# Formal Verification and Automated Generation of Invariant Sets

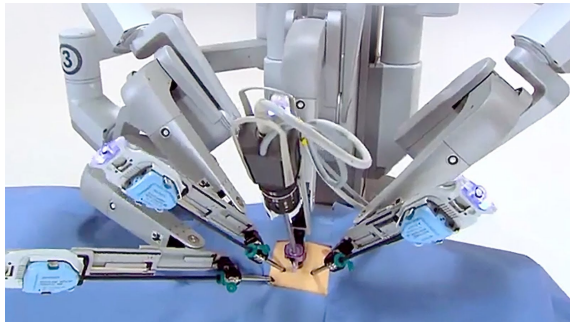
**Khalil Ghorbal**

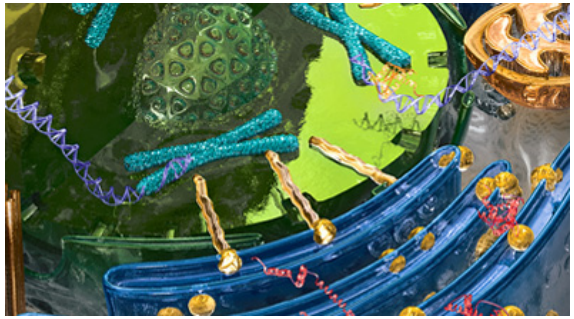
Carnegie Mellon University

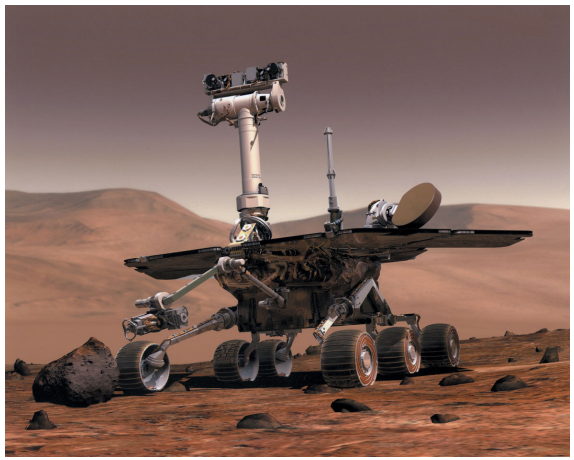
Joint work with **Andrew Sogokon** and **André Platzer**

Toulouse, France
11-12 June, 2015

# Cyber-Physical Systems







Init

$\longrightarrow$

[

(

Sensing: read data from sensors

Control: actuate

Plant: evolve ◀ ◀ ◀ ◀ ◀

)*

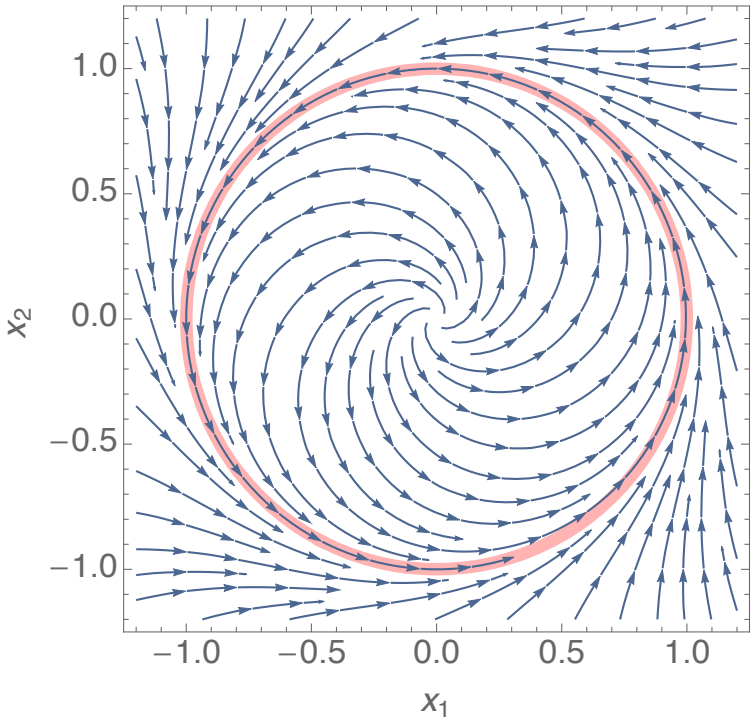
]

