

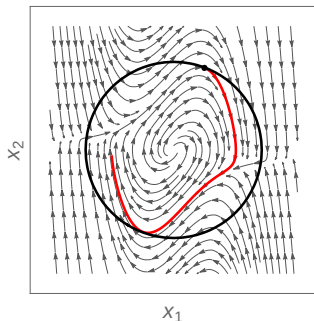
A Hierarchy of Proof Rules for Checking Differential Invariance of Algebraic Sets

Khalil Ghorbal¹ **Andrew Sogokon**² **André Platzer**¹

1. Carnegie Mellon University
2. University of Edinburgh

VMCAI, Mumbai, India
January 13th, 2015

Problem: Checking the Invariance of Algebraic Sets



Ordinary Differential Equation

$$\begin{pmatrix} \dot{x} \\ \dot{y} \end{pmatrix} = \begin{pmatrix} y \\ -x + (1 - x^2)y \end{pmatrix} = \mathbf{p}$$

(Real) Algebraic Sets

$$V_{\mathbb{R}}(h) = \{(x, y) \in \mathbb{R} \mid \underbrace{x^2 + y^2 - 1}_{h(x,y)=0} = 0\}$$

Context

Motivations

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

Current Status

- Invariance of algebraic sets is **decidable**
- A decision procedure exists
- Many sufficient conditions are known

Contributions

Hierarchy of the different proof rules

- Compare the deductive power of 7 proof rules, **2 of which are novel**
- **Subclasses** of algebraic sets **characterized** by each proof rule

Assess the deductive power versus efficiency trade-off

- **Deductive power** increase $\rightsquigarrow$ **computational cost** increase ?
- What is the **practical efficiency** of those proof rules ?

Outline

- 1 Introduction
- 2 Proof rules
- 3 Deductive Hierarchy
- 4 Practical performance analysis
- 5 Square-free Reduction
- 6 Conclusion

Definitions

Gradient $\nabla h := \left(\frac{\partial h}{\partial x_1}, \dots, \frac{\partial h}{\partial x_n} \right)$

Lie Derivation $\mathfrak{D}_{\mathbf{p}}(h) := \frac{dh(\mathbf{x}(t))}{dt} = \langle \nabla h, \mathbf{p} \rangle \quad (\dot{\mathbf{x}} = \mathbf{p})$

Singular Locus

$$\text{SL}(h) := \{ \mathbf{x} \in \mathbb{R}^n \mid \nabla h = \mathbf{0} \} = \left\{ \mathbf{x} \in \mathbb{R}^n \mid \frac{\partial h}{\partial x_1} = 0 \wedge \dots \wedge \frac{\partial h}{\partial x_n} = 0 \right\}$$

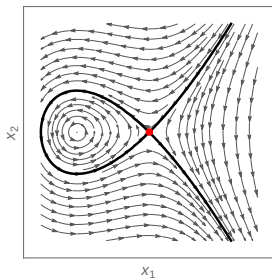
$h(\mathbf{x}) = 0$ ($\mathbf{x} \in V_{\mathbb{R}}(h)$) is **singular** if $\mathbf{x} \in \text{SL}(h)$, **regular** otherwise.

Lie's Criterion

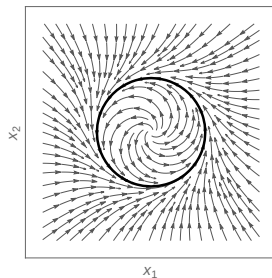
[Platzer, ITP 2012]

Necessary and sufficient for smooth invariant manifolds (Lie, 1893).

$$(\text{Lie}) \frac{h = 0 \rightarrow (\mathfrak{D}_{\mathbf{p}}(h) = 0 \wedge \nabla h \neq \mathbf{0})}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}] (h = 0)}$$



$h = 0$ non-smooth ✗



$h = 0$ smooth ✓

Extensions of Lie

Contribution

Handling certain **singularities** (points where $\nabla h = \mathbf{0}$)

