

Characterizing Algebraic Invariants by Differential Radical Invariants

Khalil Ghorbal
Carnegie Mellon university

Joint work with André Platzer

CEA List
April 3rd, 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

→

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

Safety

Context: Hybrid Systems Model

Init

→

[

(Sensing: read data from sensors

Control: actuate

Plant: evolve)*

]

Safety

Context: Hybrid Systems Model

Init

→

[

(Sensing: read data from sensors

Control: actuate

Plant: Evolve)*

]

Safety

Evolution

- Continuous time
- Ordinary Differential Equations (ODE)

Algebraic Differential Equations

Example

$$\dot{x}_1 = -x_2$$

$$\dot{x}_2 = x_1$$

$$\dot{x}_3 = x_4^2$$

$$\dot{x}_4 = x_3 x_4$$

Formally

$$\frac{dx_i(t)}{dt} = \dot{x}_i = p_i(\mathbf{x}), 1 \leq i \leq n .$$

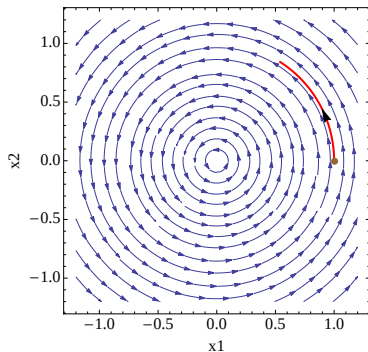
Algebraic Invariant Expression

$$\dot{x}_1 = -x_2$$

$$\dot{x}_2 = x_1$$

$$\dot{x}_3 = x_4^2$$

$$\dot{x}_4 = x_3 x_4$$



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

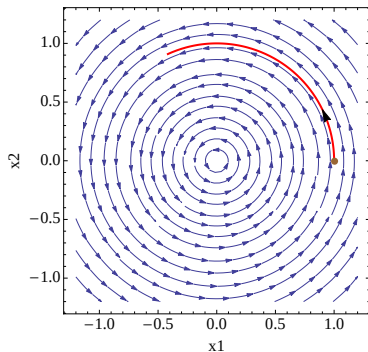
Algebraic Invariant Expression

$$\dot{x}_1 = -x_2$$

$$\dot{x}_2 = x_1$$

$$\dot{x}_3 = x_4^2$$

$$\dot{x}_4 = x_3 x_4$$



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

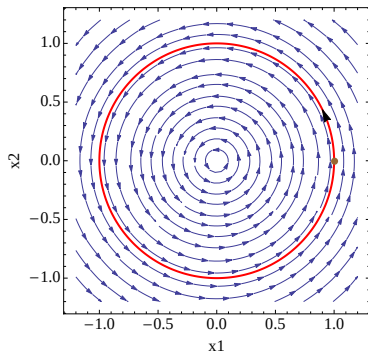
Algebraic Invariant Expression

$$\dot{x}_1 = -x_2$$

$$\dot{x}_2 = x_1$$

$$\dot{x}_3 = x_4^2$$

$$\dot{x}_4 = x_3 x_4$$



$$\forall t, x_1(t)^2 + x_2(t)^2 - 1 = 0$$

Algebraic Invariant Expression

Geometrically

$\mathcal{O}(\mathbf{x}_0) \stackrel{\text{def}}{=} \{\mathbf{x}(t) \mid t \geq 0\} \in \text{Set of roots of } h(x_1, x_2)$

Algebraic Invariant Expression

Geometrically

$\mathcal{O}(\mathbf{x}_0) \stackrel{\text{def}}{=} \{\mathbf{x}(t) \mid t \geq 0\} \in \text{Set of roots of } h(x_1, x_2)$

Algebraically

$$h(x_1, x_2) = x_1^2 + x_2^2 - 1 (= 0)$$

Algebraic Invariant Expression

Geometrically

$\mathcal{O}(\mathbf{x}_0) \stackrel{\text{def}}{=} \{\mathbf{x}(t) \mid t \geq 0\} \in \text{Set of roots of } h(x_1, x_2)$

Algebraically

$$h(x_1, x_2) = x_1^2 + x_2^2 - 1 (= 0)$$

Algebraic Invariant Expression

$$\forall t, h(\mathbf{x}(t)) = 0,$$

for all $\mathbf{x}(t)$ solution of the Initial Value Problem.