Safety

## Evolution

- Continuous time
- Ordinary Differential Equations (ODE)

$$(\dot{x_1}, \dot{x_2}) = (x_1 - x_1^3 - x_2 - x_1 x_2^2, x_1 + x_2 - x_1^2 x_2 - x_2^3)$$




**Algebraic Invariant Equation**

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

# Why Are Invariants Important ?

## Numerical Integration & Qualitative Analysis

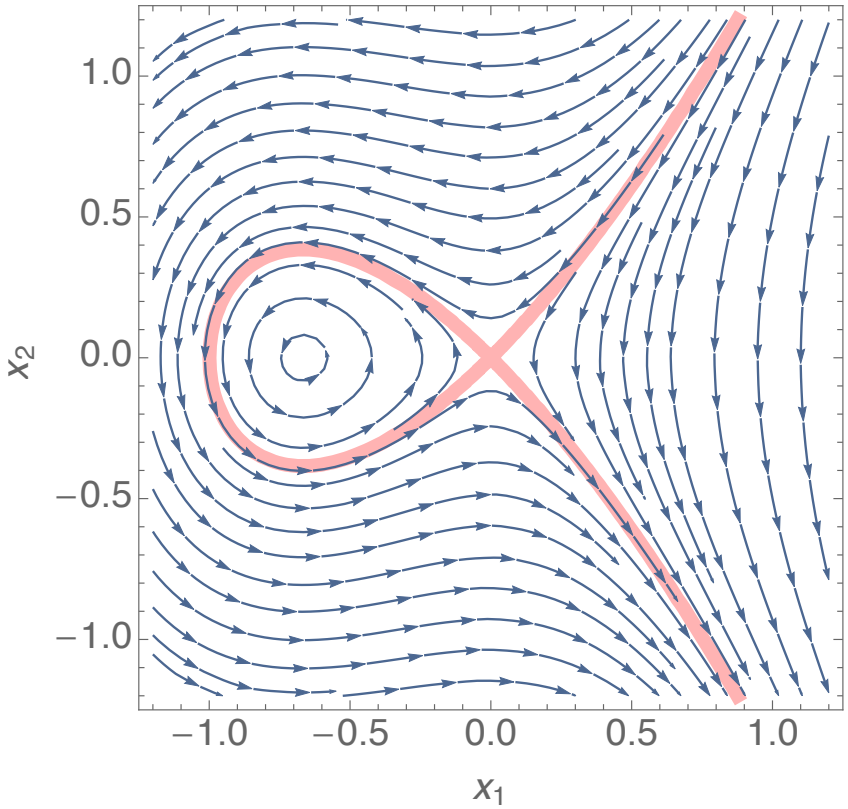
- More precise numerical integration (Geometrical Integration)
- Better understanding of the dynamics without solving the problem (some invariants represent conserved quantities like momentum or energy)

## Formal Verification

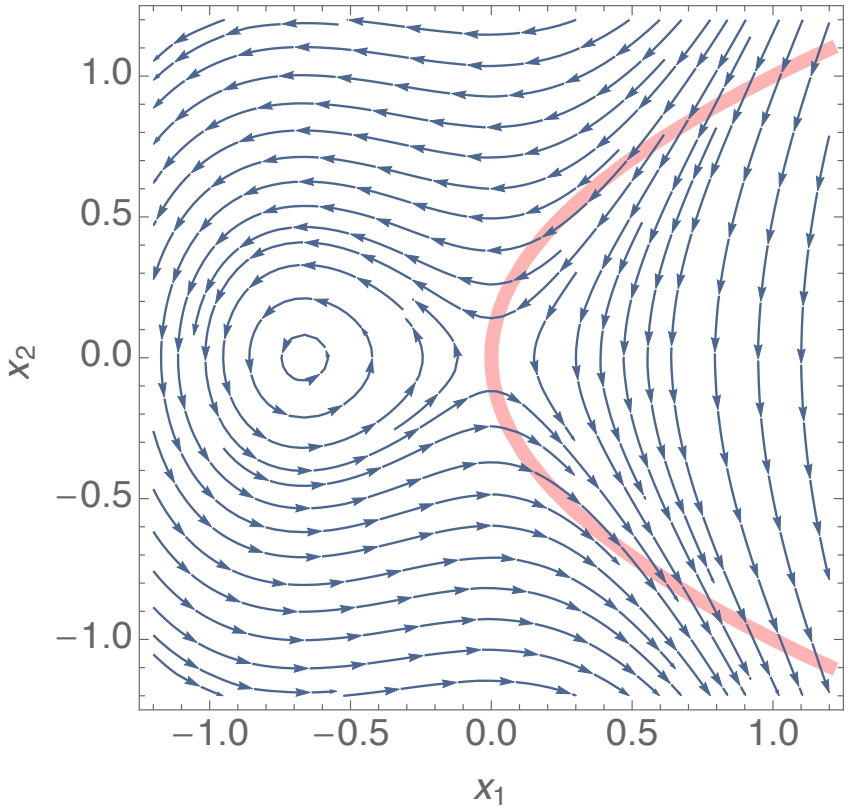
- Formal verification for dynamical and hybrid systems
- Static Analysis (as templates to statically analyze an implementation)
- Safety, Reachability, Stability

