf{x}} = \mathbf{p}$, how to generate h such that $h(\mathbf{x}(t)) = 0$?



Problem II. *Generate Algebraic Invariant Equations*

Given $\dot{\mathbf{x}} = \mathbf{p}$, how to generate h such that $h(\mathbf{x}(t)) = 0$?





$$h_{(x_1(0),x_2(0))}(x_1, x_2) = (x_2(0) - x_1(0)x_2(0)^2)x_1 - x_1(0)(x_2 - x_1 x_2^2)$$

Outline

Some definitions

Lie Derivative along a vector field $\dot{\mathbf{x}} = \mathbf{f}$

$$\mathfrak{D}(p) \stackrel{\text{def}}{=} \sum_{i=1}^{n} \frac{\partial p}{\partial x_i} \dot{\mathbf{x}}_i = \sum_{i=1}^{n} \frac{\partial p}{\partial x_i} \mathbf{f}_i = \frac{dp(\mathbf{x}(t))}{dt}$$

Higher-order Lie derivatives:

$$\mathfrak{D}^{(k+1)}(p) = \mathfrak{D}(\mathfrak{D}^{(k)}(p))$$

Ideal Membership

$$\exists \lambda_i \in \mathbb{R}[\mathbf{x}] : p = \lambda_1 q_1 + \cdots + \lambda_r q_r \quad \leftrightarrow \quad p \in \langle q_1, \ldots, q_r \rangle$$

Ideal membership can be checked effectively using Gröbner bases algorithm.

Checking Invariance of Candidates

Already existing proof rules

I. Checking the invariance of Algebraic Equations

Given $\dot{\mathbf{x}} = \mathbf{p}$, and $\mathbf{x}_0$ such that $h(\mathbf{x}_0) = 0$, is $h(\mathbf{x}(t)) = 0$ for all t ?

$$\mathfrak{D}(h) = \lambda h \quad (\lambda \in \mathbb{R}[\mathbf{x}])$$

$$\frac{\mathfrak{D}(h) = 0}{(h = 0) \to [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

Checking Invariance of Candidates

Already existing proof rules

I. Checking the invariance of Algebraic Equations

Given $\dot{\mathbf{x}} = \mathbf{p}$, and $\mathbf{x}_0$ such that $h(\mathbf{x}_0) = 0$, is $h(\mathbf{x}(t)) = 0$ for all t ?

$$\frac{\mathfrak{D}(h) = \lambda h \quad (\lambda \in \mathbb{R}[\mathbf{x}]) \qquad \mathfrak{D}(h) = 0}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

Checking Invariance of Candidates

Already existing proof rules

I. Checking the invariance of Algebraic Equations

Given $\dot{\mathbf{x}} = \mathbf{p}$, and $\mathbf{x}_0$ such that $h(\mathbf{x}_0) = 0$, is $h(\mathbf{x}(t)) = 0$ for all t ?

$$\dfrac{\begin{array}{c} h = 0 \longrightarrow \mathfrak{D}(h) = 0 \\ \mathfrak{D}(h) = \lambda h \quad (\lambda \in \mathbb{R}[\mathbf{x}]) \\ \mathfrak{D}(h) = 0 \end{array}}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

Checking Invariance of Candidates

Already existing proof rules

I. Checking the invariance of Algebraic Equations

Given $\dot{\mathbf{x}} = \mathbf{p}$, and $\mathbf{x}_0$ such that $h(\mathbf{x}_0) = 0$, is $h(\mathbf{x}(t)) = 0$ for all t ?

$$\frac{\begin{array}{c} h = 0 \longrightarrow \mathfrak{D}(h) = 0 \quad \text{(unsound)} \\ \mathfrak{D}(h) = \lambda h \quad (\lambda \in \mathbb{R}[\mathbf{x}]) \\ \mathfrak{D}(h) = 0 \end{array}}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

Checking Invariance of Candidates

Already existing proof rules

I. Checking the invariance of Algebraic Equations

Given $\dot{\mathbf{x}} = \mathbf{p}$, and $\mathbf{x}_0$ such that $h(\mathbf{x}_0) = 0$, is $h(\mathbf{x}(t)) = 0$ for all t ?

$$\frac{h = 0 \overset{?}{\longrightarrow} \mathfrak{D}(h) = 0 \quad \text{(unsound)} \qquad \mathfrak{D}(h) = \lambda h \quad (\lambda \in \mathbb{R}[\mathbf{x}]) \qquad \mathfrak{D}(h) = 0}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

Checking Invariance of Candidates

Example

I. Checking the invariance of Algebraic Equations

Given $\dot{\mathbf{x}} = \mathbf{p}$, and $\mathbf{x}_0$ such that $h(\mathbf{x}_0) = 0$, is $h(\mathbf{x}(t)) = 0$ for all t ?

- $(\dot{x}_1, \dot{x}_2) = (x_2, x_1)$
- $h = x_1^2 + x_2^2$
- $\mathfrak{D}(h) = 2x_1\mathfrak{D}(x_1) + 2x_2\mathfrak{D}(x_2) = 4x_1x_2$ (Chain Rule)
- $\mathfrak{D}^{(2)}(h) = 4(x_1^2 + x_2^2)$

$$\dfrac{\begin{array}{c}\mathfrak{D}^{(2)}(h) = 4h \\ \textbf{No } \lambda \in \mathbb{R}[x] \text{ s.t. } 4x_1x_2 = \lambda(x_1^2 + x_2^2) \\ \mathfrak{D}(h) = 4x_1x_2 \neq 0\end{array}}{(h = 0) \to [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

Checking Invariance of Candidates

Example

I. Checking the invariance of Algebraic Equations

Given $\dot{\mathbf{x}} = \mathbf{p}$, and $\mathbf{x}_0$ such that $h(\mathbf{x}_0) = 0$, is $h(\mathbf{x}(t)) = 0$ for all t ?