Problems

I. Checking the invariance of Algebraic Expression

Given $\mathbf{p}$, and $\mathbf{x}_0$ root of $h(\mathbf{x})$ ($h(\mathbf{x}_0) = 0$), is $h(\mathbf{x}) = 0$ an algebraic invariant expression ? ($\forall t \geq 0, h(\mathbf{x}(t)) = 0$)

II. Generate Algebraic Invariant Expression

Given $\mathbf{p}$, and **Init**, how to generate algebraic invariant expressions ? ($h(\mathbf{x}) = 0$)

Outline

- 1 Introduction
- 2 Time Abstraction**
- 3 Characterization of Invariant Expressions
- 4 Checking & Generation
- 5 Conclusion

Variety Embedding of Orbits

Zariski Closure

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

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

Affine (Real) Variety: common roots of all polynomials in I

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

Closure: Sound Abstraction

$$\mathcal{O}(\mathbf{x}_0) \subseteq V(I(\mathcal{O}(\mathbf{x}_0)))$$

Variety Embedding of Orbits

Zariski Closure

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

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

Affine (Real) Variety: common roots of all polynomials in I

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

Closure: Sound Abstraction

$$\mathcal{O}(\mathbf{x}_0) \subseteq V(I(\mathcal{O}(\mathbf{x}_0)))$$

Variety Embedding of Orbits

Zariski Closure

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

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

Affine (Real) Variety: common roots of all polynomials in I

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

Closure: Sound Abstraction

$$\mathcal{O}(\mathbf{x}_0) \subseteq V(I(\mathcal{O}(\mathbf{x}_0)))$$

Variety Embedding of Orbits

Zariski Closure

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

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

Affine (Real) Variety: common roots of all polynomials in I

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

Closure: Sound Abstraction

$$\mathcal{O}(\mathbf{x}_0) \subseteq V(I(\mathcal{O}(\mathbf{x}_0)))$$

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

Variety Embedding

$$\begin{array}{ccccc}
 \mathcal{O}(\mathbf{x}_0) & \xrightarrow{\alpha} & I(\mathcal{O}(\mathbf{x}_0)) & \xrightarrow{\gamma} & V(I(\mathcal{O}(\mathbf{x}_0))) \\
 \text{Orbit} & & \text{Vanishing Ideal} & & \text{Closure} \supseteq \text{Orbit}
 \end{array}$$

Variety Embedding

$$\begin{array}{ccccc}
 \mathcal{O}(\mathbf{x}_0) & \xrightarrow{\alpha} & I(\mathcal{O}(\mathbf{x}_0)) & \xrightarrow{\gamma} & V(I(\mathcal{O}(\mathbf{x}_0))) \\
 \text{Orbit} & & \text{Vanishing Ideal} & & \text{Closure}
 \end{array}
 \supseteq
 \begin{array}{c}
 \mathcal{O}(\mathbf{x}_0) \\
 \text{Orbit}
 \end{array}$$

Variety Embedding

$$\begin{array}{ccccc}
 \mathcal{O}(\mathbf{x}_0) & \xrightarrow{\alpha} & I(\mathcal{O}(\mathbf{x}_0)) & \xrightarrow{\gamma} & V(I(\mathcal{O}(\mathbf{x}_0))) \\
 \text{Orbit} & & \text{Vanishing Ideal} & & \text{Closure}
 \end{array}
 \supseteq \mathcal{O}(\mathbf{x}_0)$$

Orbit

Variety Embedding

$$\begin{array}{ccccc}
 \mathcal{O}(\mathbf{x}_0) & \xrightarrow{\alpha} & I(\mathcal{O}(\mathbf{x}_0)) & \xrightarrow{\gamma} & V(I(\mathcal{O}(\mathbf{x}_0))) \\
 \text{Orbit} & & \text{Vanishing Ideal} & & \text{Closure} \quad \supseteq \quad \text{Orbit}
 \end{array}$$

