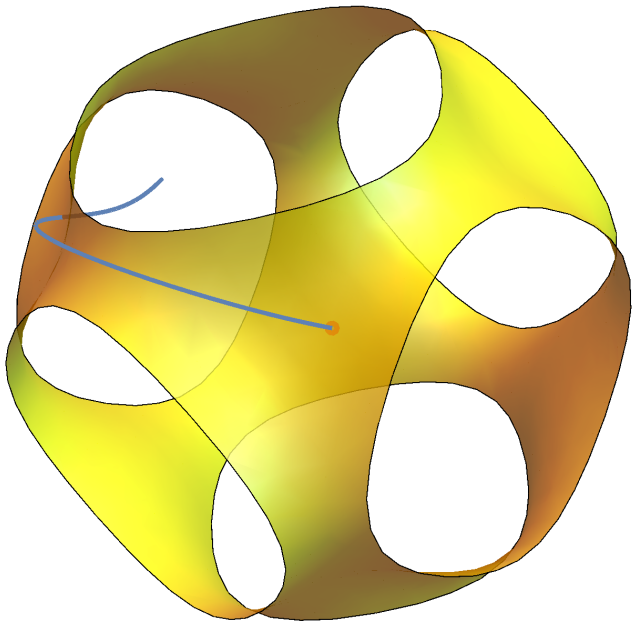
Invariance of Conjunctions of Polynomial Equalities for Algebraic Differential Equations

Khalil Ghorbal[1] Andrew Sogokon[2] André Platzer[1]

1. Carnegie Mellon University
2. University of Edinburgh

SAS, Munich, Germany
September 11th, 2014

Problem: Checking the Invariance of Algebraic Sets



Ordinary Differential Equation

$$\begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{pmatrix} = \begin{pmatrix} yz \\ -xz \\ -xy \end{pmatrix} = \mathbf{f}$$

Algebraic Sets

$$S = \{(x, y, z) \mid \underbrace{3x^2 + 3y^2 - 2x^2y^2 + 3z^2 - 2x^2z^2 - 2y^2z^2}_{p(x,y,z)} = 0\}$$

Motivations

- Theorem Proving with Hybrid Systems
- Stability and Safety Analysis of Dynamical Systems
- Qualitative Analysis of Differential Equations

Related and Previous Work

- Invariance of algebraic sets is **decidable**
- 2 procedures are available:
  - Liu et al. [Liu Zhan Zhao 2011]
  - Differential Radical Characterization [TACAS'14]

In this talk

We build on top of our previous work [TACAS'14]:

- New efficient procedure for algebraic sets
- New proof strategies exploiting differential cuts

Related and Previous Work

- Invariance of algebraic sets is **decidable**
- 2 procedures are available:
  - Liu et al. [Liu Zhan Zhao 2011]
  - Differential Radical Characterization [TACAS'14]

In this talk

We build on top of our previous work [TACAS'14]:

- New efficient procedure for algebraic sets
- New proof strategies exploiting differential cuts

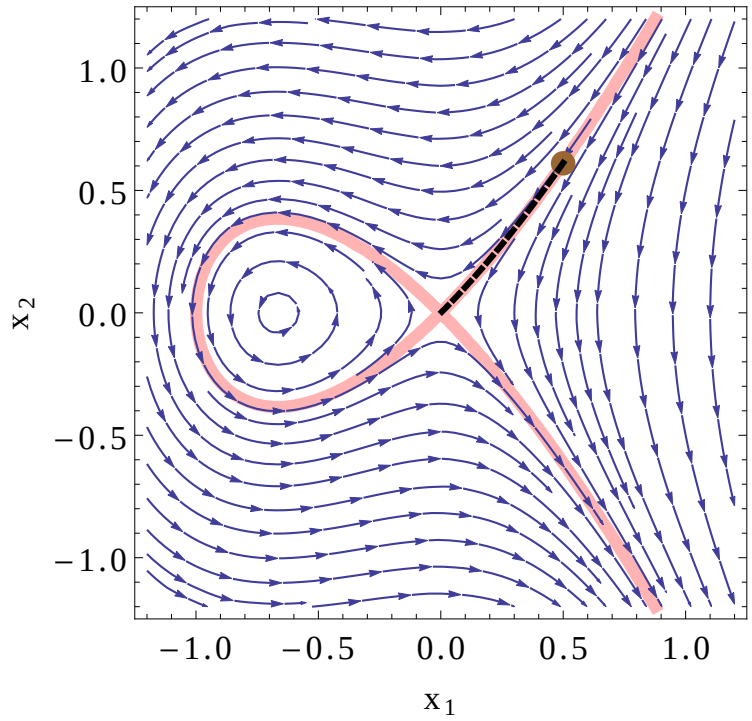
Abstracting Orbits Using Algebraic Sets

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 ?

Outline

Notation for "$p = 0$ is invariant for $\mathbf{f}$"

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

$$\equiv$$

Zero set of p is an invariant algebraic set for $\mathbf{f}$

$$\equiv$$

Starting with $\mathbf{x}_0$ s.t $p(\mathbf{x}_0) = 0$: for all $t > 0$, $\mathbf{x}(t)$ solution of the IVP $(\dot{\mathbf{x}} = \mathbf{f}, \mathbf{x}(0) = \mathbf{x}_0)$ is a zero of p

N.B. Treating $\dot{\mathbf{x}} = \mathbf{f}$ as a program, one can think of the top formula as representing the Hoare triple $\{p = 0\}\ \dot{\mathbf{x}} = \mathbf{f}\ \{p = 0\}$.

Notation for "$p = 0$ is invariant for $\mathbf{f}$"

$$(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p = 0)$$
$$\equiv$$
Zero set of p is an invariant algebraic set for $\mathbf{f}$
$$\equiv$$
Starting with $\mathbf{x}_0$ s.t $p(\mathbf{x}_0) = 0$: for all $t > 0$, $\mathbf{x}(t)$ solution of the IVP $(\dot{\mathbf{x}} = \mathbf{f}, \mathbf{x}(0) = \mathbf{x}_0)$ is a zero of p

N.B. Treating $\dot{\mathbf{x}} = \mathbf{f}$ as a program, one can think of the top formula as representing the Hoare triple $\{p = 0\}\ \dot{\mathbf{x}} = \mathbf{f}\ \{p = 0\}$.