No flow in the problem variables at singularities on the variety

$$(\text{Lie}^\circ) \frac{h = 0 \rightarrow (\mathfrak{D}_{\mathbf{p}}(h) = 0 \wedge (\nabla h = \mathbf{0} \rightarrow \mathbf{p} = \mathbf{0}))}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}] (h = 0)}$$

Flow at singularities on the variety is directed into the variety

$$(\text{Lie}^*) \frac{h = 0 \rightarrow (\mathfrak{D}_{\mathbf{p}}(h) = 0 \wedge (\nabla h = \mathbf{0} \rightarrow h(\mathbf{x} + \lambda \mathbf{p}) = 0))}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}] (h = 0)} .$$

Extensions of Lie

Contribution

Handling certain **singularities** (points where $\nabla h = \mathbf{0}$)

No flow in the problem variables at singularities on the variety

$$(\text{Lie}^\circ) \frac{h = 0 \rightarrow (\mathfrak{D}_{\mathbf{p}}(h) = 0 \wedge (\nabla h = \mathbf{0} \rightarrow \mathbf{p} = \mathbf{0}))}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}] (h = 0)}$$

Flow at singularities on the variety is directed into the variety

$$(\text{Lie}^*) \frac{h = 0 \rightarrow (\mathfrak{D}_{\mathbf{p}}(h) = 0 \wedge (\nabla h = \mathbf{0} \rightarrow h(\mathbf{x} + \lambda \mathbf{p}) = 0))}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}] (h = 0)} .$$

Extensions of Lie

Contribution

Handling certain **singularities** (points where $\nabla h = \mathbf{0}$)

No flow in the problem variables at singularities on the variety

$$(\text{Lie}^\circ) \frac{h = 0 \rightarrow (\mathfrak{D}_{\mathbf{p}}(h) = 0 \wedge (\nabla h = \mathbf{0} \rightarrow \mathbf{p} = \mathbf{0}))}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}] (h = 0)}$$

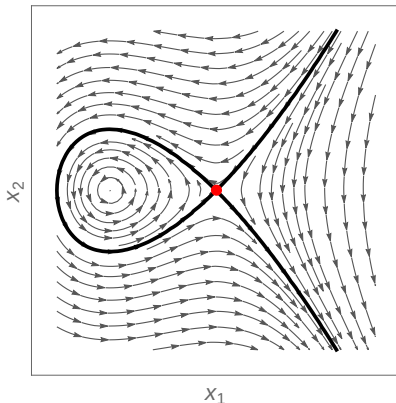
Flow at singularities on the variety is directed into the variety

$$(\text{Lie}^*) \frac{h = 0 \rightarrow (\mathfrak{D}_{\mathbf{p}}(h) = 0 \wedge (\nabla h = \mathbf{0} \rightarrow h(\mathbf{x} + \lambda \mathbf{p}) = 0))}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}] (h = 0)} .$$

Extensions of Lie: Lie^o

Contribution

Handling certain **singularities** (points where $\nabla h = \mathbf{0}$)



Lie ✗

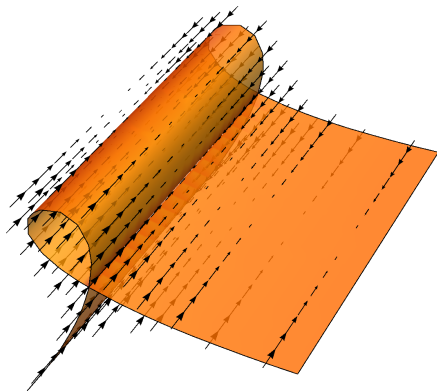
Lie^o ✓

Lie* ✓

Extensions of Lie: Lie*

Contribution

Handling certain **singularities** (points where $\nabla h = \mathbf{0}$)



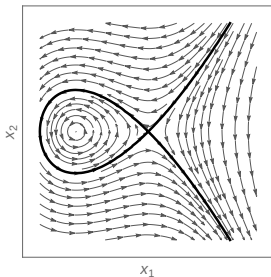
Lie ✗ Lie^o ✗ Lie* ✓

Differential Invariant ($DI_=$)

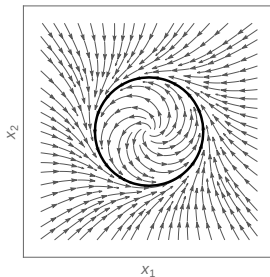
[Platzer, J. Log. Comput. 2010]

Necessary and sufficient for conserved quantities (integrals of motion).