Variety Embedding

$$\begin{array}{ccccc}
 \mathcal{O}(\mathbf{x}_0) & \xrightarrow{\alpha} & I(\mathcal{O}(\mathbf{x}_0)) & \xrightarrow{\gamma} & V(I(\mathcal{O}(\mathbf{x}_0))) \\
 \text{Orbit} & & \text{Vanishing Ideal} & & \text{Closure}
 \end{array}
 \supseteq
 \begin{array}{c}
 \mathcal{O}(\mathbf{x}_0) \\
 \text{Orbit}
 \end{array}$$

Limitation: Zariski Dense Varieties

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

Outline

- 1 Introduction
- 2 Time Abstraction
- 3 Characterization of Invariant Expressions**
- 4 Checking & Generation
- 5 Conclusion

Properties of $I(\mathcal{O}(\mathbf{x}_0))$ (abstract domain)

$I(\mathcal{O}(\mathbf{x}_0))$: The set of all polynomials that vanish on $\mathcal{O}(\mathbf{x}_0)$

$I(\mathcal{O}(\mathbf{x}_0))$ is an ideal

- $0 \in I(\mathcal{O}(\mathbf{x}_0))$
- if $h_1, h_2 \in I(\mathcal{O}(\mathbf{x}_0))$, then $h_1 + h_2 \in I(\mathcal{O}(\mathbf{x}_0))$
- if $h \in I(\mathcal{O}(\mathbf{x}_0))$, then $q h \in I(\mathcal{O}(\mathbf{x}_0))$, for any polynomial q

Properties of $I(\mathcal{O}(\mathbf{x}_0))$ (abstract domain)

$I(\mathcal{O}(\mathbf{x}_0))$: The set of all polynomials that vanish on $\mathcal{O}(\mathbf{x}_0)$

$I(\mathcal{O}(\mathbf{x}_0))$ is an ideal

- $0 \in I(\mathcal{O}(\mathbf{x}_0))$
- if $h_1, h_2 \in I(\mathcal{O}(\mathbf{x}_0))$, then $h_1 + h_2 \in I(\mathcal{O}(\mathbf{x}_0))$
- if $h \in I(\mathcal{O}(\mathbf{x}_0))$, then $q h \in I(\mathcal{O}(\mathbf{x}_0))$, for any polynomial q

$I(\mathcal{O}(\mathbf{x}_0))$ is a Differential Ideal

if $h \in I(\mathcal{O}(\mathbf{x}_0))$, then $\frac{dh}{dt} \in I(\mathcal{O}(\mathbf{x}_0))$.

Properties of $I(\mathcal{O}(\mathbf{x}_0))$ (abstract domain)

$I(\mathcal{O}(\mathbf{x}_0))$: The set of all polynomials that vanish on $\mathcal{O}(\mathbf{x}_0)$

$I(\mathcal{O}(\mathbf{x}_0))$ is an ideal

- $0 \in I(\mathcal{O}(\mathbf{x}_0))$
- if $h_1, h_2 \in I(\mathcal{O}(\mathbf{x}_0))$, then $h_1 + h_2 \in I(\mathcal{O}(\mathbf{x}_0))$
- if $h \in I(\mathcal{O}(\mathbf{x}_0))$, then $q h \in I(\mathcal{O}(\mathbf{x}_0))$, for any polynomial q

$I(\mathcal{O}(\mathbf{x}_0))$ is a Differential Ideal

if $h \in I(\mathcal{O}(\mathbf{x}_0))$, then $\frac{dh}{dt} \in I(\mathcal{O}(\mathbf{x}_0))$.

Instead of $\frac{dh}{dt}$, we will use $\mathfrak{L}_{\mathbf{p}}(h)$: The **Lie Derivative** of h .

