Characterizing Algebraic Invariants by Differential Radical Invariants

Khalil Ghorbal
Carnegie Mellon university

Joint work with André Platzer

CMACS AVACS
November 21st, 2013

Context: ODE in Computer Science/Formal Verification

Goal.

Automated Formal Reasoning about Ordinary Differential Equations.

Formal Reasoning: **Global** Properties of **All** solutions.

Applications to the Formal Verification of Hybrid Systems

- Reachability Analysis
- Proof Rules
- Synthesis

Useful in many other fields: Control Theory, Stability Analysis, Numerical Integration, Integrability of ODE.

Algebraic Differential Equations

Example

$$\mathbf{x}_\iota = (1, 0, 0, 1)$$

$$\dot{x_1} = -x_2 \qquad \dot{x_2} = x_1$$

$$\dot{x_3} = x_4^2 \qquad \dot{x_4} = x_3 x_4$$

Formally, we study the Initial Value Problem:

$$\frac{dx_i(t)}{dt} = \dot{x}_i = p_i(\mathbf{x}), 1 \leq i \leq n,\ \mathbf{x}(0) = \mathbf{x}_\iota \in \mathbb{R}^n \ .$$

- ⊕ Parameters are allowed
- ⊕ Many analytic functions can be encoded (sin, cos, ln, . . .)
- ⊕/⊖ The initial value ($\mathbf{x}_\iota$) are not restricted
- ⊖ Evolution domain abstracted (still sound)

Approach

Algebraic Invariant Expression

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

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

Tools

- Classical Algebraic Geometry: Polynomial Ring, Ideals, Varieties
- Symbolic Linear Algebra

Outline

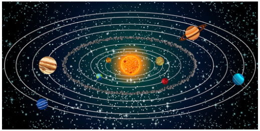
Orbits

Definition

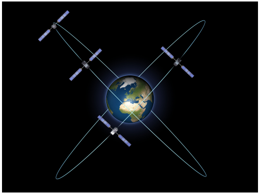
$$\mathcal{O}(\mathbf{x}_\iota) \overset{\text{def}}{=} \{\mathbf{x}(t) \mid t \in U_t\} \subseteq \mathbb{R}^n$$

U_t domain of definition of the maximal solution of the Initial Value Problem $(\dot{\mathbf{x}} = \mathbf{p}(\mathbf{x}), \mathbf{x}(0) = \mathbf{x}_\iota)$.

Example



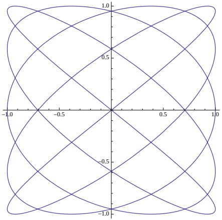
Solar System



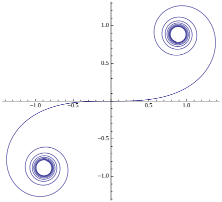
Galileo Orbit

Orbits: Issues

Example



Lissajous Curve



Cornu Spiral

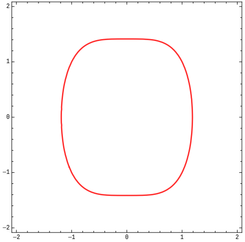
Solutions → Exact Orbit

- Computation issues
- Decidability issues

➔ Idea: **Time Abstraction**

Affine Varieties and Ideals

Roots of h



Polynomials

$$h \stackrel{\text{def}}{=} x_1^4 + x_2^2 - 2$$

What about the polynomials ph ?

Ideal: stable set of polynomials under external multiplication

$$I = \langle h_1, \ldots, h_r \rangle \stackrel{\text{def}}{=} \{\textstyle\sum_{i=1}^{r} g_i h_i \mid g_1, \ldots, g_r \in \mathbb{R}[\mathbf{x}]\}$$

Affine Variety: common roots of all polynomials in I

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

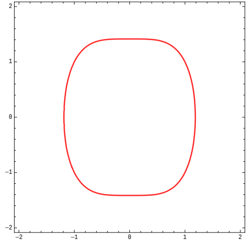
Affine Varieties and Ideals

Polynomials

$$h \stackrel{\text{def}}{=} x_1^4 + x_2^2 - 2$$

What about the polynomials ph ?