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



h conserved ✓



h not conserved ✗

Extensions of $DI_{=}$

[Sankaranarayanan et al., FMSD 2008]

Continuous consecutions (C-c) and **polynomial consecutions** (P-c) are Darboux polynomials (Darboux, 1878).

$$(C-c) \frac{\exists \lambda \in \mathbb{R}, \mathfrak{D}_{\mathbf{p}}(h) = \lambda h}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}] (h = 0)},$$

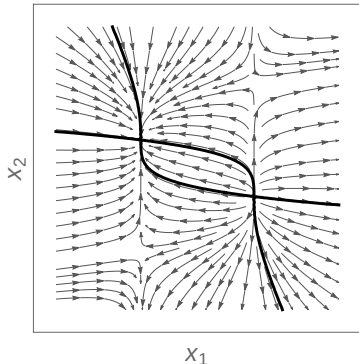
$$(P-c) \frac{\exists \lambda \in \mathbb{R}[\mathbf{x}], \mathfrak{D}_{\mathbf{p}}(h) = \lambda h}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}] (h = 0)} .$$

Extensions of $DI_=$

[Sankaranarayanan et al., FMSSD 2008]

$$\mathbf{p} = (3(x_1^2 - 4), -x_2^2 + x_1x_2 + 3), \quad h = x_2^4 + 2x_1x_2^3 + 6x_2^2 + 2x_1x_2 + x_1^2 + 3,$$

$$\mathfrak{D}_{\mathbf{p}}(h) = \underbrace{(6x_1 - 4x_2)}_{\lambda} h$$



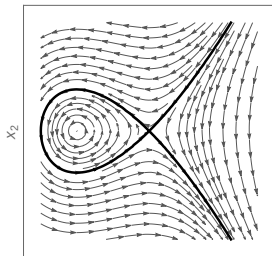
$DI_=$ ✗ $C-c$ ✗ $P-c$ ✓

Differential Radical Invariants (DRI)

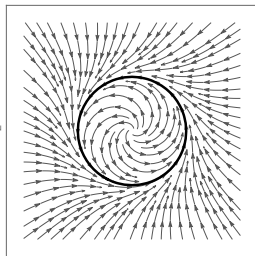
[G. et al., TACAS 2014, SAS 2014]

Necessary and sufficient for invariant varieties.

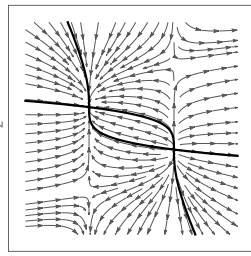
$$\text{(DRI)} \frac{h = 0 \rightarrow \bigwedge_{i=0}^{N-1} \mathfrak{D}_{\mathbf{p}}^{(i)}(h) = 0}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}] (h = 0)}$$



x_1



x_1



x_1



How to compare these different proof rules ?

$$\{DI=, C-c, P-c, Lie, Lie^{\circ}, Lie^{*}, DRI\}$$

For some classes of problems, the premises of the proof rules lead to *decision procedures*.

Natural questions:

- Given two decision procedures, which is more practical?
- Are any of these proof rules redundant?

To answer these, we perform

- Theoretical comparison
- Empirical performance analysis

How to compare these different proof rules ?

$$\{DI=, C-c, P-c, Lie, Lie^{\circ}, Lie^*, DRI\}$$

For some classes of problems, the premises of the proof rules lead to *decision procedures*.

Natural questions:

- Given two decision procedures, which is more practical?
- Are any of these proof rules redundant?

To answer these, we perform

- Theoretical comparison
- Empirical performance analysis

How to compare these different proof rules ?

$$\{DI=, C-c, P-c, Lie, Lie^{\circ}, Lie^{*}, DRI\}$$

For some classes of problems, the premises of the proof rules lead to *decision procedures*.