# Problem I. *Checking Invariance of Algebraic Equations*

Given $\dot{\mathbf{x}} = (-2x_2, -2x_1 - 3x_1^2)$, $p(\mathbf{x}_0) = 0$, is $p(\mathbf{x}(t)) = 0$ for all $t$ ?



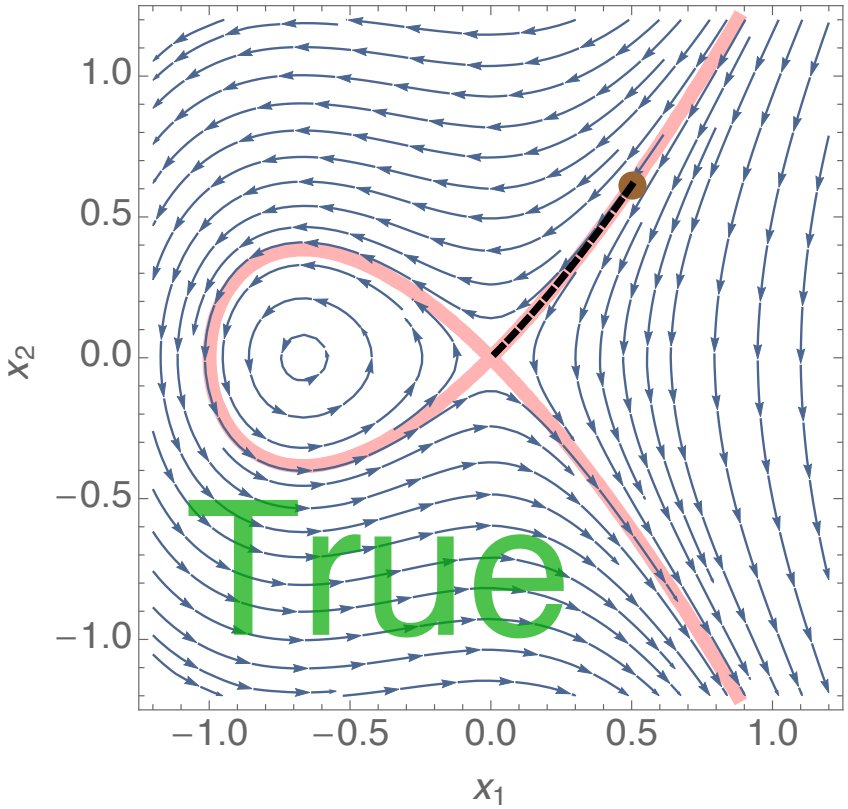

$$p(x_1, x_2) = x_1^2 + x_1^3 - x_2^2$$



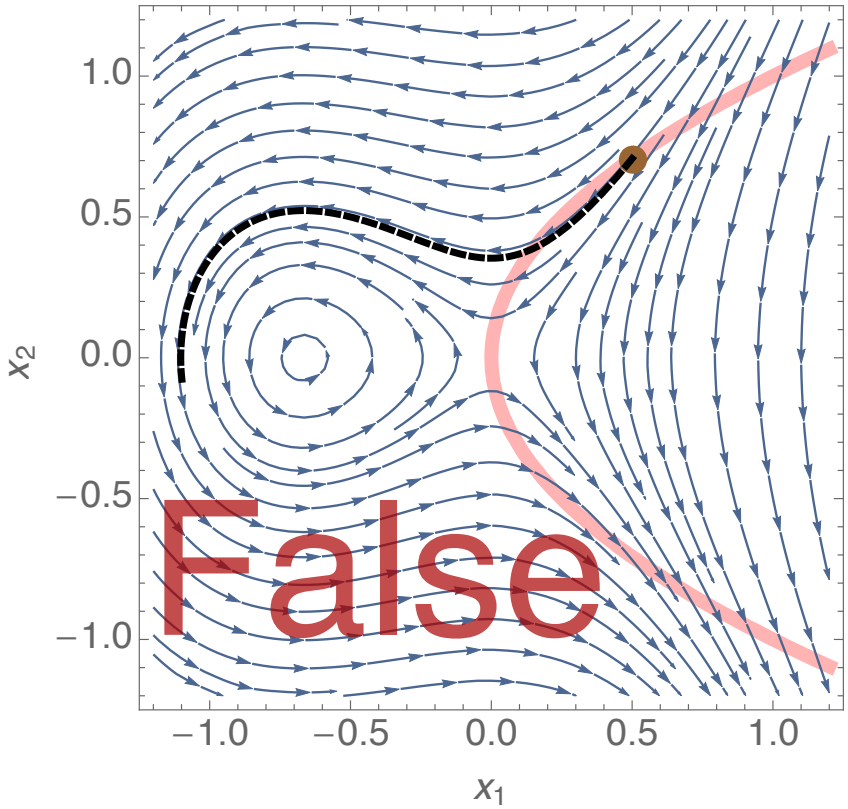

$$p(x_1, x_2) = x_1 - x_2^2$$

# Problem I. *Checking Invariance of Algebraic Equations*

Given $\dot{\mathbf{x}} = (-2x_2, -2x_1 - 3x_1^2)$, $p(\mathbf{x}_0) = 0$, is $p(\mathbf{x}(t)) = 0$ for all $t$ ?