Lie derivative along a vector field

Definition

$$\mathcal{L}_{\mathbf{p}}(h) \stackrel{\text{def}}{=} \sum_{i=1}^n \frac{\partial h}{\partial x_i} p_i(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$$

Properties

- Algebraic differentiation (chain rule)
- Do not require $\mathbf{x}(t)$ (the solution of the ODE)
- Corresponds to the time derivative when $\mathbf{x} = \mathbf{x}(t)$

Differential Radical Invariants

Theorem

$h \in I(\mathcal{O}(\mathbf{x}_0))$ if and only if

- $\exists g_0, \dots, g_{N-1} \in \mathbb{R}[\mathbf{x}]: \mathfrak{L}_{\mathbf{p}}^{(N)}(h) = \sum_{i=0}^{N-1} g_i \mathfrak{L}_{\mathbf{p}}^{(i)}(h)$
- N **finite**
- $\mathfrak{L}_{\mathbf{p}}^{(0)}(h)(\mathbf{x}_0) = 0, \dots, \mathfrak{L}_{\mathbf{p}}^{(N-1)}(h)(\mathbf{x}_0) = 0$

Special Cases

Invariant Polynomial Functions

$$\mathcal{L}_p(h) = 0 \iff N = 1 \text{ and } g_0 = 0$$

Darboux Polynomials [Darboux 1878, Painlevé, Poincaré ...]

$$\mathcal{L}_p(h) = g_0 h \iff N = 1$$

Special Cases

Invariant Polynomial Functions

$$\mathcal{L}_{\mathbf{p}}(h) = 0 \longleftrightarrow N = 1 \text{ and } g_0 = 0$$

Darboux Polynomials [Darboux 1878, Painlevé, Poincaré ...]

$$\mathcal{L}_{\mathbf{p}}(h) = g_0 h \longleftrightarrow N = 1$$

Outline

- 1 Introduction
- 2 Time Abstraction
- 3 Characterization of Invariant Expressions
- 4 Checking & Generation**
- 5 Conclusion

Checking Invariance of Candidates

I. Checking the invariance of Algebraic Expression

Given $\mathbf{p}$, and $\mathbf{x}_0$ root of $h(\mathbf{x})$ ($h(\mathbf{x}_0) = 0$), is $h(\mathbf{x}) = 0$ is an algebraic invariant expression ? ($\forall t \geq 0, h(\mathbf{x}(t)) = 0$)

A Necessary and Sufficient Proof Rule

$$(\text{DRI}) \frac{h = 0 \rightarrow \bigwedge_{i=0}^{N-1} \mathcal{L}_{\mathbf{p}}^{(i)}(h) = 0}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)} .$$

DRI: Algorithm

Data: $h, \mathbf{p}, \mathbf{x}$

Result: Boolean: True, False.

$N \leftarrow 1$

$\text{GB} \leftarrow \{h\}$

$\ell \leftarrow h$

$\text{syms} \leftarrow \text{Variables}[\mathbf{p}, h]$

while true **do**

$\text{GB} \leftarrow \text{GröbnerBasis}[\text{GB}, \mathbf{x}]$

$\text{LieD} \leftarrow \text{LieDerivative}[\ell, \mathbf{p}, \mathbf{x}]$

$\text{Rem} \leftarrow \text{PolynomialRemainder}[\text{LieD}, \text{GB}, \mathbf{x}]$

if $\text{Rem} = 0$ **then**

return True

else

$\text{Reduce} \leftarrow \text{QE}[\forall \text{ syms}, h = 0 \rightarrow \text{LieD} = 0]$

if $\neg \text{Reduce}$

then

return False

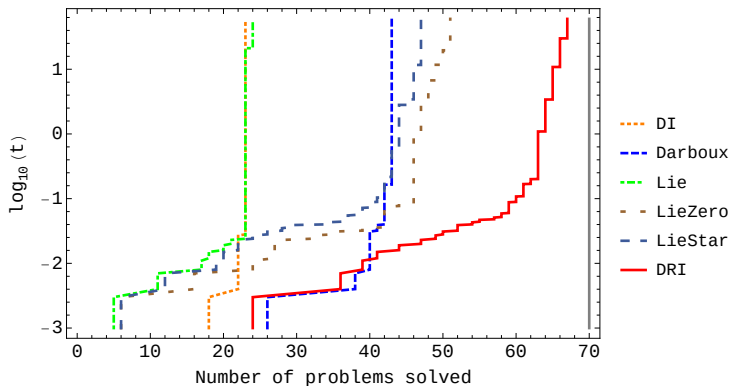
$\text{Append}[\text{GB}, \text{LieD}]$

$\ell \leftarrow \text{LieD}$

$N \leftarrow N + 1$

Benchmarks

Joint work with Andrew Sogokon



Generation of Invariant Varieties

II. Generate Algebraic Invariant Expression

Given $\mathbf{p}$, and Init , how to generate algebraic invariant expressions ?
 $(h(\mathbf{x}) = 0)$

Theorem

$S \subseteq \mathbb{R}^n$ is an invariant variety **if and only if** S is the set of roots of the system

$$\bigwedge_{0 \leq i \leq N-1} \mathcal{L}_{\mathbf{p}}^{(i)}(h) = 0,$$

for some polynomial h .