Natural questions:

- Given two decision procedures, which is more practical?
- Are any of these proof rules redundant?

To answer these, we perform

- Theoretical comparison
- Empirical performance analysis

How to compare these different proof rules ?

$$\{DI=, C-c, P-c, Lie, Lie^{\circ}, Lie^*, DRI\}$$

For some classes of problems, the premises of the proof rules lead to *decision procedures*.

Natural questions:

- Given two decision procedures, which is more practical?
- Are any of these proof rules redundant?

To answer these, we perform

- Theoretical comparison
- Empirical performance analysis

Outline

- 1 Introduction
- 2 Proof rules
- 3 Deductive Hierarchy**
- 4 Practical performance analysis
- 5 Square-free Reduction
- 6 Conclusion

Order Relation

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

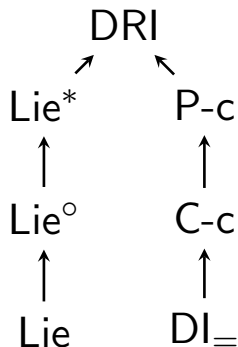
$$(R_B) \frac{B}{(h=0) \longrightarrow [\dot{\mathbf{x}} = \mathbf{p}](h=0)}$$

Partial Order

$R_A \preceq R_B$ if and only if $A \implies B$.

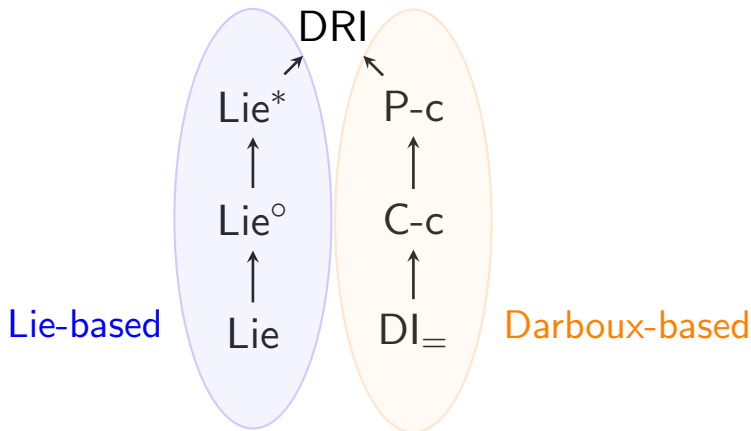
- $R_A \sim R_B$ ($R_A \preceq R_B$ and $R_A \succeq R_B$) **Equivalence.**
- $R_A \prec R_B$ ($R_A \preceq R_B$ and $R_A \not\succeq R_B$) **Strict increase** of deductive power

Hasse Diagram: Deductive Hierarchy



- $R_A \rightarrow R_B$ means everything proved by R_A can be proved by R_B .
- **no link** means R_A and R_B are **incomparable**.

Hasse Diagram: Deductive Hierarchy



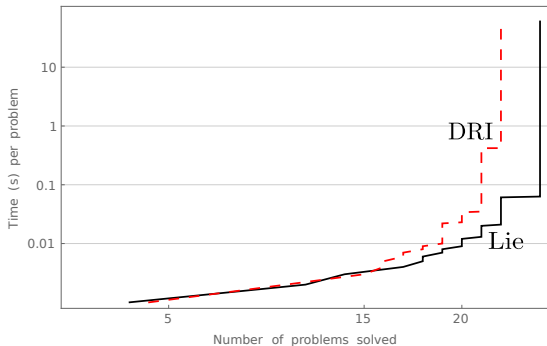
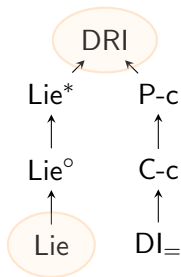
- $R_A \rightarrow R_B$ means everything proved by R_A can be proved by R_B .
- **no link** means R_A and R_B are **incomparable**.