- $(\dot{x}_1, \dot{x}_2) = (x_2, x_1)$
- $h = x_1^2 + x_2^2$
- $\mathfrak{D}(h) = 2x_1\mathfrak{D}(x_1) + 2x_2\mathfrak{D}(x_2) = 4x_1x_2$ (Chain Rule)
- $\mathfrak{D}^{(2)}(h) = 4(x_1^2 + x_2^2)$

$$\mathfrak{D}^{(2)}(h) = 4h$$

No $\lambda \in \mathbb{R}[x]$ s.t. $4x_1x_2 = \lambda(x_1^2 + x_2^2)$

$$\frac{\mathfrak{D}(h) = 4x_1x_2 \neq 0}{(h = 0) \to [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

Checking Invariance of Candidates

Example

I. Checking the invariance of Algebraic Equations

Given $\dot{\mathbf{x}} = \mathbf{p}$, and $\mathbf{x}_0$ such that $h(\mathbf{x}_0) = 0$, is $h(\mathbf{x}(t)) = 0$ for all t ?

- $(\dot{x}_1, \dot{x}_2) = (x_2, x_1)$
- $h = x_1^2 + x_2^2$
- $\mathfrak{D}(h) = 2x_1\mathfrak{D}(x_1) + 2x_2\mathfrak{D}(x_2) = 4x_1x_2$ (Chain Rule)
- $\mathfrak{D}^{(2)}(h) = 4(x_1^2 + x_2^2)$

$$\mathfrak{D}^{(2)}(h) = 4h$$

No $\lambda \in \mathbb{R}[x]$ s.t. $4x_1x_2 = \lambda(x_1^2 + x_2^2)$

$$\frac{\mathfrak{D}(h) = 4x_1x_2 \neq 0}{(h = 0) \to [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

Checking Invariance of Candidates

Example

I. Checking the invariance of Algebraic Equations

Given $\dot{\mathbf{x}} = \mathbf{p}$, and $\mathbf{x}_0$ such that $h(\mathbf{x}_0) = 0$, is $h(\mathbf{x}(t)) = 0$ for all t ?

- $(\dot{x}_1, \dot{x}_2) = (x_2, x_1)$
- $h = x_1^2 + x_2^2$
- $\mathfrak{D}(h) = 2x_1\mathfrak{D}(x_1) + 2x_2\mathfrak{D}(x_2) = 4x_1x_2$ (Chain Rule)
- $\mathfrak{D}^{(2)}(h) = 4(x_1^2 + x_2^2)$

$$\mathfrak{D}^{(2)}(h) = 4h$$

$$\frac{\textbf{No } \lambda \in \mathbb{R}[x] \text{ s.t. } 4x_1x_2 = \lambda(x_1^2 + x_2^2) \qquad \mathfrak{D}(h) = 4x_1x_2 \neq 0}{(h = 0) \to [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

Checking Invariance of Candidates

Example

I. Checking the invariance of Algebraic Equations

Given $\dot{\mathbf{x}} = \mathbf{p}$, and $\mathbf{x}_0$ such that $h(\mathbf{x}_0) = 0$, is $h(\mathbf{x}(t)) = 0$ for all t ?

- $(\dot{x}_1, \dot{x}_2) = (x_2, x_1)$
- $h = x_1^2 + x_2^2$
- $\mathfrak{D}(h) = 2x_1\mathfrak{D}(x_1) + 2x_2\mathfrak{D}(x_2) = 4x_1x_2$ (Chain Rule)
- $\mathfrak{D}^{(2)}(h) = 4(x_1^2 + x_2^2)$

$$\frac{\mathfrak{D}^{(2)}(h) = 4h \qquad \textbf{No } \lambda \in \mathbb{R}[x] \text{ s.t. } 4x_1x_2 = \lambda(x_1^2 + x_2^2) \qquad \mathfrak{D}(h) = 4x_1x_2 \neq 0}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

Checking Invariance of Candidates

Example

I. Checking the invariance of Algebraic Equations

Given $\dot{\mathbf{x}} = \mathbf{p}$, and $\mathbf{x}_0$ such that $h(\mathbf{x}_0) = 0$, is $h(\mathbf{x}(t)) = 0$ for all t ?

- $(\dot{x}_1, \dot{x}_2) = (x_2, x_1)$
- $h = x_1^2 + x_2^2$
- $\mathfrak{D}(h) = 2x_1\mathfrak{D}(x_1) + 2x_2\mathfrak{D}(x_2) = 4x_1x_2$ (Chain Rule)
- $\mathfrak{D}^{(2)}(h) = 4(x_1^2 + x_2^2)$

still unsound! (counterexample: $h = x_1$)

$$\mathfrak{D}^{(2)}(h) = 4h$$

No $\lambda \in \mathbb{R}[x]$ s.t. $4x_1x_2 = \lambda(x_1^2 + x_2^2)$

$$\mathfrak{D}(h) = 4x_1x_2 \neq 0$$

$$\frac{}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

Checking Invariance of Candidates

Differential Radical Invariants [Theorem 2, TACAS'14]

$$\mathfrak{D}^{(N)}(h) = \sum_{i=0}^{N-1} \lambda_i \mathfrak{D}^{(i)}(h)\ (\lambda_i \in \mathbb{R}[\mathbf{x}])\ \wedge\ h = 0 \rightarrow \bigwedge_{i=1}^{N-1} \mathfrak{D}^{(i)}(h) = 0$$

$$\cdots$$

$$\mathfrak{D}^{(3)}(h) = \sum_{i=0}^{2} \lambda_i \mathfrak{D}^{(i)}(h)\ (\lambda_i \in \mathbb{R}[\mathbf{x}])\ \wedge\ h = 0 \rightarrow \bigwedge_{i=1}^{2} \mathfrak{D}^{(i)}(h) = 0$$

$$\mathfrak{D}^{(2)}(h) = \lambda_0 h + \lambda_1 \mathfrak{D}(h)\ (\lambda_i \in \mathbb{R}[\mathbf{x}])\ \wedge\ h = 0 \rightarrow \mathfrak{D}(h) = 0$$

$$\frac{\mathfrak{D}(h) = \lambda h\ (\lambda \in \mathbb{R}[\mathbf{x}])}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

- order N is **finite**
- **Necessary** and **sufficient** condition
- **Decidable**
  - Existence of λ_i: Gröbner Basis
  - $h = 0 \rightarrow \mathfrak{D}^{(i)}(h) = 0$: Quantifier Elimination