In practice

In practice

Find h and N , such that:

$$\mathfrak{L}_{\mathbf{p}}^{(N)}(h) = \sum_{i=0}^{N-1} g_i \mathfrak{L}_{\mathbf{p}}^{(i)}(h)$$

→ The set of roots of

$$\bigwedge_{0 \leq i \leq N-1} \mathfrak{L}_{\mathbf{p}}^{(i)}(h) = 0,$$

is an **invariant variety**.

Matrix Representation: Intuition

invariant of degree 1

$$\dot{x}_1 = a_1 x_1 + a_2 x_2$$

$$h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_0$$

$$\dot{x}_2 = b_1 x_1 + b_2 x_2$$

$$\mathcal{L}_p(h) = \alpha_1(a_1 x_1 + a_2 x_2) + \alpha_2(b_1 x_1 + b_2 x_2)$$

$$\exists ? \beta \in \mathbb{R} \text{ s.t. } \mathcal{L}_p(h) = \beta h$$

$$\begin{aligned} (-a_1 + \beta)\alpha_1 + (-b_1)\alpha_2 &= 0 \\ (-a_2)\alpha_1 + (-b_2 + \beta)\alpha_2 &= 0 \\ (\beta)\alpha_3 &= 0 \end{aligned} \Leftrightarrow \begin{pmatrix} -a_1 + \beta & -b_1 & 0 \\ -a_2 & -b_2 + \beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = 0$$

Matrix Representation

$$\begin{array}{ll}
 \text{Polynomial} & \leftrightarrow \binom{n+d}{d} \text{ Coefficients } (d \text{ degree of } h) \\
 h & \leftrightarrow \alpha = (\alpha_1, \alpha_2, \dots, \alpha_r) \\
 g_i & \leftrightarrow \beta_i = (\beta_1, \beta_2, \dots, \beta_{s_i})
 \end{array}$$

Matrix Representation

$$\mathcal{L}_{\mathbf{p}}^{(N)}(h) = \sum_{i=0}^{N-1} g_i \mathcal{L}_{\mathbf{p}}^{(i)}(h) \leftrightarrow M(\beta) \alpha = 0$$

α lies in the **Kernel** of $M(\beta) \stackrel{\text{def}}{=} \{\alpha \in \mathbb{R}^r \mid M(\beta) \alpha = 0\}$

Example: $n = 2$, $d = 1$, $N = 1$

invariant of degree 1

$$\begin{aligned}\dot{x}_1 &= a_1 x_1 + a_2 x_2 & h &= \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_0 \\ \dot{x}_2 &= b_1 x_1 + b_2 x_2 & \mathfrak{L}_{\mathbf{p}}(h) &= \alpha_1 (a_1 x_1 + a_2 x_2) + \alpha_2 (b_1 x_1 + b_2 x_2)\end{aligned}$$

$$|M(\beta)| = \beta(\beta^2 - (a_1 + b_2)\beta - a_2 b_1 + a_1 b_2)$$

- $\ker(M(0)) = \langle (0, 0, 1) \rangle$
- $\alpha \in \langle (0, 0, 1) \rangle \cap \mathbf{x}_0^\perp$