Outline

- 1 Introduction
- 2 Proof rules
- 3 Deductive Hierarchy
- 4 Practical performance analysis**
- 5 Square-free Reduction
- 6 Conclusion

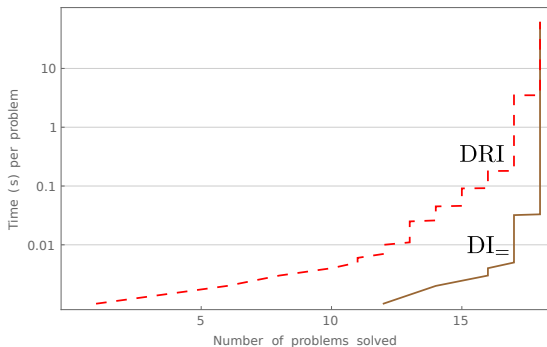
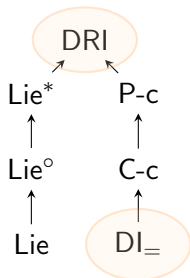
Smooth invariant manifolds (Lie vs DRI)

Lie and DRI **decide** invariance for **smooth invariant manifolds**.



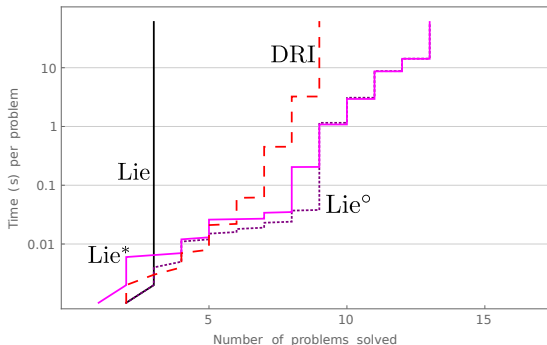
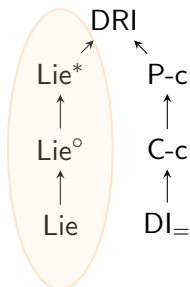
Functional invariants (DI vs DRI)

DI₌ and DRI **decide** invariance of varieties of **conserved quantities**.

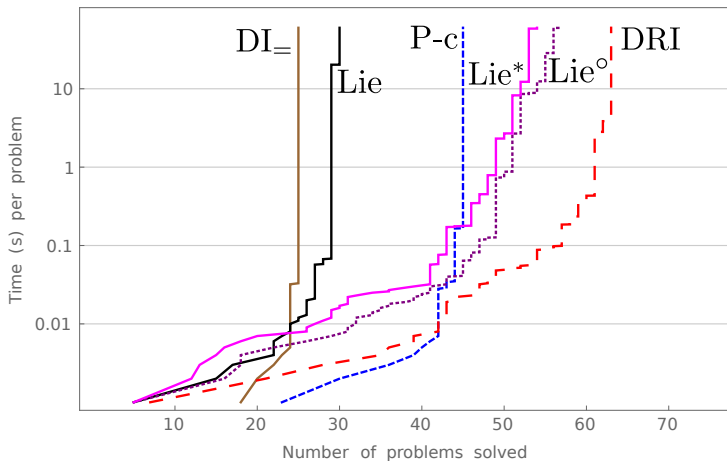


Singularities at Equilibria (Lie , Lie° & Lie^* vs DRI)

Lie° , Lie^* and DRI **decide** invariance for varieties of with **singularities** that are **equilibrium points**.



Experimental Performance of All Proof Rules



Outline

- 1 Introduction
- 2 Proof rules
- 3 Deductive Hierarchy
- 4 Practical performance analysis
- 5 Square-free Reduction**
- 6 Conclusion

Square-free Reduction

Square-free reduction of a polynomial

$$h = h_1^{\alpha_1} h_2^{\alpha_2} \dots h_k^{\alpha_k}$$

Geometrically $V_{\mathbb{R}}(h) \equiv_{\mathbb{R}} V_{\mathbb{R}}(\text{SF}(h))$.

- SF **automated pre-processing** step in **computer algebra** systems
- Is it a “good idea” to apply SF for invariance checking ?