Checking Invariance of Candidates

Differential Radical Invariants [Theorem 2, TACAS'14]

$$\frac{\begin{array}{c}\mathfrak{D}^{(N)}(h) = \sum_{i=0}^{N-1} \lambda_i \mathfrak{D}^{(i)}(h) \; (\lambda_i \in \mathbb{R}[\mathbf{x}]) \;\wedge\; h = 0 \rightarrow \bigwedge_{i=1}^{N-1} \mathfrak{D}^{(i)}(h) = 0 \\ \dots \\ \mathfrak{D}^{(3)}(h) = \sum_{i=0}^{2} \lambda_i \mathfrak{D}^{(i)}(h) \; (\lambda_i \in \mathbb{R}[\mathbf{x}]) \;\wedge\; h = 0 \rightarrow \bigwedge_{i=1}^{2} \mathfrak{D}^{(i)}(h) = 0 \\ \mathfrak{D}^{(2)}(h) = \lambda_0 h + \lambda_1 \mathfrak{D}(h) \; (\lambda_i \in \mathbb{R}[\mathbf{x}]) \;\wedge\; h = 0 \rightarrow \mathfrak{D}(h) = 0 \\ \mathfrak{D}(h) = \lambda h \; (\lambda \in \mathbb{R}[\mathbf{x}])\end{array}}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

- order N is **finite**
- **Necessary** and **sufficient** condition
- **Decidable**
  - Existence of λ_i: Gröbner Basis
  - $h = 0 \rightarrow \mathfrak{D}^{(i)}(h) = 0$: Quantifier Elimination

Checking Invariance of Candidates

Differential Radical Invariants [Theorem 2, TACAS'14]

$$\mathfrak{D}^{(N)}(h) = \sum_{i=0}^{N-1} \lambda_i \mathfrak{D}^{(i)}(h)\ (\lambda_i \in \mathbb{R}[\mathbf{x}])\ \wedge\ h = 0 \rightarrow \bigwedge_{i=1}^{N-1} \mathfrak{D}^{(i)}(h) = 0$$

$$\cdots$$

$$\mathfrak{D}^{(3)}(h) = \sum_{i=0}^{2} \lambda_i \mathfrak{D}^{(i)}(h)\ (\lambda_i \in \mathbb{R}[\mathbf{x}])\ \wedge\ h = 0 \rightarrow \bigwedge_{i=1}^{2} \mathfrak{D}^{(i)}(h) = 0$$

$$\mathfrak{D}^{(2)}(h) = \lambda_0 h + \lambda_1 \mathfrak{D}(h)\ (\lambda_i \in \mathbb{R}[\mathbf{x}])\ \wedge\ h = 0 \rightarrow \mathfrak{D}(h) = 0$$

$$\mathfrak{D}(h) = \lambda h\ (\lambda \in \mathbb{R}[\mathbf{x}])$$

$$\overline{}$$

$$(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)$$

- order N is **finite**
- **Necessary** and **sufficient** condition
- **Decidable**
  - Existence of λ_i: Gröbner Basis
  - $h = 0 \rightarrow \mathfrak{D}^{(i)}(h) = 0$: Quantifier Elimination

Checking Invariance of Candidates

Differential Radical Invariants [Theorem 2, TACAS'14]

$$\frac{\begin{array}{c}\mathfrak{D}^{(N)}(h) = \sum_{i=0}^{N-1} \lambda_i \mathfrak{D}^{(i)}(h)\ (\lambda_i \in \mathbb{R}[\mathbf{x}])\ \wedge\ h = 0 \rightarrow \bigwedge_{i=1}^{N-1} \mathfrak{D}^{(i)}(h) = 0 \\ \cdots \\ \mathfrak{D}^{(3)}(h) = \sum_{i=0}^{2} \lambda_i \mathfrak{D}^{(i)}(h)\ (\lambda_i \in \mathbb{R}[\mathbf{x}])\ \wedge\ h = 0 \rightarrow \bigwedge_{i=1}^{2} \mathfrak{D}^{(i)}(h) = 0 \\ \mathfrak{D}^{(2)}(h) = \lambda_0 h + \lambda_1 \mathfrak{D}(h)\ (\lambda_i \in \mathbb{R}[\mathbf{x}])\ \wedge\ h = 0 \rightarrow \mathfrak{D}(h) = 0 \\ \mathfrak{D}(h) = \lambda h\ (\lambda \in \mathbb{R}[\mathbf{x}])\end{array}}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

- order N is **finite**
- **Necessary** and **sufficient** condition
- **Decidable**
  - Existence of λ_i: Gröbner Basis
  - $h = 0 \rightarrow \mathfrak{D}^{(i)}(h) = 0$: Quantifier Elimination

Checking Invariance of Candidates

Differential Radical Invariants [Theorem 2, TACAS'14]

$$\frac{\begin{array}{c}\mathfrak{D}^{(N)}(h) = \sum_{i=0}^{N-1} \lambda_i \mathfrak{D}^{(i)}(h)\ (\lambda_i \in \mathbb{R}[\mathbf{x}]) \ \wedge\ h = 0 \to \bigwedge_{i=1}^{N-1} \mathfrak{D}^{(i)}(h) = 0 \\ \cdots \\ \mathfrak{D}^{(3)}(h) = \sum_{i=0}^{2} \lambda_i \mathfrak{D}^{(i)}(h)\ (\lambda_i \in \mathbb{R}[\mathbf{x}]) \ \wedge\ h = 0 \to \bigwedge_{i=1}^{2} \mathfrak{D}^{(i)}(h) = 0 \\ \mathfrak{D}^{(2)}(h) = \lambda_0 h + \lambda_1 \mathfrak{D}(h)\ (\lambda_i \in \mathbb{R}[\mathbf{x}]) \ \wedge\ h = 0 \to \mathfrak{D}(h) = 0 \\ \mathfrak{D}(h) = \lambda h\ (\lambda \in \mathbb{R}[\mathbf{x}])\end{array}}{(h = 0) \to [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

- order N is **finite**
- **Necessary** and **sufficient** condition
- **Decidable**
  - Existence of λ_i: Gröbner Basis
  - $h = 0 \to \mathfrak{D}^{(i)}(h) = 0$: Quantifier Elimination