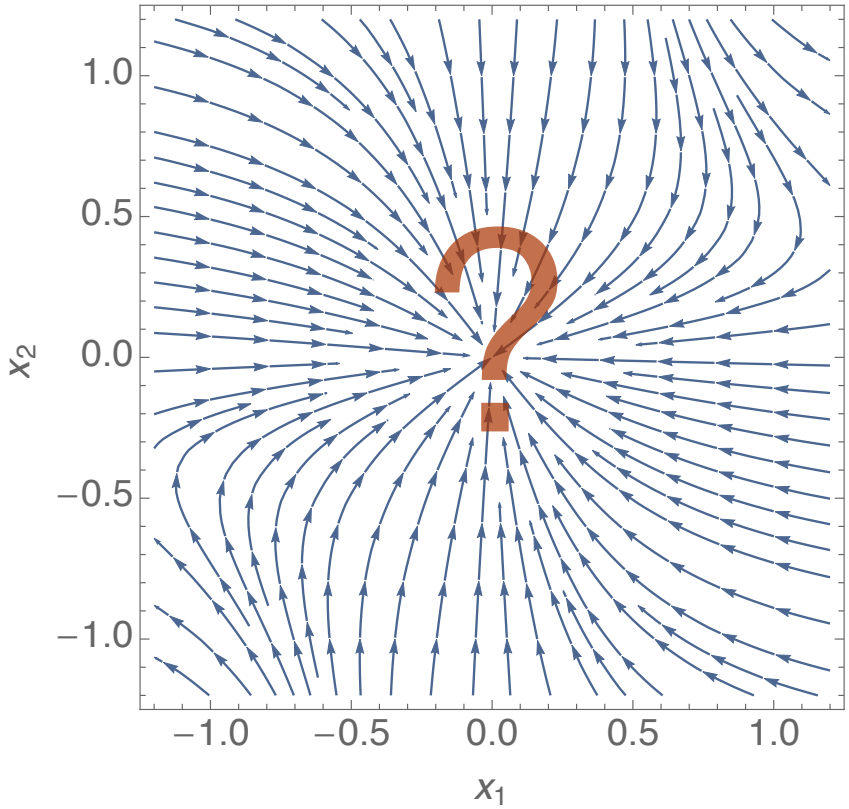

$$p(x_1, x_2) = x_1^2 + x_1^3 - x_2^2$$




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

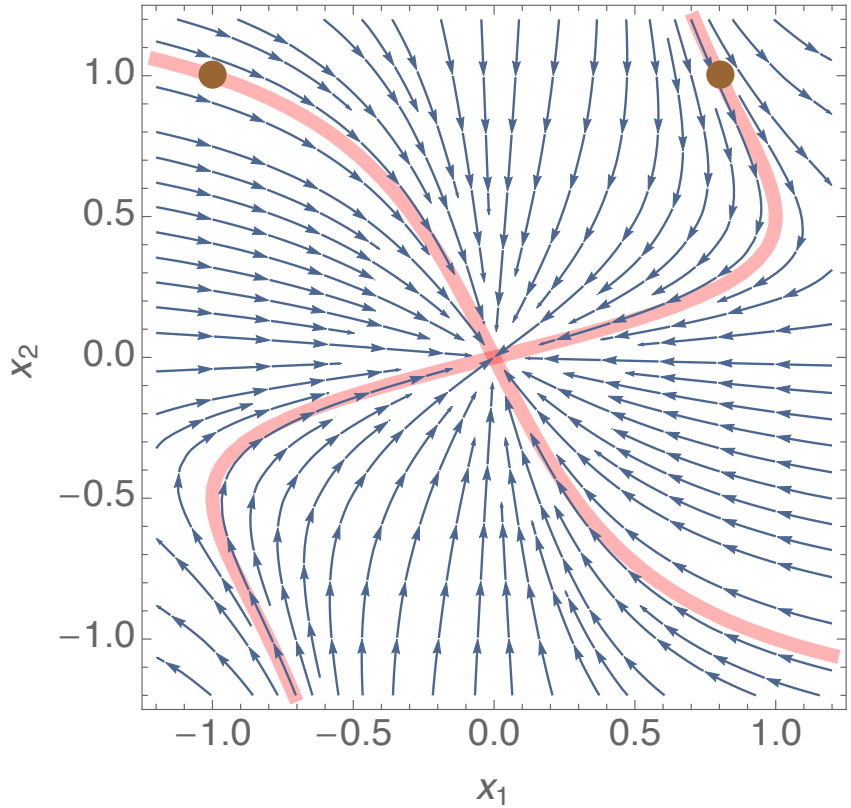
# Problem II. *Generate Algebraic Invariant Equations*

Given $\dot{\mathbf{x}} = (-x_1 + 2x_1^2 