Notation for "$p = 0$ is invariant for $\mathbf{f}$"

$$(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p = 0)$$
$$\equiv$$
Zero set of p is an invariant algebraic set for $\mathbf{f}$
$$\equiv$$
Starting with $\mathbf{x}_0$ s.t $p(\mathbf{x}_0) = 0$: for all $t > 0$, $\mathbf{x}(t)$ solution of the IVP $(\dot{\mathbf{x}} = \mathbf{f}, \mathbf{x}(0) = \mathbf{x}_0)$ is a zero of p

N.B. Treating $\dot{\mathbf{x}} = \mathbf{f}$ as a program, one can think of the top formula as representing the Hoare triple $\{p = 0\}\ \dot{\mathbf{x}} = \mathbf{f}\ \{p = 0\}$.

Some Useful 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.

Differential Radical Characterization

[TACAS'14]

$$\mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{(N_p-1)}(p)\rangle \ \wedge \ p = 0 \rightarrow \mathfrak{D}^{(N_p-1)}(p) = 0$$

$$\vdots$$

$$\mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge \ p = 0 \rightarrow \mathfrak{D}^{(2)}(p) = 0$$

$$\mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge \ p = 0 \rightarrow \mathfrak{D}(p) = 0$$

$$\frac{\mathfrak{D}(p) \in \langle p\rangle \ (\exists \lambda \in \mathbb{R}[\mathbf{x}] : \mathfrak{D}(p) = \lambda p)}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p = 0)}$$

- order N_p is **finite**: **unknown** a priori and **computed on the fly**
- $< N_p$ ideal membership problems: $\mathfrak{D}^{(i+1)}(p) \in \langle p, \ldots, \mathfrak{D}^{(i)}(p)\rangle$
- $< N_p - 1$ quantifier elimination problems: $p = 0 \rightarrow \mathfrak{D}^{(i)}(p) = 0$

Differential Radical Characterization

[TACAS'14]

$$\mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{(N_p-1)}(p)\rangle \ \wedge \ p = 0 \rightarrow \mathfrak{D}^{(N_p-1)}(p) = 0$$

$$\vdots$$

$$\mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge \ p = 0 \rightarrow \mathfrak{D}^{(2)}(p) = 0$$

$$\mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge \ p = 0 \rightarrow \mathfrak{D}(p) = 0$$

$$\text{✗}\mathfrak{D}(p) \in \langle p\rangle \ (\exists \lambda \in \mathbb{R}[\mathbf{x}] : \mathfrak{D}(p) = \lambda p)$$

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

- order N_p is **finite**: **unknown** a priori and **computed on the fly**
- $< N_p$ ideal membership problems: $\mathfrak{D}^{(i+1)}(p) \in \langle p, \ldots, \mathfrak{D}^{(i)}(p)\rangle$
- $< N_p - 1$ quantifier elimination problems: $p = 0 \rightarrow \mathfrak{D}^{(i)}(p) = 0$

Differential Radical Characterization

[TACAS'14]

$$\mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{(N_p-1)}(p)\rangle \ \wedge \ p = 0 \rightarrow \mathfrak{D}^{(N_p-1)}(p) = 0$$

$$\vdots$$

$$\mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge \ p = 0 \rightarrow \mathfrak{D}^{(2)}(p) = 0$$

$$\text{✗}\mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge \ p = 0 \rightarrow \mathfrak{D}(p) = 0\text{✓}$$

$$\text{✗}\mathfrak{D}(p) \in \langle p\rangle \ (\exists \lambda \in \mathbb{R}[\mathbf{x}] : \mathfrak{D}(p) = \lambda p)$$

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

- order N_p is **finite**: **unknown** a priori and **computed on the fly**
- $< N_p$ ideal membership problems: $\mathfrak{D}^{(i+1)}(p) \in \langle p, \ldots, \mathfrak{D}^{(i)}(p)\rangle$
- $< N_p - 1$ quantifier elimination problems: $p = 0 \rightarrow \mathfrak{D}^{(i)}(p) = 0$

Differential Radical Characterization

[TACAS'14]

$$\frac{\begin{array}{c}\checkmark\mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{(N_p-1)}(p)\rangle \ \wedge\ p = 0 \rightarrow \mathfrak{D}^{(N_p-1)}(p) = 0\checkmark \\ \vdots \\ \times\mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge\ p = 0 \rightarrow \mathfrak{D}^{(2)}(p) = 0\checkmark \\ \times\mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge\ p = 0 \rightarrow \mathfrak{D}(p) = 0\checkmark \\ \times\mathfrak{D}(p) \in \langle p\rangle \ (\exists \lambda \in \mathbb{R}[\mathbf{x}] : \mathfrak{D}(p) = \lambda p)\end{array}}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p = 0)}$$

- order N_p is **finite**: **unknown** a priori and **computed on the fly**
- $< N_p$ ideal membership problems: $\mathfrak{D}^{(i+1)}(p) \in \langle p, \ldots, \mathfrak{D}^{(i)}(p)\rangle$
- $< N_p - 1$ quantifier elimination problems: $p = 0 \rightarrow \mathfrak{D}^{(i)}(p) = 0$

Differential Radical Characterization

[TACAS'14]

$$\frac{\begin{array}{c}\checkmark\mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{(N_p-1)}(p)\rangle \ \wedge\ p = 0 \rightarrow \mathfrak{D}^{(N_p-1)}(p) = 0\checkmark \\ \vdots \\ \times\mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge\ p = 0 \rightarrow \mathfrak{D}^{(2)}(p) = 0\checkmark \\ \times\mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge\ p = 0 \rightarrow \mathfrak{D}(p) = 0\checkmark \\ \times\mathfrak{D}(p) \in \langle p\rangle \ (\exists \lambda \in \mathbb{R}[\mathbf{x}] : \mathfrak{D}(p) = \lambda p)\end{array}}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p = 0)}$$

- order N_p is **finite**: **unknown** a priori and **computed on the fly**
- $< N_p$ ideal membership problems: $\mathfrak{D}^{(i+1)}(p) \in \langle p, \ldots, \mathfrak{D}^{(i)}(p)\rangle$
- $< N_p - 1$ quantifier elimination problems: $p = 0 \rightarrow \mathfrak{D}^{(i)}(p) = 0$