Roots of h



Ideal: stable set of polynomials under external multiplication

$$I = \langle h_1, \ldots, h_r \rangle \stackrel{\text{def}}{=} \{\textstyle\sum_{i=1}^{r} g_i h_i \mid g_1, \ldots, g_r \in \mathbb{R}[\mathbf{x}]\}$$

Affine Variety: common roots of all polynomials in I

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

Variety Embedding of Orbits

Zariski Closure

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

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

Closure: Sound Abstraction

$$\mathcal{O}(\mathbf{x}_\iota) \subseteq \bar{\mathcal{O}}(\mathbf{x}_\iota) \stackrel{\text{def}}{=} V(I(\mathcal{O}(\mathbf{x}_\iota)))$$

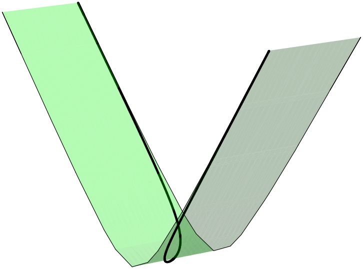
Orbit $\longrightarrow$ **Vanishing Ideal** $\longrightarrow$ **Closure** $\supseteq$ **Orbit**

Closure is the **smallest variety** that **contains Orbit**.

Example

$$\dot{x} = x \rightsquigarrow x(t) = \mathbf{x}_\iota e^t \rightsquigarrow \mathcal{O}(\mathbf{x}_\iota) = [\mathbf{x}_\iota, \infty[\rightsquigarrow I = \langle 0 \rangle \rightsquigarrow \bar{\mathcal{O}}(\mathbf{x}_\iota) = \mathbb{R}$$

Example: Variety Embedding



Zariski Closure (Intuition)

Outline

Hold on ...

Sound Abstraction

Orbit $\subseteq$ **Closure**

Goal

Explicit Characterization of the Vanishing Ideal $I(\mathcal{O}(\mathbf{x}_\iota))$

Lie Derivation

Lie derivative along a vector field

$$\mathfrak{L}_{\mathbf{p}}(h) \stackrel{\text{def}}{=} \sum_{i=1}^{n} \frac{\partial h}{\partial x_i} p_i(\mathbf{x})$$

Properties

- Algebraic differentiation
- Applies to the polynomial h (not the function $t \mapsto h(\mathbf{x}(t))$)
- Corresponds to the time derivative when the solution is substituted back

The Vanishing Ideal is a Differential Ideal

$\mathfrak{L}_{\mathbf{p}}(h) \in I(\mathcal{O}(\mathbf{x}_\iota))$ for all $h \in I(\mathcal{O}(\mathbf{x}_\iota))$.

Differential Radical Invariants

Theorem

$h \in I(\mathcal{O}(\mathbf{x}_\iota))$ **if and only if** there exists a **finite** integer N s.t.

$$\mathfrak{L}_{\mathbf{p}}^{(N)}(h) \in \langle \mathfrak{L}_{\mathbf{p}}^{(0)}(h), \ldots, \mathfrak{L}_{\mathbf{p}}^{(N-1)}(h) \rangle \subseteq I(\mathcal{O}(\mathbf{x}_\iota)) \qquad (\imath)$$

$$\mathfrak{L}_{\mathbf{p}}^{(0)}(h)(\mathbf{x}_\iota) = 0, \ldots, \mathfrak{L}_{\mathbf{p}}^{(N-1)}(h)(\mathbf{x}_\iota) = 0 \;. \qquad (\imath\imath)$$

Proof Sketch

"$\Rightarrow$" **Ascending Chain Condition** on ideals ($\mathbb{R}[\mathbf{x}]$ is **Notherian**)