x_2, -x_2)$, how to generate $p$ such that $p(\mathbf{x}(t)) = 0$ ?



# Problem II. *Generate Algebraic Invariant Equations*

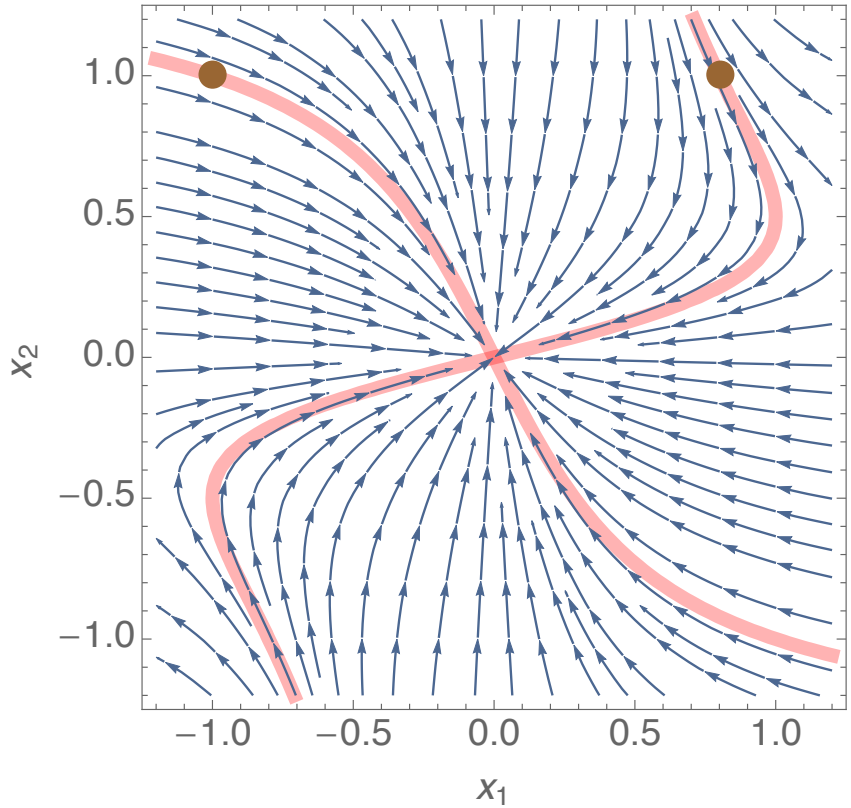
Given $\dot{\mathbf{x}} = (-x_1 + 2x_1^2 x_2, -x_2)$, how to generate $p$ such that $p(\mathbf{x}(t)) = 0$ ?