Checking Invariance of Candidates

Differential Radical Invariants [Theorem 2, TACAS'14]

$$\dfrac{\begin{array}{c}\mathfrak{D}^{(N)}(h) = \sum_{i=0}^{N-1} \lambda_i \mathfrak{D}^{(i)}(h) \ (\lambda_i \in \mathbb{R}[\mathbf{x}]) \ \wedge \ h = 0 \rightarrow \bigwedge_{i=1}^{N-1} \mathfrak{D}^{(i)}(h) = 0 \\ \cdots \\ \mathfrak{D}^{(3)}(h) = \sum_{i=0}^{2} \lambda_i \mathfrak{D}^{(i)}(h) \ (\lambda_i \in \mathbb{R}[\mathbf{x}]) \ \wedge \ h = 0 \rightarrow \bigwedge_{i=1}^{2} \mathfrak{D}^{(i)}(h) = 0 \\ \mathfrak{D}^{(2)}(h) = \lambda_0 h + \lambda_1 \mathfrak{D}(h) \ (\lambda_i \in \mathbb{R}[\mathbf{x}]) \ \wedge \ h = 0 \rightarrow \mathfrak{D}(h) = 0 \\ \mathfrak{D}(h) = \lambda h \ (\lambda \in \mathbb{R}[\mathbf{x}])\end{array}}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}$$

- order N is **finite**
- **Necessary** and **sufficient** condition
- **Decidable**
  - Existence of λ_i: Gröbner Basis
  - $h = 0 \rightarrow \mathfrak{D}^{(i)}(h) = 0$: Quantifier Elimination

Checking Invariance of Candidates

Differential Radical Invariants [Theorem 2, TACAS'14]

$$\mathfrak{D}^{(N)}(h) = \sum_{i=0}^{N-1} \lambda_i \mathfrak{D}^{(i)}(h)\ (\lambda_i \in \mathbb{R}[\mathbf{x}])\ \wedge\ h = 0 \rightarrow \bigwedge_{i=1}^{N-1} \mathfrak{D}^{(i)}(h) = 0$$

$$\cdots$$

$$\mathfrak{D}^{(3)}(h) = \sum_{i=0}^{2} \lambda_i \mathfrak{D}^{(i)}(h)\ (\lambda_i \in \mathbb{R}[\mathbf{x}])\ \wedge\ h = 0 \rightarrow \bigwedge_{i=1}^{2} \mathfrak{D}^{(i)}(h) = 0$$

$$\mathfrak{D}^{(2)}(h) = \lambda_0 h + \lambda_1 \mathfrak{D}(h)\ (\lambda_i \in \mathbb{R}[\mathbf{x}])\ \wedge\ h = 0 \rightarrow \mathfrak{D}(h) = 0$$

$$\mathfrak{D}(h) = \lambda h\ (\lambda \in \mathbb{R}[\mathbf{x}])$$

$$(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)$$

- order N is **finite**
- **Necessary** and **sufficient** condition
- **Decidable**
  - Existence of λ_i: Gröbner Basis
  - $h = 0 \rightarrow \mathfrak{D}^{(i)}(h) = 0$: Quantifier Elimination

Naïve Approach: DRI + Sum of Squares

$$p = 0 \wedge q = 0$$

$$\equiv_{\mathbb{R}}$$

$$p^2 + q^2 = 0$$

$$(\text{SoSDRI})\frac{(p^2 + q^2 = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p^2 + q^2 = 0)}{(p = 0 \wedge q = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p = 0 \wedge q = 0)}$$

Drawback: Bad complexity

+ Already decides algebraic invariants
− Increases total polynomial degree

Conjunctive Differential Radical Characterization

Theorem 2, Algorithm 1, [SAS'14]

$$\frac{\begin{array}{c}\mathfrak{D}^{(N_{p,q})}(p), \mathfrak{D}^{(N_{p,q})}(q) \in \langle p, q, \ldots, \mathfrak{D}^{(N_{p,q}-1)}(p), \mathfrak{D}^{(N_{p,q}-1)}(q)\rangle \\ \wedge \ \ p = 0 \wedge q = 0 \rightarrow \mathfrak{D}^{(N_{p,q}-1)}(p) = 0 \wedge \mathfrak{D}^{(N_{p,q}-1)}(q) = 0 \\ \ldots \\ \mathfrak{D}^{(2)}(p), \mathfrak{D}^{(2)}(q) \in \langle p, q, \mathfrak{D}(p), \mathfrak{D}(q)\rangle \\ \wedge \ \ p = 0 \wedge q = 0 \rightarrow \mathfrak{D}(p) = 0 \wedge \mathfrak{D}(q) = 0 \\ \mathfrak{D}(p), \mathfrak{D}(q) \in \langle p, q\rangle\end{array}}{(p = 0 \wedge q = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p = 0 \wedge q = 0)}$$

- $N_{p,q}$ is defined as the length of the chain of **larger** ideals $\langle p, q\rangle$, $\langle p, q, \mathfrak{D}(p), \mathfrak{D}(q)\rangle$ ...
- $N_{p,q}$ is now **shared** between p and q; its value depends on p, q and $\mathbf{f}$.

Conjunctive Differential Radical Characterization

Theorem 2, Algorithm 1, [SAS'14]

$$\frac{\begin{array}{c}\mathfrak{D}^{(N_{p,q})}(p), \mathfrak{D}^{(N_{p,q})}(q) \in \langle p, q, \ldots, \mathfrak{D}^{(N_{p,q}-1)}(p), \mathfrak{D}^{(N_{p,q}-1)}(q)\rangle \\ \wedge\ \ p = 0 \wedge q = 0 \rightarrow \mathfrak{D}^{(N_{p,q}-1)}(p) = 0 \wedge \mathfrak{D}^{(N_{p,q}-1)}(q) = 0 \\ \ldots \\ \mathfrak{D}^{(2)}(p), \mathfrak{D}^{(2)}(q) \in \langle p, q, \mathfrak{D}(p), \mathfrak{D}(q)\rangle \\ \wedge\ \ p = 0 \wedge q = 0 \rightarrow \mathfrak{D}(p) = 0 \wedge \mathfrak{D}(q) = 0 \\ \mathfrak{D}(p), \mathfrak{D}(q) \in \langle p, q\rangle \end{array}}{(p = 0 \wedge q = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p = 0 \wedge q = 0)}$$

- $N_{p,q}$ is defined as the length of the chain of **larger** ideals $\langle p, q\rangle$, $\langle p, q, \mathfrak{D}(p), \mathfrak{D}(q)\rangle$ ...
- $N_{p,q}$ is now **shared** between p and q; its value depends on p, q and $\mathbf{f}$.