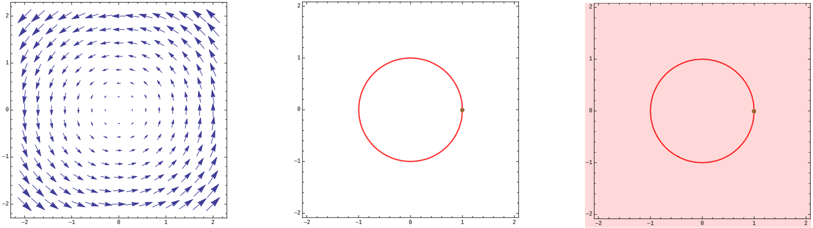
"$\Leftarrow$" (Global) Cauchy-Lipschitz Theorem

Special Case: Invariant (Algebraic) Functions

$N = 1$ and $\mathfrak{L}_{\mathbf{p}}(h) \in \langle 0 \rangle$

- $\mathfrak{L}_{\mathbf{p}}(h) = 0 \wedge h(\mathbf{x}_\iota) = 0 \longrightarrow h = 0$

Example



Vector Field $\dot{x_1} = -x_2$, $\dot{x_2} = x_1$, $\mathbf{x}_\iota = (1, 0)$

Roots of $h \stackrel{\text{def}}{=} x_1^2 + x_2^2 - 1$

Roots of $\mathfrak{L}_{\mathbf{p}}(h)$: **Whole Space**

Special Case ($N = 1$) Darboux Invariants

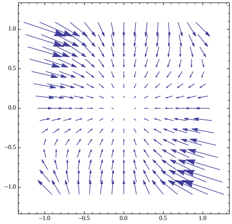
a.k.a. λ-Invariant, Exponential Invariants, P-Consecution,

- $\mathfrak{L}_{\mathbf{p}}(h) = ph \wedge h(\mathbf{x}_\iota) = 0 \longrightarrow h = 0$

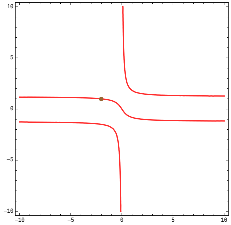
$$\dot{x}_1 = -x_1 + 2x_1^2 x_2 \qquad h = (\mathbf{x}_{\iota 2} - \mathbf{x}_{\iota 1}\mathbf{x}_{\iota 2}^2)x_1 - \mathbf{x}_{\iota 1}(x_2 - x_1 x_2^2)$$

$$\dot{x}_2 = x_2 \qquad \mathfrak{L}_{\mathbf{p}}(h) = (-1 + 2x_1x_2)h$$

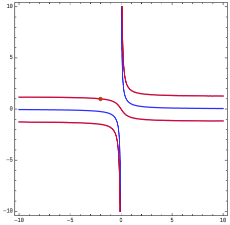
Example



Vector Field



Roots of h



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

Decidability

Corollary

It is decidable whether a polynomial h with real algebraic coefficients is an algebraic invariant of an algebraic differential system with real algebraic coefficients and real algebraic initial values.

Related Work

Generalizes the decidability of invariant functions [A. Platzer ITP'12]

Sound Approximation of the Closure $\bar{\mathcal{O}}(\mathbf{x}_\iota)$

Differential Radical Ideals

$$J_j \stackrel{\text{def}}{=} \langle \mathfrak{L}_{\mathbf{p}}^{(i)}(h_j) \rangle_{0 \leq i \leq N-1}$$

Underapproximation of $I(\mathcal{O}(\mathbf{x}_\iota))$

$$\bigoplus_{j \in \Im} J_j = I(\mathcal{O}(\mathbf{x}_\iota)), \Im \text{ **finite**}$$

Overapproximation of $\bar{\mathcal{O}}(\mathbf{x}_\iota)$

$$\bar{\mathcal{O}}(\mathbf{x}_\iota) \subseteq \bigcap_{1 \leq i \leq r} V(J_i)$$