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

# Problem II. *Generate Algebraic Invariant Equations*

Given $\dot{\mathbf{x}} = (-x_1 + 2x_1^2 x_2, -x_2)$, how to generate $p$ such that $p(\mathbf{x}(t)) = 0$ ?




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

$\frac{x_1}{x_2 - x_1 x_2^2}$ is an invariant **rational function**.

**Gradient** $\nabla p := (\frac{\partial p}{\partial x_1}, \ldots, \frac{\partial p}{\partial x_n})$

**Lie Derivation** $\mathfrak{D}_{\mathbf{f}}(p) := \frac{dp(\mathbf{x}(t))}{dt} = \langle \nabla p, \mathbf{f} \rangle \qquad (\dot{\mathbf{x}} = \mathbf{f})$

**Singular Locus**

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

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

# Outline


1. Context
2. The Checking Problem
3. The Generation Problem
4. Future Avenues

# Notation for "$S \subseteq \mathbb{R}^n$ is invariant for $\mathbf{f}$"

$$S \rightarrow [\dot{\mathbf{x}} = \mathbf{f}]S$$

$$\equiv$$

The set $S$ is an invariant set for $\mathbf{f}$

$$\equiv$$

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

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

# Notation for "$S \subseteq \mathbb{R}^n$ is invariant for $\mathbf{f}$"

$$S \rightarrow [\dot{\mathbf{x}} = \mathbf{f}]S$$

$$\equiv$$

The set $S$ is an invariant set for $\mathbf{f}$

$$\equiv$$

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

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

# Notation for "$S \subseteq \mathbb{R}^n$ is invariant for $\mathbf{f}$"

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

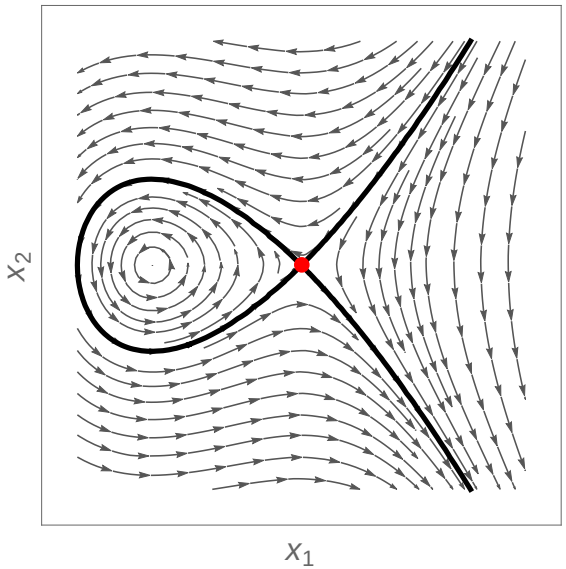
N.B. Treating $\dot{\mathbf{x}} = \mathbf{f}$ as a program, one can think of the top formula as representing the Hoare triple $\{S\}\ \dot{\mathbf{x}} = \mathbf{f}\ \{S\}$.

# Lie's Criterion

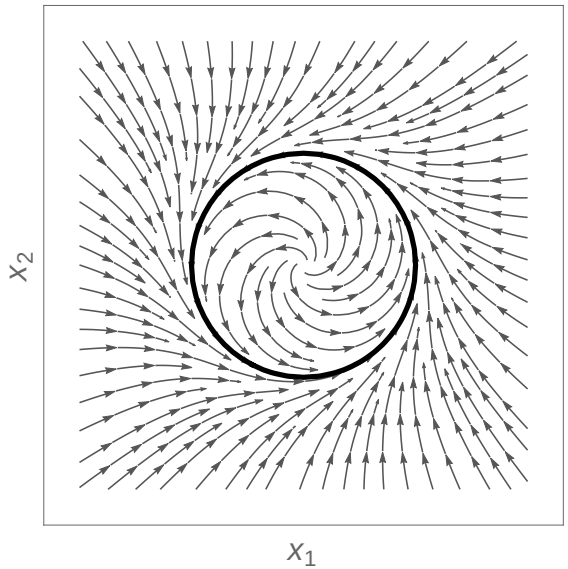
[Platzer, ITP 2012]