Differential Radical Characterization

[TACAS'14]

$$\frac{\begin{array}{c}\checkmark\mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{(N_p-1)}(p)\rangle \ \wedge\ p = 0 \rightarrow \mathfrak{D}^{(N_p-1)}(p) = 0\checkmark \\ \vdots \\ \times\mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge\ p = 0 \rightarrow \mathfrak{D}^{(2)}(p) = 0\checkmark \\ \times\mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge\ p = 0 \rightarrow \mathfrak{D}(p) = 0\checkmark \\ \times\mathfrak{D}(p) \in \langle p\rangle \ (\exists \lambda \in \mathbb{R}[\mathbf{x}] : \mathfrak{D}(p) = \lambda p)\end{array}}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p = 0)}$$

- order N_p is **finite**: **unknown** a priori and **computed on the fly**
- $< N_p$ ideal membership problems: $\mathfrak{D}^{(i+1)}(p) \in \langle p, \ldots, \mathfrak{D}^{(i)}(p)\rangle$
- $< N_p - 1$ quantifier elimination problems: $p = 0 \rightarrow \mathfrak{D}^{(i)}(p) = 0$

Differential Radical Characterization

[TACAS'14]

$$\frac{\begin{array}{c}\checkmark\mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{(N_p-1)}(p)\rangle \ \wedge\ p = 0 \rightarrow \mathfrak{D}^{(N_p-1)}(p) = 0\checkmark \\ \vdots \\ \times\mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge\ p = 0 \rightarrow \mathfrak{D}^{(2)}(p) = 0\checkmark \\ \times\mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge\ p = 0 \rightarrow \mathfrak{D}(p) = 0\checkmark \\ \times\mathfrak{D}(p) \in \langle p\rangle \ (\exists \lambda \in \mathbb{R}[\mathbf{x}] : \mathfrak{D}(p) = \lambda p)\end{array}}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p = 0)}$$

- order N_p is **finite**: **unknown** a priori and **computed on the fly**
- $< N_p$ ideal membership problems: $\mathfrak{D}^{(i+1)}(p) \in \langle p, \ldots, \mathfrak{D}^{(i)}(p)\rangle$
- $< N_p - 1$ quantifier elimination problems: $p = 0 \rightarrow \mathfrak{D}^{(i)}(p) = 0$

Naïve Approach: DRI + Sum of Squares

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

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

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

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

- ⊕ Decides **all** algebraic invariants
- ⊖ Increases the total polynomial degree $\rightsquigarrow$ **bad complexity**

Liu et al. EMSOTF'11

$$\frac{\begin{array}{c}\mathfrak{D}^{(N_q)}(q) \in \langle q, \ldots, \mathfrak{D}^{N_q-1}(q)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_q-1)}(q)=0 \\ \vdots \\ \mathfrak{D}^{(3)}(q) \in \langle q, \mathfrak{D}(q), \mathfrak{D}^{(2)}(q)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(q)=0 \\ \mathfrak{D}^{(2)}(q) \in \langle q, \mathfrak{D}(q)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(q)=0 \\ \mathfrak{D}(q) \in \langle q\rangle \\ \wedge \\ \mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{N_p-1}(p)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_p-1)}(p)=0 \\ \vdots \\ \mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(p)=0 \\ \mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(p)=0 \\ \mathfrak{D}(p) \in \langle p\rangle \end{array}}{(p=0 \wedge q=0) \rightarrow [\dot{\mathbf{x}}=\mathbf{f}](p=0 \wedge q=0)}$$

- Two **different** orders N_p and N_q
- $< N_p + N_q$ ideal membership problems
- $< N_p - 1 + N_q - 1$ quantifier elimination problems

Liu et al. EMSOTF'11

$$\mathfrak{D}^{(N_q)}(q) \in \langle q, \ldots, \mathfrak{D}^{N_q-1}(q)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_q-1)}(q) = 0$$
$$\vdots$$
$$\mathfrak{D}^{(3)}(q) \in \langle q, \mathfrak{D}(q), \mathfrak{D}^{(2)}(q)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(q) = 0$$
$$\mathfrak{D}^{(2)}(q) \in \langle q, \mathfrak{D}(q)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(q) = 0$$
$$\mathfrak{D}(q) \in \langle q\rangle$$
$$\wedge$$
$$\mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{N_p-1}(p)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_p-1)}(p) = 0$$
$$\vdots$$
$$\mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(p) = 0$$
$$\mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(p) = 0$$
$$\mathfrak{D}(p) \in \langle p\rangle$$

$$(p=0 \wedge q=0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p=0 \wedge q=0)$$

- Two **different** orders N_p and N_q
- $< N_p + N_q$ ideal membership problems
- $< N_p - 1 + N_q - 1$ quantifier elimination problems

Liu et al. EMSOTF'11

$$\mathfrak{D}^{(N_q)}(q) \in \langle q, \ldots, \mathfrak{D}^{N_q-1}(q)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_q-1)}(q)=0$$
$$\vdots$$
$$\mathfrak{D}^{(3)}(q) \in \langle q, \mathfrak{D}(q), \mathfrak{D}^{(2)}(q)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(q)=0$$
$$\mathfrak{D}^{(2)}(q) \in \langle q, \mathfrak{D}(q)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(q)=0$$
$$\mathfrak{D}(q) \in \langle q\rangle$$
$$\wedge$$
$$\mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{N_p-1}(p)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_p-1)}(p)=0$$
$$\vdots$$
$$\mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(p)=0$$
$$\mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(p)=0$$
$$\mathfrak{D}(p) \in \langle p\rangle$$

$$(p=0 \wedge q=0) \rightarrow [\dot{\mathbf{x}}=\mathbf{f}](p=0 \wedge q=0)$$

- Two **different** orders N_p and N_q
- $< N_p + N_q$ ideal membership problems
- $< N_p - 1 + N_q - 1$ quantifier elimination problems