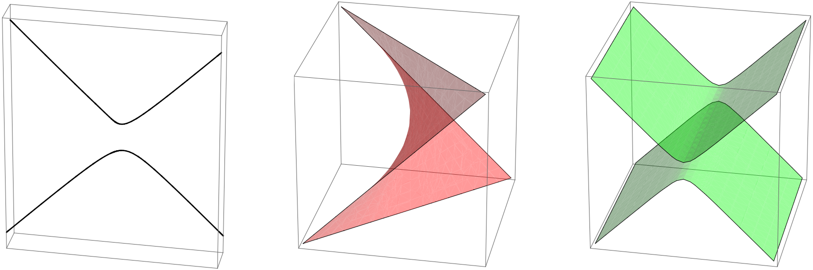
Example

System

$$\dot{x}_1 = -x_2 \qquad \dot{x}_2 = x_1$$
$$\dot{x}_3 = x_4^2 \qquad \dot{x}_4 = x_3 x_4$$

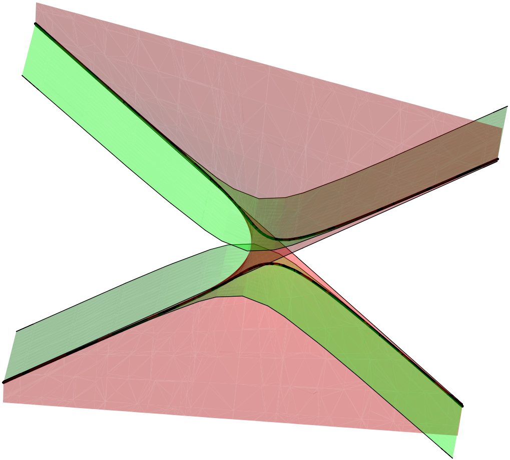
Differential Radical Invariants

$h_1 = x_3 - x_2 x_4$ and $h_2 = x_4^2 - x_3^2 - 1$



Orbit — Roots of h_1 — Roots of h_2

Example: cont'd



Overapproximation of $\bar{\mathcal{O}}(\mathbf{x}_\iota)$

Outline

So ...

Sound Abstraction

Orbit $\subseteq$ Closure

Characterization of $I(\mathcal{O}(\mathbf{x}_\iota))$

Explicit Characterization of $I(\mathcal{O}(\mathbf{x}_\iota))$ by **Differential Radical Invariants**

Goal

Automate the generation of Differential Radical Invariants

Matrix Representation: Intuition

invariant of degree 1

$$\dot{x_1} = a_1 x_1 + a_2 x_2 \qquad h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_0$$
$$\dot{x_2} = b_1 x_1 + b_2 x_2 \qquad \mathfrak{L}_{\mathbf{p}}(h) = \alpha_1(a_1 x_1 + a_2 x_2) + \alpha_2(b_1 x_1 + b_2 x_2)$$

$\mathfrak{L}_{\mathbf{p}}(h) \in \langle h \rangle$ **if and only if** $\exists \beta \in \mathbb{R}$ s.t. $\mathfrak{L}_{\mathbf{p}}(h) = \beta h$

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

Matrix Representation

Explicit Ideal Membership

$$\mathfrak{L}_{\mathbf{p}}^{(N)}(h) \in \langle \mathfrak{L}_{\mathbf{p}}^{(0)}(h), \ldots, \mathfrak{L}_{\mathbf{p}}^{(N-1)}(h) \rangle \leftrightarrow \mathfrak{L}_{\mathbf{p}}^{(N)}(h) = \sum_{i=0}^{N-1} g_i \mathfrak{L}_{\mathbf{p}}^{(i)}(h)$$

Polynomial	$\leftrightarrow$	$\binom{n+d}{d}$ Coefficients (up to monomial order)
h	$\leftrightarrow$	$\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_r)$
g_i	$\leftrightarrow$	$\boldsymbol{\beta}_i = (\beta_1, \beta_2, \ldots, \beta_{s_i})$