Conjunctive Differential Radical Characterization

Theorem 2, Algorithm 1, [SAS'14]

$$\frac{\begin{array}{c}\mathfrak{D}^{(N_{p,q})}(p), \mathfrak{D}^{(N_{p,q})}(q) \in \langle p, q, \ldots, \mathfrak{D}^{(N_{p,q}-1)}(p), \mathfrak{D}^{(N_{p,q}-1)}(q)\rangle \\ \wedge\ p = 0 \wedge q = 0 \rightarrow \mathfrak{D}^{(N_{p,q}-1)}(p) = 0 \wedge \mathfrak{D}^{(N_{p,q}-1)}(q) = 0 \\ \ldots \\ \mathfrak{D}^{(2)}(p), \mathfrak{D}^{(2)}(q) \in \langle p, q, \mathfrak{D}(p), \mathfrak{D}(q)\rangle \\ \wedge\ p = 0 \wedge q = 0 \rightarrow \mathfrak{D}(p) = 0 \wedge \mathfrak{D}(q) = 0 \\ \mathfrak{D}(p), \mathfrak{D}(q) \in \langle p, q\rangle\end{array}}{(p = 0 \wedge q = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p = 0 \wedge q = 0)}$$

- $N_{p,q}$ is defined as the length of the chain of **larger** ideals $\langle p, q\rangle$, $\langle p, q, \mathfrak{D}(p), \mathfrak{D}(q)\rangle$ ...
- $N_{p,q}$ is now **shared** between p and q; its value depends on p, q and $\mathbf{f}$.

Outline

Generation of Invariant Algebraic Sets

Necessary and sufficient condition [Theorem 3, TACAS'14]

II. Generate Algebraic Invariant Equations

Given $\dot{\mathbf{x}} = \mathbf{p}$, how to generate h such that $h(\mathbf{x}(t)) = 0$?

Theorem

$S \in \mathbb{R}^n$ is an invariant algebraic set **if and only if**

$$S = \text{ Set of roots of the system } \begin{cases} h & = 0 \\ & \vdots \\ \mathfrak{D}^{(N-1)}(h) & = 0 \end{cases}$$

for some polynomial h with **order N**, that is

$$\boxed{\mathfrak{D}^{(N)}(h) = \sum_{i=0}^{N-1} \lambda_i \mathfrak{D}^{(i)}(h)}$$

Generation of Invariant Algebraic Sets

First integrals vs. Local invariant regions [Theorem 4, TACAS'14]

Suppose we found h and N such that

$$\boxed{\mathfrak{D}^{(N)}(h) = \sum_{i=0}^{N-1} \lambda_i \mathfrak{D}^{(i)}(h)}$$

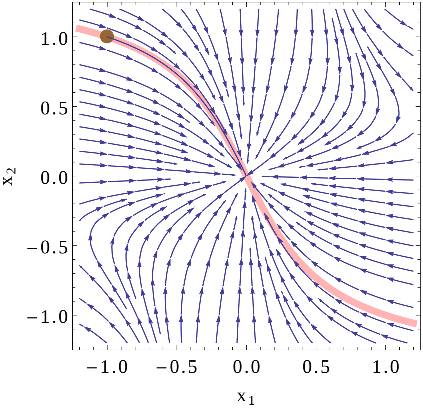
Case 1: First Integral

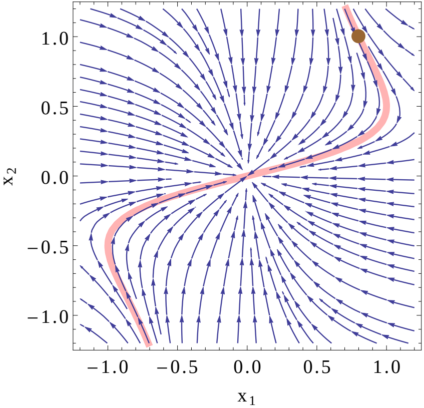
For all $\mathbf{x}_0 \in \mathbb{R}^n$, $h(\mathbf{x}_0) = 0 \wedge \cdots \wedge \mathfrak{D}^{(N-1)}(h)(\mathbf{x}_0) = 0$

Case 2: Local Invariant Regions (e.g. limiting cycle, equilibria)

Restrict $\mathbf{x}_0$ such that $h(\mathbf{x}_0) = 0 \wedge \cdots \wedge \mathfrak{D}^{(N-1)}(h)(\mathbf{x}_0) = 0$

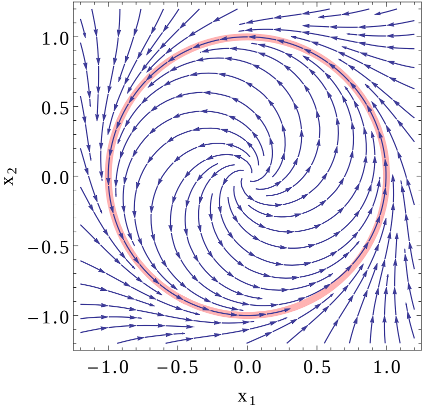
Example: First Integrals



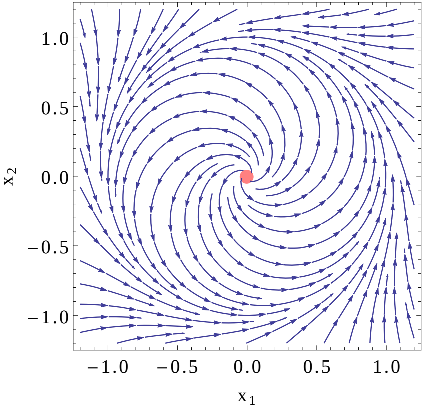


$$h_{(x_1(0),x_2(0))}(x_1, x_2) = (x_2(0) - x_1(0)x_2(0)^2)x_1 - x_1(0)(x_2 - x_1 x_2^2)$$

Example: Local invariant regions



$h(x_1, x_2) = x_1^2 + x_2^2 - 1$



$h(x_1, x_2) = x_1^2 + x_2^2$

But ...