Liu et al. EMSOTF'11

$$\mathfrak{D}^{(N_q)}(q) \in \langle q, \ldots, \mathfrak{D}^{N_q-1}(q)\rangle \ \wedge \ (p = 0 \wedge q = 0) \rightarrow \mathfrak{D}^{(N_q-1)}(q) = 0$$
$$\vdots$$
$$\mathfrak{D}^{(3)}(q) \in \langle q, \mathfrak{D}(q), \mathfrak{D}^{(2)}(q)\rangle \ \wedge \ (p = 0 \wedge q = 0) \rightarrow \mathfrak{D}^{(2)}(q) = 0$$
$$\mathfrak{D}^{(2)}(q) \in \langle q, \mathfrak{D}(q)\rangle \ \wedge \ (p = 0 \wedge q = 0) \rightarrow \mathfrak{D}(q) = 0$$
$$\mathfrak{D}(q) \in \langle q\rangle$$
$$\wedge$$
$$\mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{N_p-1}(p)\rangle \ \wedge \ (p = 0 \wedge q = 0) \rightarrow \mathfrak{D}^{(N_p-1)}(p) = 0$$
$$\vdots$$
$$\mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge \ (p = 0 \wedge q = 0) \rightarrow \mathfrak{D}^{(2)}(p) = 0$$
$$\mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge \ (p = 0 \wedge q = 0) \rightarrow \mathfrak{D}(p) = 0$$
$$\mathfrak{D}(p) \in \langle p\rangle$$

$$(p = 0 \wedge q = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p = 0 \wedge q = 0)$$

- Two **different** orders N_p and N_q
- $< N_p + N_q$ ideal membership problems
- $< N_p - 1 + N_q - 1$ quantifier elimination problems

Liu et al. EMSOTF'11

$$\mathfrak{D}^{(N_q)}(q) \in \langle q, \ldots, \mathfrak{D}^{N_q-1}(q)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_q-1)}(q) = 0$$
$$\vdots$$
$$\mathfrak{D}^{(3)}(q) \in \langle q, \mathfrak{D}(q), \mathfrak{D}^{(2)}(q)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(q) = 0$$
$$\mathfrak{D}^{(2)}(q) \in \langle q, \mathfrak{D}(q)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(q) = 0$$
$$\mathfrak{D}(q) \in \langle q\rangle$$

$$\wedge$$

$$\mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{N_p-1}(p)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_p-1)}(p) = 0$$
$$\vdots$$
$$\mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(p) = 0$$
$$\mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(p) = 0$$
$$\mathfrak{D}(p) \in \langle p\rangle$$

$$(p=0 \wedge q=0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p=0 \wedge q=0)$$

- Two **different** orders N_p and N_q
- $< N_p + N_q$ ideal membership problems
- $< N_p - 1 + N_q - 1$ quantifier elimination problems

Liu et al. EMSOTF'11

$$\frac{\begin{array}{c}\mathfrak{D}(q) \in \langle q \rangle \\ \wedge \\ \mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{N_p-1}(p) \rangle \ \wedge \ (p = 0 \wedge q = 0) \rightarrow \mathfrak{D}^{(N_p-1)}(p) = 0 \\ \vdots \\ \mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p) \rangle \ \wedge \ (p = 0 \wedge q = 0) \rightarrow \mathfrak{D}^{(2)}(p) = 0 \\ \mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p) \rangle \ \wedge \ (p = 0 \wedge q = 0) \rightarrow \mathfrak{D}(p) = 0 \\ \mathfrak{D}(p) \in \langle p \rangle \end{array}}{(p = 0 \wedge q = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p = 0 \wedge q = 0)}$$

- Two **different** orders N_p and N_q
- $< N_p + N_q$ ideal membership problems
- $< N_p - 1 + N_q - 1$ quantifier elimination problems

Liu et al. EMSOTF'11

$$\mathfrak{D}^{(N_q)}(q) \in \langle q, \ldots, \mathfrak{D}^{N_q-1}(q)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_q-1)}(q)=0$$

$$\vdots$$

$$\mathfrak{D}^{(3)}(q) \in \langle q, \mathfrak{D}(q), \mathfrak{D}^{(2)}(q)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(q)=0$$

$$\mathfrak{D}^{(2)}(q) \in \langle q, \mathfrak{D}(q)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(q)=0$$

$$\mathfrak{D}(q) \in \langle q\rangle$$

$$\wedge$$

$$\mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{N_p-1}(p)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_p-1)}(p)=0$$

$$\vdots$$

$$\mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(p)=0$$

$$\mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(p)=0$$

$$\mathfrak{D}(p) \in \langle p\rangle$$

$$(p=0 \wedge q=0) \rightarrow [\dot{\mathbf{x}}=\mathbf{f}](p=0 \wedge q=0)$$

- Two **different** orders N_p and N_q
- $< N_p + N_q$ ideal membership problems
- $< N_p - 1 + N_q - 1$ quantifier elimination problems

Liu et al. EMSOTF'11

$$\frac{\begin{array}{c}\mathfrak{D}^{(N_q)}(q) \in \langle q, \ldots, \mathfrak{D}^{N_q-1}(q)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_q-1)}(q)=0 \\ \vdots \\ \mathfrak{D}^{(3)}(q) \in \langle q, \mathfrak{D}(q), \mathfrak{D}^{(2)}(q)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(q)=0 \\ \mathfrak{D}^{(2)}(q) \in \langle q, \mathfrak{D}(q)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(q)=0 \\ \mathfrak{D}(q) \in \langle q\rangle \\ \wedge \\ \mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{N_p-1}(p)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_p-1)}(p)=0 \\ \vdots \\ \mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(p)=0 \\ \mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(p)=0 \\ \mathfrak{D}(p) \in \langle p\rangle \end{array}}{(p=0 \wedge q=0) \rightarrow [\dot{\mathbf{x}}=\mathbf{f}](p=0 \wedge q=0)}$$

- Two **different** orders N_p and N_q
- $< N_p + N_q$ ideal membership problems
- $< N_p - 1 + N_q - 1$ quantifier elimination problems

Liu et al. EMSOTF'11

$$\frac{\begin{array}{c}\mathfrak{D}^{(N_q)}(q) \in \langle q, \ldots, \mathfrak{D}^{N_q-1}(q)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_q-1)}(q)=0 \\ \vdots \\ \mathfrak{D}^{(3)}(q) \in \langle q, \mathfrak{D}(q), \mathfrak{D}^{(2)}(q)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(q)=0 \\ \mathfrak{D}^{(2)}(q) \in \langle q, \mathfrak{D}(q)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(q)=0 \\ \mathfrak{D}(q) \in \langle q\rangle \\ \wedge \\ \mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{N_p-1}(p)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_p-1)}(p)=0 \\ \vdots \\ \mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(p)=0 \\ \mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(p)=0 \\ \mathfrak{D}(p) \in \langle p\rangle\end{array}}{(p=0 \wedge q=0) \rightarrow [\dot{\mathbf{x}}=\mathbf{f}](p=0 \wedge q=0)}$$