Square-free Reduction

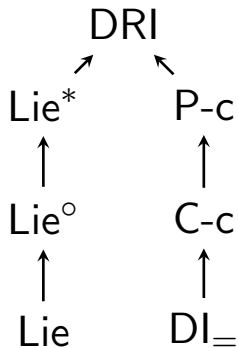
Square-free reduction of a polynomial

$$\text{SF}(h) = h_1^{\cancel{q_1}} h_2^{\cancel{q_2}} \dots h_k^{\cancel{q_k}}$$

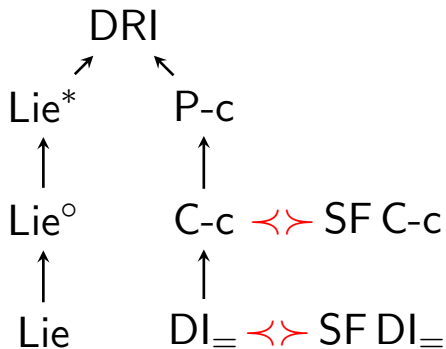
Geometrically $V_{\mathbb{R}}(h) \equiv_{\mathbb{R}} V_{\mathbb{R}}(\text{SF}(h))$.

- SF **automated pre-processing** step in **computer algebra** systems
- Is it a “good idea” to apply SF for invariance checking ?

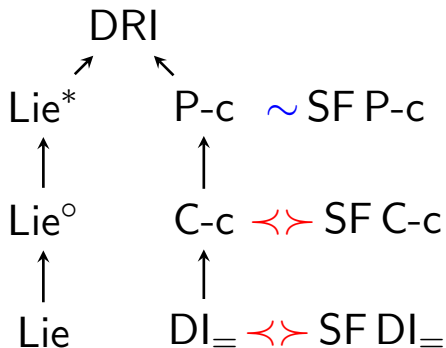
Square-free Reduction



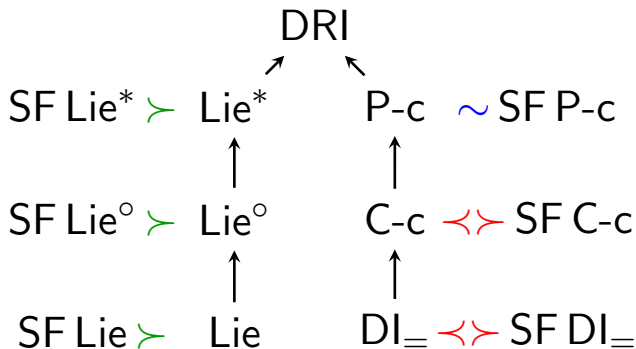
Square-free Reduction



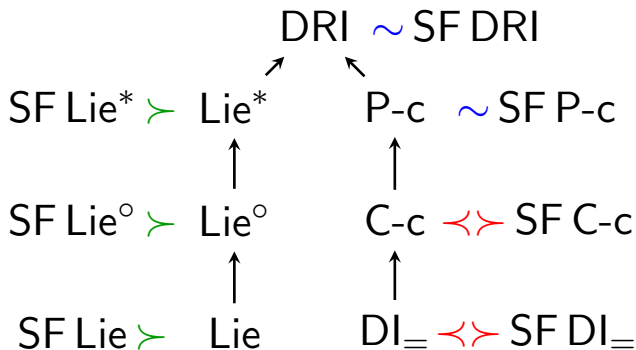
Square-free Reduction



Square-free Reduction



Square-free Reduction



Summary

- The **most deductively powerful** rule DRI **performs very well**.
- C-c and P-c are made **redundant** by DRI.
- SF reduction is always of **benefit** to the Lie-**based** proof rules
- SF with $DI_{=}$ and C-c yields new **incomparable** proof rules.
- SF with P-c is **as powerful as** P-c alone.
- SF may introduce a **performance penalty** for DRI.

Conclusions

DRI has good performance on average

Apply DRI first with a time-out.

Sufficient proof rules are useful

Exploit the computational sweet spots of sufficient conditions

Thank you for attending !