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

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




$p = 0$ non-smooth ✗




$p = 0$ smooth ✓

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

No flow in the problem variables at singularities on the variety

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

Flow at singularities on the variety is directed into the variety

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

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

No flow in the problem variables at singularities on the variety

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

Flow at singularities on the variety is directed into the variety

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

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

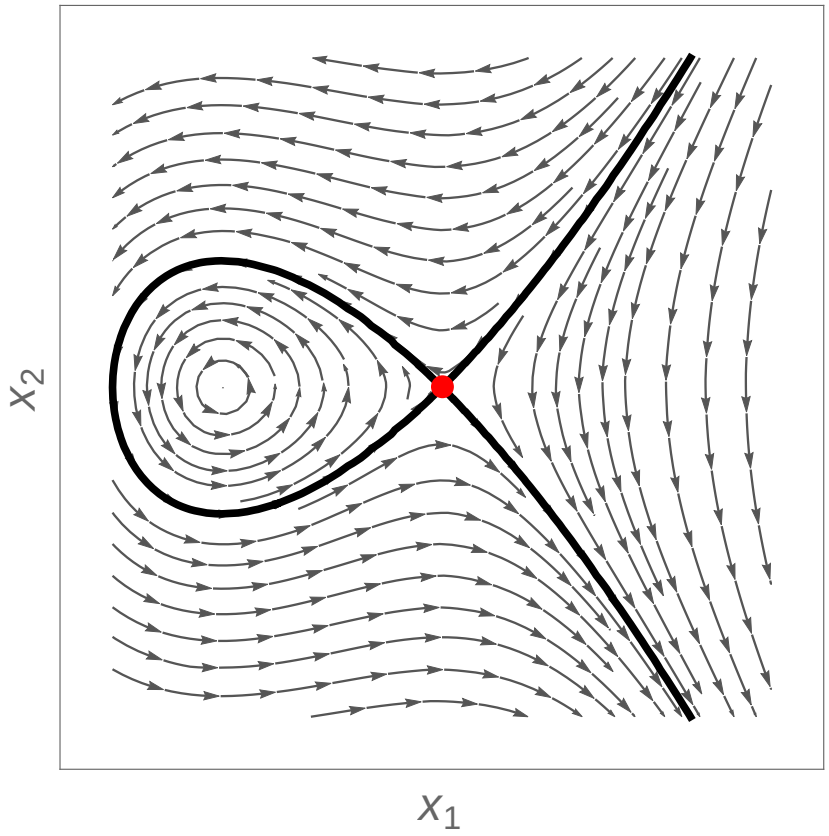
No flow in the problem variables at singularities on the variety