- Two **different** orders N_p and N_q
- $< N_p + N_q$ ideal membership problems
- $< N_p - 1 + N_q - 1$ quantifier elimination problems

Liu et al. EMSOTF'11

$$\frac{\begin{array}{c}
\mathfrak{D}^{(N_q)}(q) \in \langle q, \ldots, \mathfrak{D}^{N_q-1}(q)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_q-1)}(q)=0 \\
\vdots \\
\mathfrak{D}^{(3)}(q) \in \langle q, \mathfrak{D}(q), \mathfrak{D}^{(2)}(q)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(q)=0 \\
\mathfrak{D}^{(2)}(q) \in \langle q, \mathfrak{D}(q)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(q)=0 \\
\mathfrak{D}(q) \in \langle q\rangle \\
\wedge \\
\mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{N_p-1}(p)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_p-1)}(p)=0 \\
\vdots \\
\mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(p)=0 \\
\mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(p)=0 \\
\mathfrak{D}(p) \in \langle p\rangle
\end{array}}{(p=0 \wedge q=0) \rightarrow [\dot{\mathbf{x}}=\mathbf{f}](p=0 \wedge q=0)}$$

- Two **different** orders N_p and N_q
- $< N_p + N_q$ ideal membership problems
- $< N_p - 1 + N_q - 1$ quantifier elimination problems

Liu et al. EMSOTF'11

$$\frac{\begin{array}{c}\mathfrak{D}^{(N_q)}(q) \in \langle q, \ldots, \mathfrak{D}^{N_q-1}(q)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_q-1)}(q)=0 \\ \vdots \\ \mathfrak{D}^{(3)}(q) \in \langle q, \mathfrak{D}(q), \mathfrak{D}^{(2)}(q)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(q)=0 \\ \mathfrak{D}^{(2)}(q) \in \langle q, \mathfrak{D}(q)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(q)=0 \\ \mathfrak{D}(q) \in \langle q\rangle \\ \wedge \\ \mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{N_p-1}(p)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_p-1)}(p)=0 \\ \vdots \\ \mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(p)=0 \\ \mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge\ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(p)=0 \\ \mathfrak{D}(p) \in \langle p\rangle\end{array}}{(p=0 \wedge q=0) \rightarrow [\dot{\mathbf{x}}=\mathbf{f}](p=0 \wedge q=0)}$$

- Two **different** orders N_p and N_q
- $< N_p + N_q$ ideal membership problems
- $< N_p - 1 + N_q - 1$ quantifier elimination problems

Liu et al. EMSOTF'11

$$\frac{\begin{array}{c}\mathfrak{D}^{(N_q)}(q) \in \langle q, \ldots, \mathfrak{D}^{N_q-1}(q)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_q-1)}(q) = 0 \\ \vdots \\ \mathfrak{D}^{(3)}(q) \in \langle q, \mathfrak{D}(q), \mathfrak{D}^{(2)}(q)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(q) = 0 \\ \mathfrak{D}^{(2)}(q) \in \langle q, \mathfrak{D}(q)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(q) = 0 \\ \mathfrak{D}(q) \in \langle q\rangle \\ \wedge \\ \mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{N_p-1}(p)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(N_p-1)}(p) = 0 \\ \vdots \\ \mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}^{(2)}(p) = 0 \\ \mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge \ (p=0 \wedge q=0) \rightarrow \mathfrak{D}(p) = 0 \\ \mathfrak{D}(p) \in \langle p\rangle \end{array}}{(p=0 \wedge q=0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}](p=0 \wedge q=0)}$$

- Two **different** orders N_p and N_q
- $< N_p + N_q$ ideal membership problems
- $< N_p - 1 + N_q - 1$ quantifier elimination problems

Conjunctive Differential Radical Characterization

Theorem 2, Algorithm 1, paper

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

- $N_{p,q}$ is a **unique** order for the **entire** conjunction, **shared** between p and q
- $N_{p,q}$ ideal membership problems
- $\min(N_p, N_{p,q}) - 1 + \min(N_q, N_{p,q}) - 1$ quantifier elimination problems

Conjunctive Differential Radical Characterization

Theorem 2, Algorithm 1, paper

$$\mathfrak{D}^{(N_{p,q})}(p), \mathfrak{D}^{(N_{p,q})}(q) \in \langle p, q, \ldots, \mathfrak{D}^{(N_{p,q}-1)}(p), \mathfrak{D}^{(N_{p,q}-1)}(q) \rangle$$
$$\wedge\ (p = 0 \wedge q = 0) \rightarrow \mathfrak{D}^{(N_{p,q}-1)}(p) = 0 \wedge \mathfrak{D}^{(N_{p,q}-1)}(q) = 0$$

$$\vdots$$

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

- $N_{p,q}$ is a **unique** order for the **entire** conjunction, **shared** between p and q
- $N_{p,q}$ ideal membership problems
- $\min(N_p, N_{p,q}) - 1 + \min(N_q, N_{p,q}) - 1$ quantifier elimination problems

Conjunctive Differential Radical Characterization

Theorem 2, Algorithm 1, paper

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

- $N_{p,q}$ is a **unique** order for the **entire** conjunction, **shared** between p and q
- $N_{p,q}$ ideal membership problems
- $\min(N_p, N_{p,q}) - 1 + \min(N_q, N_{p,q}) - 1$ quantifier elimination problems

Conjunctive Differential Radical Characterization

Theorem 2, Algorithm 1, paper

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

- $N_{p,q}$ is a **unique** order for the **entire** conjunction, **shared** between p and q
- $N_{p,q}$ ideal membership problems
- $\min(N_p, N_{p,q}) - 1 + \min(N_q, N_{p,q}) - 1$ quantifier elimination problems

Conjunctive Differential Radical Characterization

Theorem 2, Algorithm 1, paper

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

- $N_{p,q}$ is a **unique** order for the **entire** conjunction, **shared** between p and q
- $N_{p,q}$ ideal membership problems
- $\min(N_p, N_{p,q}) - 1 + \min(N_q, N_{p,q}) - 1$ quantifier elimination problems

Conjunctive Differential Radical Characterization

Theorem 2, Algorithm 1, paper

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

- $N_{p,q}$ is a **unique** order for the **entire** conjunction, **shared** between p and q
- $N_{p,q}$ ideal membership problems
- $\min(N_p, N_{p,q}) - 1 + \min(N_q, N_{p,q}) - 1$ quantifier elimination problems