How to **generate** h and N such that

$$\boxed{\mathfrak{D}^{(N)}(h) = \sum_{i=0}^{N-1} \lambda_i \mathfrak{D}^{(i)}(h)}$$

Matrix Representation: Intuition

$\boxed{\text{Suppose we have a 2-dimensional ODE } (\dot{x}_1, \dot{x}_2) = (x_1, x_2)}$

Matrix Representation: Intuition

$\boxed{\text{Suppose we have a 2-dimensional ODE } (\dot{x}_1, \dot{x}_2) = (x_1, x_2)}$

1. Start with parametric h of degree 1: $h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$

Matrix Representation: Intuition

$\boxed{\text{Suppose we have a 2-dimensional ODE } (\dot{x}_1, \dot{x}_2) = (x_1, x_2)}$

1. Start with parametric h of degree 1: $h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$
2. Start with $N = 1$

Matrix Representation: Intuition

$\boxed{\text{Suppose we have a 2-dimensional ODE } (\dot{x}_1, \dot{x}_2) = (x_1, x_2)}$

1. Start with parametric h of degree 1: $h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$
2. Start with $N = 1$
3. Find $\beta \in \mathbb{R}$ such that: $\mathfrak{D}(h) = \beta h$

Matrix Representation: Intuition

$\boxed{\text{Suppose we have a 2-dimensional ODE } (\dot{x}_1, \dot{x}_2) = (x_1, x_2)}$

1. Start with parametric h of degree 1: $h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$
2. Start with $N = 1$
3. Find $\beta \in \mathbb{R}$ such that: $\mathfrak{D}(h) = \beta h$

$$\mathfrak{D}(h) = \alpha_1 x_1 + \alpha_2 x_2 = \beta(\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3)$$

Matrix Representation: Intuition

$$\boxed{\text{Suppose we have a 2-dimensional ODE } (\dot{x}_1, \dot{x}_2) = (x_1, x_2)}$$

1. Start with parametric h of degree 1: $h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$
2. Start with $N = 1$
3. Find $\beta \in \mathbb{R}$ such that: $\mathfrak{D}(h) = \beta h$

$$\mathfrak{D}(h) = \alpha_1 x_1 + \alpha_2 x_2 = \beta(\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3)$$

$$\begin{aligned} (-1+\beta)\alpha_1 &= 0 \\ (-1+\beta)\alpha_2 &= 0 \\ (\beta)\alpha_3 &= 0 \end{aligned} \leftrightarrow \begin{pmatrix} -1+\beta & 0 & 0 \\ 0 & -1+\beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = 0$$

Matrix Representation: Intuition

Suppose we have a 2-dimensional ODE $(\dot{x}_1, \dot{x}_2) = (x_1, x_2)$

1. Start with parametric h of degree 1: $h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$
2. Start with $N = 1$
3. Find $\beta \in \mathbb{R}$ such that: $\mathfrak{D}(h) = \beta h$

$$\mathfrak{D}(h) = \alpha_1 x_1 + \alpha_2 x_2 = \beta(\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3)$$

$$\begin{aligned} (-1+\beta)\alpha_1 &= 0 \\ (-1+\beta)\alpha_2 &= 0 \\ (\beta)\alpha_3 &= 0 \end{aligned} \leftrightarrow \begin{pmatrix} -1+\beta & 0 & 0 \\ 0 & -1+\beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = 0$$

Study the **null space** (kernel) of $M(\beta)$

Symbolic Linear Algebra

$$h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$$

$$\begin{aligned} (-1+\beta)\alpha_1 &= 0 \\ (-1+\beta)\alpha_2 &= 0 \\ (\beta)\alpha_3 &= 0 \end{aligned} \leftrightarrow \begin{pmatrix} -1+\beta & 0 & 0 \\ 0 & -1+\beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = 0$$

Study the **null space** (kernel) of $M(\beta)$

- Max dim of ker of $M(\beta) \rightsquigarrow$ more freedom for $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$
- Increases the chances of finding **first integrals**
- Dually, minimize the rank of $M(\beta)$

Symbolic Linear Algebra

$$h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$$

$$\begin{aligned}(-1+\beta)\alpha_1 &= 0\\ (-1+\beta)\alpha_2 &= 0\\ (\beta)\alpha_3 &= 0\end{aligned} \leftrightarrow \begin{pmatrix} -1+\beta & 0 & 0\\ 0 & -1+\beta & 0\\ 0 & 0 & \beta\end{pmatrix}\begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{pmatrix} = 0$$

Study the **null space** (kernel) of $M(\beta)$

- Max dim of ker of $M(\beta) \rightsquigarrow$ more freedom for $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$
- Increases the chances of finding **first integrals**
- Dually, minimize the rank of $M(\beta)$

Symbolic Linear Algebra

$$h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$$

$$\begin{aligned} (-1+\beta)\alpha_1 &= 0 \\ (-1+\beta)\alpha_2 &= 0 \\ (\beta)\alpha_3 &= 0 \end{aligned} \leftrightarrow \begin{pmatrix} -1+\beta & 0 & 0 \\ 0 & -1+\beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = 0$$

Study the **null space** (kernel) of $M(\beta)$

- Max dim of ker of $M(\beta) \rightsquigarrow$ more freedom for $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$
- Increases the chances of finding **first integrals**
- Dually, minimize the rank of $M(\beta)$

Symbolic Linear Algebra

$$h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$$

$$\begin{aligned} (-1+\beta)\alpha_1 &= 0 \\ (-1+\beta)\alpha_2 &= 0 \\ (\beta)\alpha_3 &= 0 \end{aligned} \leftrightarrow \begin{pmatrix} -1+\beta & 0 & 0 \\ 0 & -1+\beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = 0$$

Study the **null space** (kernel) of $M(\beta)$

- Max dim of ker of $M(\beta)$ $\rightsquigarrow$ more freedom for $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$
- Increases the chances of finding **first integrals**
- Dually, minimize the rank of $M(\beta)$ $\rightsquigarrow$ **NP-hard** [Buss et al. 1999]

Symbolic Linear Algebra

$$h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$$

$$\begin{aligned} (-1+\beta)\alpha_1 &= 0 \\ (-1+\beta)\alpha_2 &= 0 \\ (\beta)\alpha_3 &= 0 \end{aligned} \leftrightarrow \begin{pmatrix} -1+\beta & 0 & 0 \\ 0 & -1+\beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = 0$$

Study the **null space** (kernel) of $M(\beta)$

- Max dim of ker of $M(\beta) \rightsquigarrow$ more freedom for $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$
- Increases the chances of finding **first integrals**
- Dually, minimize the rank of $M(\beta) \rightsquigarrow$ **NP-hard** [Buss et al. 1999]

$$h = x_2(0)x_1 - x_1(0)x_2$$

Toward a Generation Procedure ?