Matrix Representation

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

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

Initial Value Constraints

$\mathbf{x}_\iota$ in the Differential Radical Ideal

$$\mathfrak{L}_{\mathbf{p}}^{(0)}(h)(\mathbf{x}_\iota) = 0 \wedge \cdots \wedge \mathfrak{L}_{\mathbf{p}}^{(N-1)}(h)(\mathbf{x}_\iota) = 0$$

$$\mathfrak{L}_{\mathbf{p}}^{(i)}(h)(\mathbf{x}_\iota) = 0 \;\leftrightarrow\; \boldsymbol{\alpha} \in H_i \stackrel{\text{def}}{=} \{\boldsymbol{\alpha} \in \mathbb{R}^r \mid \mathfrak{L}_{\mathbf{p}}^{(i)}(h)(\mathbf{x}_\iota) = 0\}$$

$\boldsymbol{\alpha}$ lies in a hyperplane parametrized by the initial value $\mathbf{x}_\iota$

$$\forall i, 0 \leq i \leq N-1, \mathfrak{L}_{\mathbf{p}}^{(i)}(h)(\mathbf{x}_\iota) = 0 \;\leftrightarrow\; \boldsymbol{\alpha} \in H(\mathbf{x}_\iota) \stackrel{\text{def}}{=} \bigcap_{0 \leq i \leq N-1} H_i$$

Summary

Differential Radical Invariants

$h \in I(\mathcal{O}(\mathbf{x}_\iota))$ **if and only if** there exists a **finite** positive integer N s.t.

$$\mathfrak{L}_{\mathbf{p}}^{(N)}(h) \in \langle \mathfrak{L}_{\mathbf{p}}^{(0)}(h), \ldots, \mathfrak{L}_{\mathbf{p}}^{(N-1)}(h) \rangle \subseteq I(\mathcal{O}(\mathbf{x}_\iota)) \qquad (\imath)$$

$$\mathfrak{L}_{\mathbf{p}}^{(0)}(h)(\mathbf{x}_\iota) = 0, \ldots, \mathfrak{L}_{\mathbf{p}}^{(N-1)}(h)(\mathbf{x}_\iota) = 0 \ . \qquad (\imath\imath)$$

Symbolic Linear Algebra Formulation

$(\imath)$ and $(\imath\imath)$ **if and only if**

$$\boldsymbol{\alpha} \in \ker(M(\boldsymbol{\beta})) \cap H(\mathbf{x}_\iota)$$

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

invariant of degree 1

$$\dot{x_1} = a_1 x_1 + a_2 x_2 \qquad h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_0$$
$$\dot{x_2} = b_1 x_1 + b_2 x_2 \qquad \mathfrak{L}_{\mathbf{p}}(h) = \alpha_1(a_1 x_1 + a_2 x_2) + \alpha_2(b_1 x_1 + b_2 x_2)$$

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

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

… and … $\mathbf{0} = \mathbf{0}$ **Ha .. Ha .. Ha ..**

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

invariant of degree 1

$$\dot{x}_1 = a_1 x_1 + a_2 x_2 \qquad h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_0$$

$$\dot{x}_2 = b_1 x_1 + b_2 x_2 \qquad \mathfrak{L}_{\mathbf{p}}(h) = \alpha_1(a_1 x_1 + a_2 x_2) + \alpha_2(b_1 x_1 + b_2 x_2)$$

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

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

... and ... $\mathbf{0} = \mathbf{0}$ **Ha .. Ha ..** Ha ..

Enforcing Invariants

$\delta \stackrel{\text{def}}{=} (a_1 - b_2)^2 + 4a_2 b_1 \geq 0$

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

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

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

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

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

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

Conclusion

Ongoing work

- **Upper Bounds** for the order N and the degree d
- Injecting **evolution domain** constraints
- **Global Invariants** for the (**whole**) Hybrid System
- Semialgebraic Invariants (**Inequalities** $h \geq 0$)

➔ contact **kghorbal@cs.cmu.edu**