Illustrative Example

$N_p, N_q > 1$:

$$\text{(Liu et al.)}\frac{\begin{array}{cc}\vdots & \vdots \\ \mathfrak{D}(x_1) = x_2 \notin \langle x_1 \rangle & \mathfrak{D}(x_2) = x_1 \notin \langle x_2 \rangle\end{array}}{(x_1 = 0 \wedge x_2 = 0) \longrightarrow [\dot{\mathbf{x}} = (x_2, x_1)]\,(x_1 = 0 \wedge x_2 = 0)}$$

$N_{p,q} = 1$ using the **larger** ideal $\langle x_1, x_2 \rangle$:

$$\text{(DRI}^{\wedge}\text{)}\frac{\mathfrak{D}(x_1), \mathfrak{D}(x_2) \in \langle x_1, x_2 \rangle}{(x_1 = 0 \wedge x_2 = 0) \longrightarrow [\dot{\mathbf{x}} = (x_2, x_1)]\,(x_1 = 0 \wedge x_2 = 0)}$$

Computational Advantages

- $N_{p,q} \leq \max(N_p, N_q) \rightsquigarrow$ polynomials with **smaller total degree**

	Liu et al.	DRI$^\wedge$
Orders:	$N_p,\ N_q$	$N_{p,q}$
Ideal membership problems:	$N_p + N_q$	$N_{p,q}$
Quantifier elimination problems:	$N_p - 1 + N_q - 1$	$\min(N_p, N_{p,q}) - 1$ $+ \min(N_q, N_{p,q}) - 1$

- Theoretically: **Better worst case complexity**
- Empirically: **Better performance on average**

Benchmarks

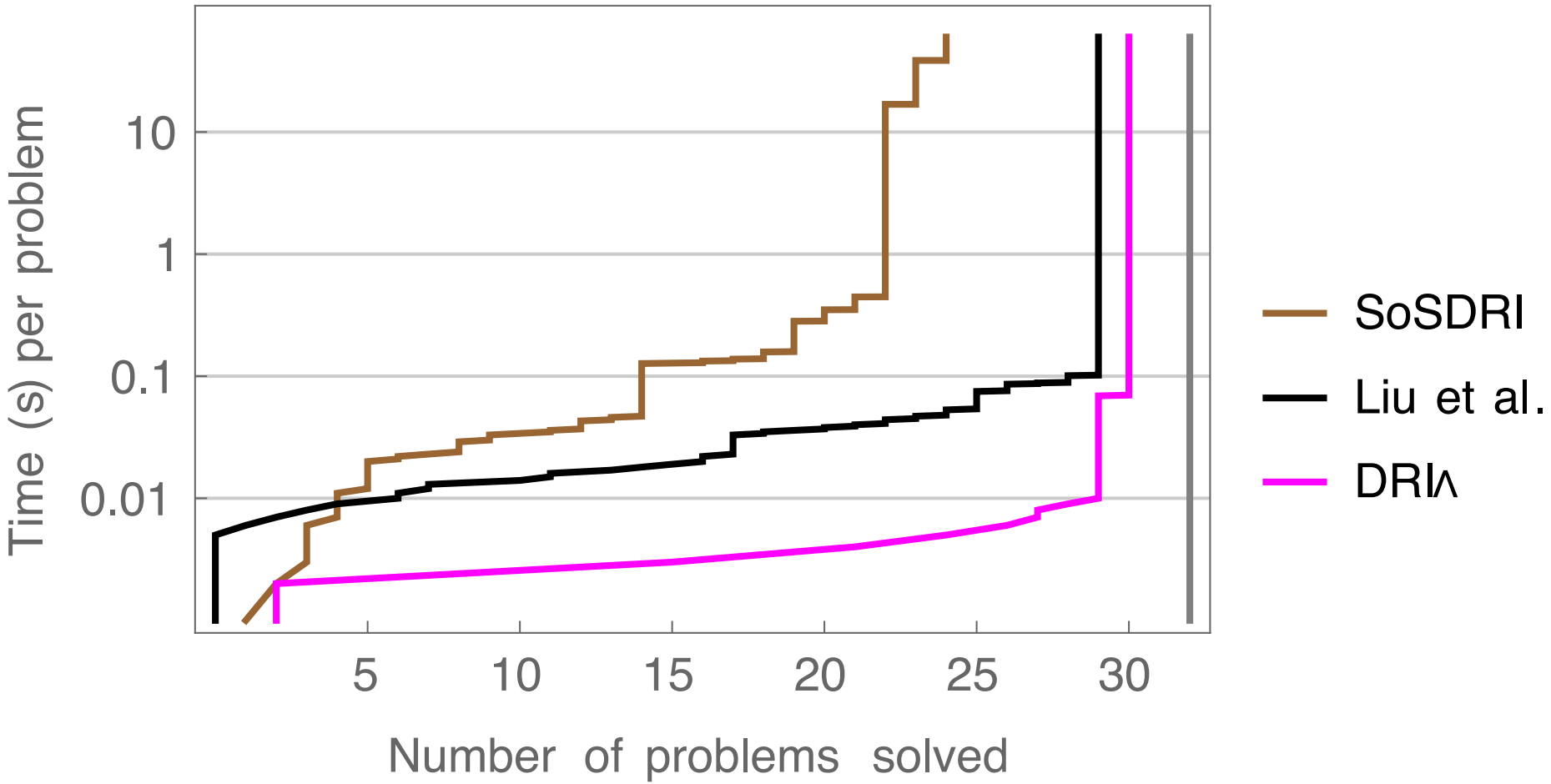
The set of benchmarks contains 32 entries:

- equilibria (16)
- singularities (8)
- higher integrals (4)
- abstract examples (4)

Originate from a number of sources:

- textbooks on Dynamical Systems
- hand-crafted to exploit sweetspots of certain proof rules

Empirical Performance Comparison



Outline

Notation for "evolution is restricted to the set C"

$$(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f} \ \& \ C](p = 0)$$

$$\equiv$$

Zero set of p is an invariant algebraic set for $\mathbf{f}$ subject to constraint C

$$\equiv$$

Restricting evolution to C and starting with $\mathbf{x}_0$ s.t. $p(\mathbf{x}_0) = 0$, for all $t > 0$, $\mathbf{x}(t) \in C$ implies $p(\mathbf{x}(t)) = 0$