We started with a parametrized polynomial h of degree 1 and $N = 1 \ldots$

If no invariants:

- Increase order N versus increase the polynomial degree of h ?
- Any bound on N ?
- Any bound on the degree of h ?

Outline

Case Study: Collision Avoidance System

[AIAA'14]

Hybrid System

$$\texttt{pilot} \equiv \omega_1 := *;$$
$$\texttt{cas} \equiv (\texttt{pilot}; ?\texttt{monitor}; \texttt{evolve})^*$$

Safety Property

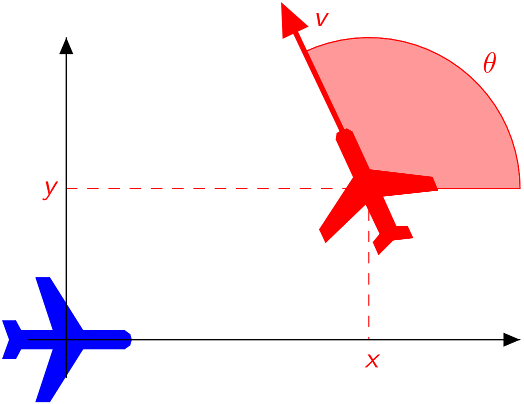
$$\texttt{safety} \equiv \forall\, t \geq 0,\ r(t) > p$$

Challenge: Synthesize `monitor` s.t.

The following d$\mathcal{L}$ formula, expressing that the safety property always holds for the whole system, is valid, i.e., true in all states:

$$\texttt{safety} \rightarrow [\texttt{cas}]\,\texttt{safety},$$

Evolution equations



$$\dot{x} = v_2 \cos\theta - v_1 + \omega_1 y$$
$$\dot{y} = v_2 \sin\theta - \omega_1 x$$
$$\dot{\theta} = \omega_2 - \omega_1$$

Synthesizing the monitor

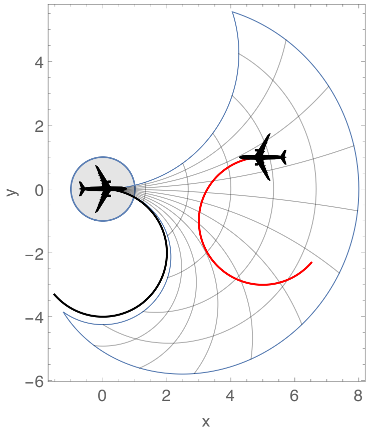
$$\texttt{monitor} \equiv (\omega_1, \omega_2) = (0,0) \longrightarrow I_1(0) > p(v_1 + v_2) \wedge$$
$$(\omega_1, \omega_2) \neq (0,0) \longrightarrow I_2(0) > 2v_1 v_2 + 2p(v_2|\omega_1| + v_1|\omega_2|) + p^2|\omega_1\omega_2|$$

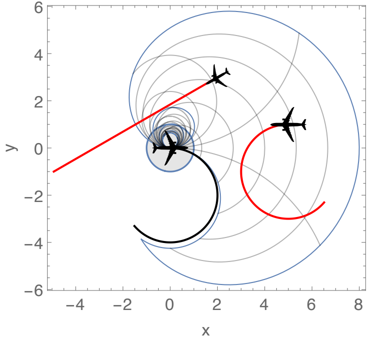
Automatically generated invariants

$$I_1(t) \stackrel{\text{def}}{=} (v_2 \sin\theta(0))x(t) - (v_2\cos\theta(0) - v_1)y(t) = I_1(0)$$

$$I_2(t) \stackrel{\text{def}}{=} -\omega_1\omega_2(x(t)^2 + y(t)^2) + 2v_2\omega_1 \sin\theta(t)x(t) + 2(v_1\omega_2 - v_2\omega_1\cos\theta(t))y(t) + 2v_1 v_2\cos\theta(t) = I_2(0)$$

Proven safe choices for the ownship





Conclusion

Checking

- **Invariance** of Algebraic Sets is **Decidable**
- **DRI** Necessary and Sufficient **Proof Rule**

Generation

- **Generation** Problem $\sim$ Symbolic **Linear Algebra**
- Equivalent to the Min Rank Problem: **NP-hard**

- **Higher-order Derivatives** are crucial
- $\boxed{\text{Real Algebraic Geometry} \leftrightharpoons \text{Logic} \leftrightharpoons \text{Verification}}$

Conclusion

Checking

- **Invariance** of Algebraic Sets is **Decidable**
- **DRI** Necessary and Sufficient **Proof Rule**

Generation

- **Generation** Problem $\sim$ Symbolic **Linear Algebra**
- Equivalent to the Min Rank Problem: **NP-hard**

- **Higher-order Derivatives** are crucial
- $\boxed{\text{Real Algebraic Geometry} \leftrightharpoons \text{Logic} \leftrightharpoons \text{Verification}}$

Conclusion

Checking

- **Invariance** of Algebraic Sets is **Decidable**
- **DRI** Necessary and Sufficient **Proof Rule**

Generation

- **Generation** Problem $\sim$ Symbolic **Linear Algebra**
- Equivalent to the Min Rank Problem: **NP-hard**

- **Higher-order Derivatives** are crucial
- $\boxed{\text{Real Algebraic Geometry} \leftrightharpoons \text{Logic} \leftrightharpoons \text{Verification}}$

Algebraic Sets Embedding

$\mathcal{O}(\mathbf{x}_0)$ **Reachable Set** $\xrightarrow{I}$ $I(\mathcal{O}(\mathbf{x}_0))$ **Vanishing Ideal** $\xrightarrow{V}$ $V(I(\mathcal{O}(\mathbf{x}_0)))$ **Closure** $\supseteq$ $\mathcal{O}(\mathbf{x}_0)$ **Reachable Set**