Example

System

$$\dot{x}_1 = -x_2$$

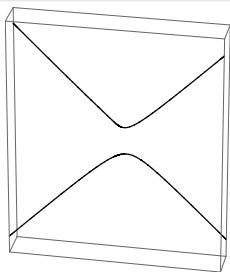
$$\dot{x}_3 = x_4^2$$

$$\dot{x}_2 = x_1$$

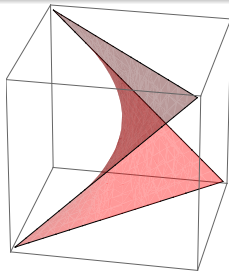
$$\dot{x}_4 = x_3 x_4$$

Differential Radical Invariants

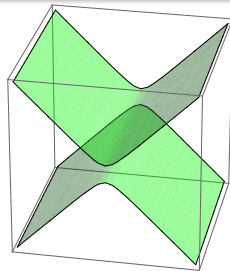
$$h = -1 + x_1 x_4 \text{ and } \mathfrak{L}_{\mathbf{p}}(h) = x_3 - x_2 x_4 \text{ and } \mathfrak{L}_{\mathbf{p}}^{(2)}(h) = x_4^2 - x_3^2 - 1$$



Orbit

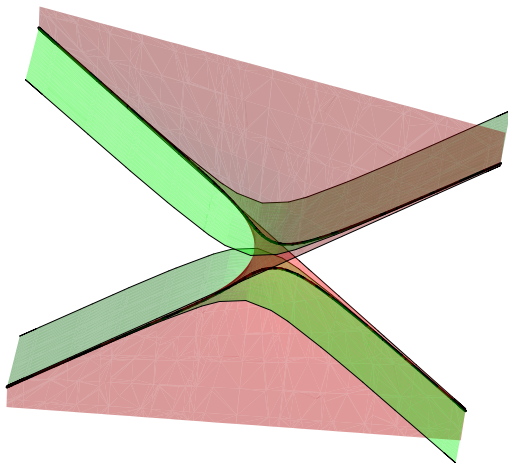


Roots of $\mathfrak{L}_{\mathbf{p}}(h)$



Roots of $\mathfrak{L}_{\mathbf{p}}^{(2)}(h)$

Example: cont'd



Overapproximation of $\mathcal{O}(\mathbf{x}_0)$

Case Study: Longitudinal Dynamics of an Airplane

6th Order Longitudinal Equations

$$\dot{u} = \frac{X}{m} - g \sin(\theta) - qw$$

u : axial velocity

$$\dot{w} = \frac{Z}{m} + g \cos(\theta) + qu$$

w : vertical velocity

$$\dot{x} = \cos(\theta)u + \sin(\theta)w$$

x : range

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

z : altitude

$$\dot{q} = \frac{M}{I_{yy}}$$

q : pitch rate

$$\dot{\theta} = q$$

θ : pitch angle

Case Study: Generated Invariants

Automatically Generated Invariant Functions

$$\begin{aligned} & \frac{Mz}{I_{yy}} + g\theta + \left(\frac{X}{m} - qw \right) \cos(\theta) + \left(\frac{Z}{m} + qu \right) \sin(\theta) \\ & \frac{Mx}{I_{yy}} - \left(\frac{Z}{m} + qu \right) \cos(\theta) + \left(\frac{X}{m} - qw \right) \sin(\theta) \\ & - q^2 + \frac{2M\theta}{I_{yy}} \end{aligned}$$

Conclusion

- Variety embedding of the reachable set (Zariski Closure)
- Characterizing elements of the vanishing ideal $I(\mathcal{O}(\mathbf{x}_0))$
- New Necessary and sufficient proof rule (DRI)
- Leveraging linear algebra tools to generate algebraic invariant equations

Thank you for attending !

kghorbal@cs.cmu.edu

Enforcing Invariants

$$\delta \stackrel{\text{def}}{=} (a_1 - b_2)^2 + 4a_2b_1 \geq 0$$

- $\beta \in \{0, \frac{1}{2}(a_1 + b_2 + \sqrt{\delta}), \frac{1}{2}(a_1 + b_2 - \sqrt{\delta})\}$
- If $\mathbf{x}_0 \in (a_1 - b_2 \pm \sqrt{\delta}, 2a_2, 0)^\perp$ then $\alpha = (a_1 - b_2 \pm \sqrt{\delta}, 2a_2, 0)$
- α is an **Eigenvector**

If $a_2 = 0$, $\beta \in \{0, a_1, b_2\} \rightsquigarrow \dots$