Notation for "evolution is restricted to the set C"

$$(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f} \ \& \ C](p = 0)$$

$$\equiv$$

Zero set of p is an invariant algebraic set for $\mathbf{f}$ subject to constraint C

$$\equiv$$

Restricting evolution to C and starting with $\mathbf{x}_0$ s.t. $p(\mathbf{x}_0) = 0$, for all $t > 0$, $\mathbf{x}(t) \in C$ implies $p(\mathbf{x}(t)) = 0$

Notation for "evolution is restricted to the set C"

$$(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f} \ \& \ C](p = 0)$$

$$\equiv$$

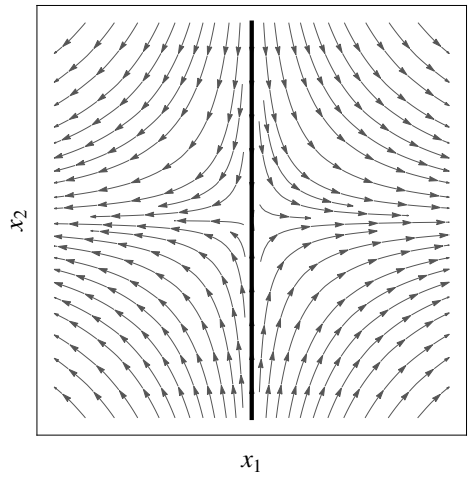
Zero set of p is an invariant algebraic set for $\mathbf{f}$ subject to constraint C

$$\equiv$$

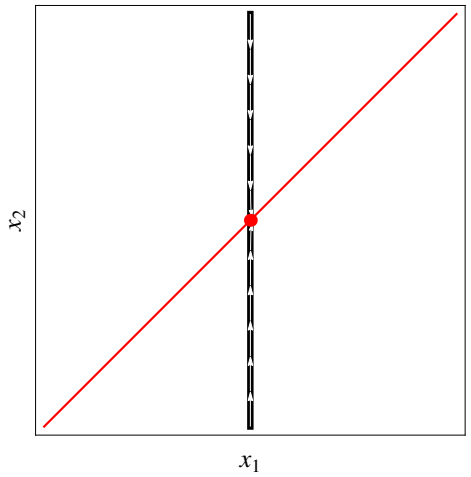
Restricting evolution to C and starting with $\mathbf{x}_0$ s.t. $p(\mathbf{x}_0) = 0$, for all $t > 0$,
$\mathbf{x}(t) \in C$ implies $p(\mathbf{x}(t)) = 0$

Idea Behind Differential Cuts

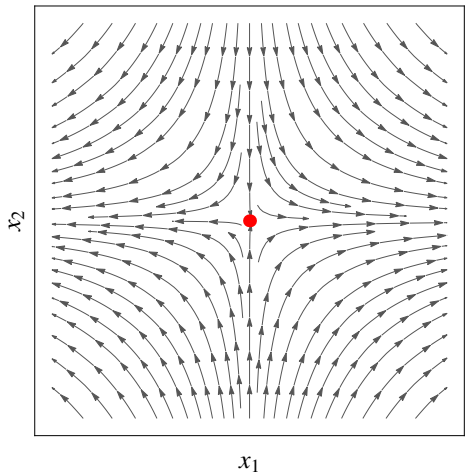
$F \to [\dot{\mathbf{x}} = \mathbf{p}]C$



$F \to [\dot{\mathbf{x}} = \mathbf{p}\ \&\ C]F$



(DC)



$F \to [\dot{\mathbf{x}} = \mathbf{p}]F$

Sufficient Conditions for Invariance of Atomic Equalities

$$(\mathrm{DI}_{=})\frac{C \vdash \mathfrak{D}(p) = 0}{(p = 0) \to [\dot{\mathbf{x}} = \mathbf{f} \;\&\; C](p = 0)} \qquad \text{Conserved quantities}$$

$$(\mathrm{Lie})\frac{C \vdash p = 0 \to (\mathfrak{D}(p) = 0 \wedge \nabla p \neq \mathbf{0})}{(p = 0) \to [\dot{\mathbf{x}} = \mathbf{f} \;\&\; C](p = 0)} \qquad \text{Smooth invariant manifolds}$$

Checking Invariance with Differential Cuts

Differential cuts increase the deductive power

- of DI [Platzer'10]
- of Lie [Theorem 11, paper]

(DC) increases the deductive power

- DC + Lie $\leftrightarrow$ embedding of smooth invariant manifolds
- DC + $\text{DI}_{=}$ $\leftrightarrow$ higher-order integrals of dynamical systems

(DC) can also combine proof rules to produce very efficient proofs of invariance where all other methods would take unreasonably long.

Example: Defeats (DRI$^\wedge$), easy to prove using (DI+DC)

$$\left.\begin{array}{rl}
\dot{x}_1 &= -292x_7(-1+x_6^2+x_7^2+x_8^2)^{145},\\
\dot{x}_2 &= -292x_8(-1+x_6^2+x_7^2+x_8^2)^{145},\\
\dot{x}_3 &= -42(2x_{10}+2x_{10}^3+2x_9)(-3+6x_{10}^2+x_{10}^4+2x_{10}x_9+2x_{10}^3x_9+x_9^2)^{41},\\
\dot{x}_4 &= -42(12x_{10}+4x_{10}^3+2x_9+6x_{10}^2x_9)(-3+6x_{10}^2+x_{10}^4+2x_{10}x_9+2x_{10}^3x_9+x_9^2)^{41},\\
\dot{x}_5 &= -2x_{13}(-1+x_{13}+x_{11}x_{13}),\\
\dot{x}_6 &= -2x_{12}(-1+x_{12}+x_{11}x_{12}),\\
\dot{x}_7 &= 26(-6x_1x_2^2+4x_1^3x_2^2+2x_1x_2^4)(1-3x_1^2x_2^2+x_1^4x_2^2+x_1^2x_2^4)^{25},\\
\dot{x}_8 &= 26(-6x_1^2x_2+2x_1^4x_2+4x_1^2x_2^3)(1-3x_1^2x_2^2+x_1^4x_2^2+x_1^2x_2^4)^{25},\\
\dot{x}_9 &= 14(4x_3^3x_4^2+2x_3x_4^4-6x_3x_4^2x_5^2)(x_3^4x_4^2+x_3^2x_4^4-3x_3^2x_4^2x_5^2+x_5^6)^{13},\\
\dot{x}_{10} &= 14(2x_3^4x_4+4x_3^2x_4^3-6x_3^2x_4x_5^2)(x_3^4x_4^2+x_3^2x_4^4-3x_3^2x_4^2x_5^2+x_5^6)^{13},\\
\dot{x}_{11} &= 14(-6x_3^2x_4^2x_5+6x_5^5)(x_3^4x_4^2+x_3^2x_4^4-3x_3^2x_4^2x_5^2+x_5^6)^{13},\\
\dot{x}_{12} &= 292x_6(-1+x_6^2+x_7^2+x_8^2)^{145},\\
\dot{x}_{13} &= -x_{13}.
\end{array}\right\} \mathbf{f}$$