Vanishing Ideal: all polynomials that vanish on $\mathcal{O}(\mathbf{x}_0)$

$$I(\mathcal{O}(\mathbf{x}_0)) \stackrel{\text{def}}{=} \{h \in \mathbb{R}[\mathbf{x}] \mid \forall \mathbf{x} \in \mathcal{O}(\mathbf{x}_0), h(\mathbf{x}) = 0\}$$

Closure: common roots of all polynomials in I

$$V(I) \stackrel{\text{def}}{=} \{\mathbf{x} \in \mathbb{R}^n \mid \forall h \in I, h(\mathbf{x}) = 0\}$$

Soundness: $V(I(\mathcal{O}(\mathbf{x}_0)))$ is the **smallest variety** that **contains** $\mathcal{O}(\mathbf{x}_0)$

Algebraic Sets Embedding

$$\underset{\textbf{Reachable Set}}{\mathcal{O}(\mathbf{x}_0)} \xrightarrow{I} \underset{\textbf{Vanishing Ideal}}{I(\mathcal{O}(\mathbf{x}_0))} \xrightarrow{V} \underset{\textbf{Closure}}{V(I(\mathcal{O}(\mathbf{x}_0)))} \supseteq \underset{\textbf{Reachable Set}}{\mathcal{O}(\mathbf{x}_0)}$$

Vanishing Ideal: all polynomials that vanish on $\mathcal{O}(\mathbf{x}_0)$

$$I(\mathcal{O}(\mathbf{x}_0)) \stackrel{\text{def}}{=} \{h \in \mathbb{R}[\mathbf{x}] \mid \forall \mathbf{x} \in \mathcal{O}(\mathbf{x}_0), h(\mathbf{x}) = 0\}$$

Closure: common roots of all polynomials in I

$$V(I) \stackrel{\text{def}}{=} \{\mathbf{x} \in \mathbb{R}^n \mid \forall h \in I, h(\mathbf{x}) = 0\}$$

Soundness: $V(I(\mathcal{O}(\mathbf{x}_0)))$ is the **smallest variety** that **contains** $\mathcal{O}(\mathbf{x}_0)$

Algebraic Sets Embedding

$$\underset{\text{Set}}{\underset{\text{Reachable}}{\mathcal{O}(\mathbf{x}_0)}} \xrightarrow{I} \underset{\text{Ideal}}{\underset{\text{Vanishing}}{I(\mathcal{O}(\mathbf{x}_0))}} \xrightarrow{V} \underset{\text{Closure}}{V(I(\mathcal{O}(\mathbf{x}_0)))} \supseteq \underset{\text{Set}}{\underset{\text{Reachable}}{\mathcal{O}(\mathbf{x}_0)}}$$

Vanishing Ideal: all polynomials that vanish on $\mathcal{O}(\mathbf{x}_0)$

$$I(\mathcal{O}(\mathbf{x}_0)) \stackrel{\text{def}}{=} \{h \in \mathbb{R}[\mathbf{x}] \mid \forall \mathbf{x} \in \mathcal{O}(\mathbf{x}_0), h(\mathbf{x}) = 0\}$$

Closure: common roots of all polynomials in I

$$V(I) \stackrel{\text{def}}{=} \{\mathbf{x} \in \mathbb{R}^n \mid \forall h \in I, h(\mathbf{x}) = 0\}$$

Soundness: $V(I(\mathcal{O}(\mathbf{x}_0)))$ is the **smallest variety** that **contains** $\mathcal{O}(\mathbf{x}_0)$

Algebraic Sets Embedding

$$\underset{\textbf{Reachable Set}}{\mathcal{O}(\mathbf{x}_0)} \xrightarrow{I} \underset{\textbf{Vanishing Ideal}}{I(\mathcal{O}(\mathbf{x}_0))} \xrightarrow{V} \underset{\textbf{Closure}}{V(I(\mathcal{O}(\mathbf{x}_0)))} \supseteq \underset{\textbf{Reachable Set}}{\mathcal{O}(\mathbf{x}_0)}$$

Vanishing Ideal: all polynomials that vanish on $\mathcal{O}(\mathbf{x}_0)$

$$I(\mathcal{O}(\mathbf{x}_0)) \overset{\text{def}}{=} \{h \in \mathbb{R}[\mathbf{x}] \mid \forall \mathbf{x} \in \mathcal{O}(\mathbf{x}_0), h(\mathbf{x}) = 0\}$$

Closure: common roots of all polynomials in I

$$V(I) \overset{\text{def}}{=} \{\mathbf{x} \in \mathbb{R}^n \mid \forall h \in I, h(\mathbf{x}) = 0\}$$

Soundness: $V(I(\mathcal{O}(\mathbf{x}_0)))$ is the **smallest variety** that **contains** $\mathcal{O}(\mathbf{x}_0)$

Limitation: Zariski Dense Varieties

Limitation: Zariski Dense Varieties

$\dot{x} = x \rightsquigarrow \mathcal{O}(\mathbf{x}_0) = [\mathbf{x}_0, \infty[\rightsquigarrow I = \langle 0 \rangle \rightsquigarrow V(I(\mathcal{O}(\mathbf{x}_0))) = \mathbb{R}$

Case Study: Longitudinal Dynamics of an Airplane

6th Order Longitudinal Equations

$$\dot{u} = \frac{X}{m} - g\sin(\theta) - qw \qquad u : \text{axial velocity}$$

$$\dot{w} = \frac{Z}{m} + g\cos(\theta) + qu \qquad w : \text{vertical velocity}$$

$$\dot{x} = \cos(\theta)u + \sin(\theta)w \qquad x : \text{range}$$

$$\dot{z} = -\sin(\theta)u + \cos(\theta)w \qquad z : \text{altitude}$$

$$\dot{q} = \frac{M}{I_{yy}} \qquad q : \text{pitch rate}$$

$$\dot{\theta} = q \qquad \theta : \text{pitch angle}$$

Case Study: Generated Invariants

Automatically Generated Invariant Functions

$$\frac{Mz}{I_{yy}} + g\theta + \left(\frac{X}{m} - qw\right)\cos(\theta) + \left(\frac{Z}{m} + qu\right)\sin(\theta)$$

$$\frac{Mx}{I_{yy}} - \left(\frac{Z}{m} + qu\right)\cos(\theta) + \left(\frac{X}{m} - qw\right)\sin(\theta)$$

$$-q^2 + \frac{2M\theta}{I_{yy}}$$