Invariant:

$$\begin{aligned}
x_{13}=0 \quad \wedge \quad & ((x_1^4x_2^2+x_1^2x_2^4-3x_1^2x_2^2+1)^{13})^2 \quad + \\
& ((x_3^4x_4^2+x_3^2x_4^4-3x_3^2x_4^2x_5^2+x_5^6)^7)^2 \quad + \\
& ((-1+x_6^2+x_7^2+x_8^2)^{73})^2 \quad + \\
& ((-3+6x_{10}^2+x_{10}^4+2x_{10}x_9+2x_{10}^3x_9+x_9^2)^{21})^2 \quad + \\
& (x_{12}+x_{11}x_{12}-1)^2=0.
\end{aligned}$$

Search for Cut Candidates

Question:

What is a suitable conjunct to "cut by" ?

Heuristics:

- Order the polynomials with respect to the number of variables and their total degrees
- Use $\mathrm{DI}_{=}$, then Lie, to try to prove invariance of each conjunct separately
- Apply some invariant equality in the conjunct to DC, obtaining a constrained system
- Remove invariant equality from the conjunct and iterate on the constrained system.

Conclusion

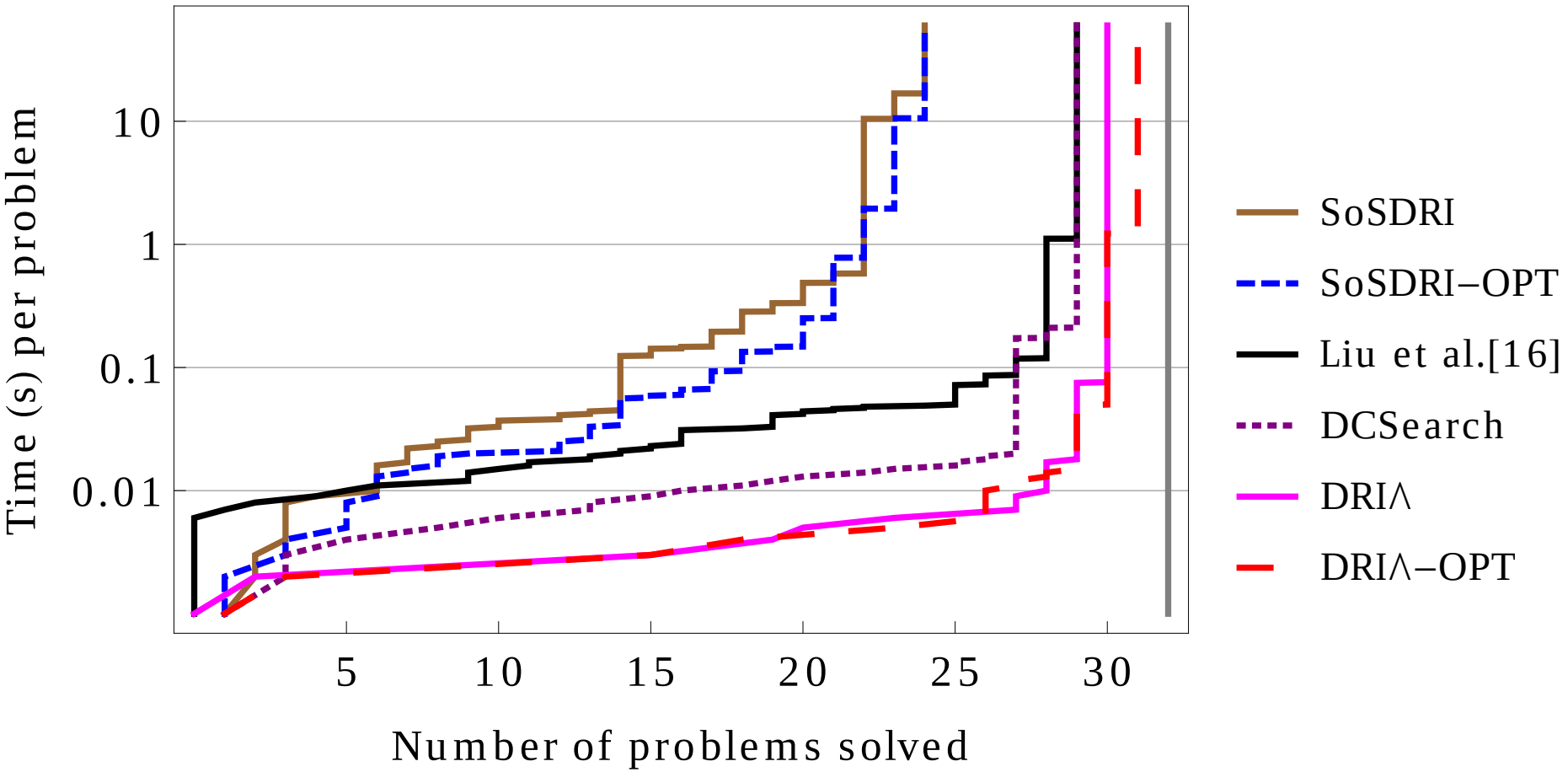
Deciding Invariance of Algebraic Sets

- New **efficient decision procedure** to check the invariance of algebraic sets
- New insights: embedding of invariants $\leftrightharpoons$ differential cut proof rule
- **efficient tactics** for the invariance of algebraic sets

Toward generalized efficient procedures and tactics for semi-algebraic sets

How to leverage the algebraic structure underlying *semi-algebraic* sets ?

Empirical Performance, Complete Comparison



Abstraction ...

Algebraic Framework

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

$$\underset{\text{smallest variety}}{}$$

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

Closure $V(I(\mathcal{O}(\mathbf{x}_0)))$ common roots of all polynomials in $I(\mathcal{O}(\mathbf{x}_0))$