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

Flow at singularities on the variety is directed into the variety

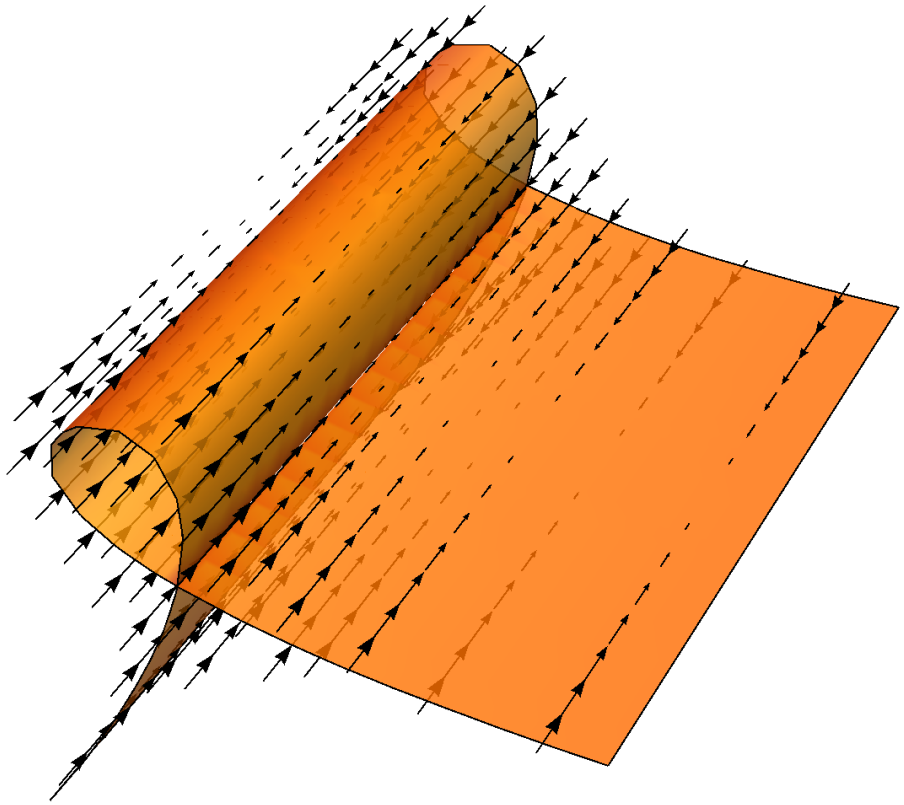
$$(\text{Lie}^{*})\frac{p = 0 \rightarrow \left(\mathfrak{D}_{\mathbf{f}}(p) = 0 \wedge (\nabla p = \mathbf{0} \rightarrow p(\mathbf{x} + \lambda \mathbf{f}) = 0)\right)}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}]\ (p = 0)}\ .$$

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




Lie ✗ Lie° ✓ Lie* ✓

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



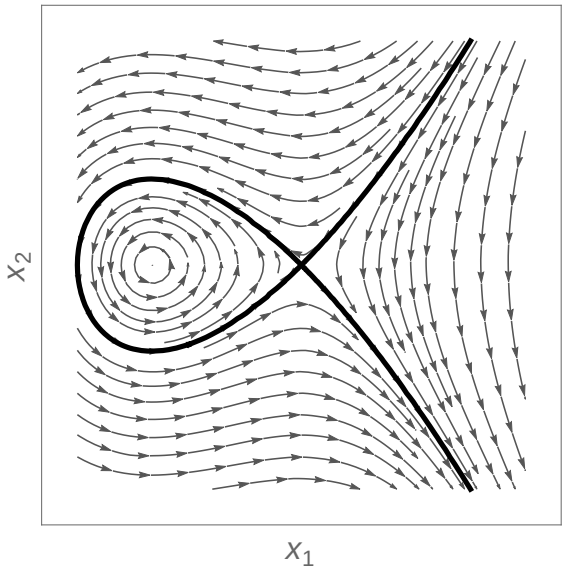
Lie ✗ Lie° ✗ Lie* ✓

# First Integral (FI)

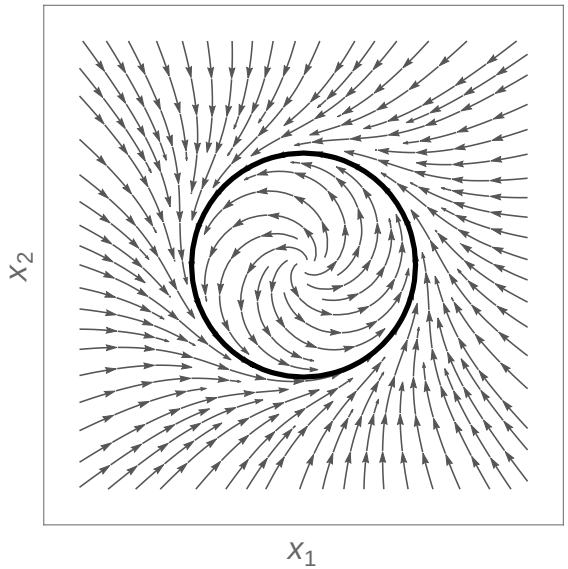
[Platzer, J. Log. Comput. 2010]

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

$$(\mathsf{FI})\frac{\mathfrak{D}_{\mathbf{f}}(p)=0}{(p=0)\rightarrow[\dot{\mathbf{x}}=\mathbf{f}]\ (p=0)}$$




$p$ conserved ✓




$p$ not conserved ✗

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

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

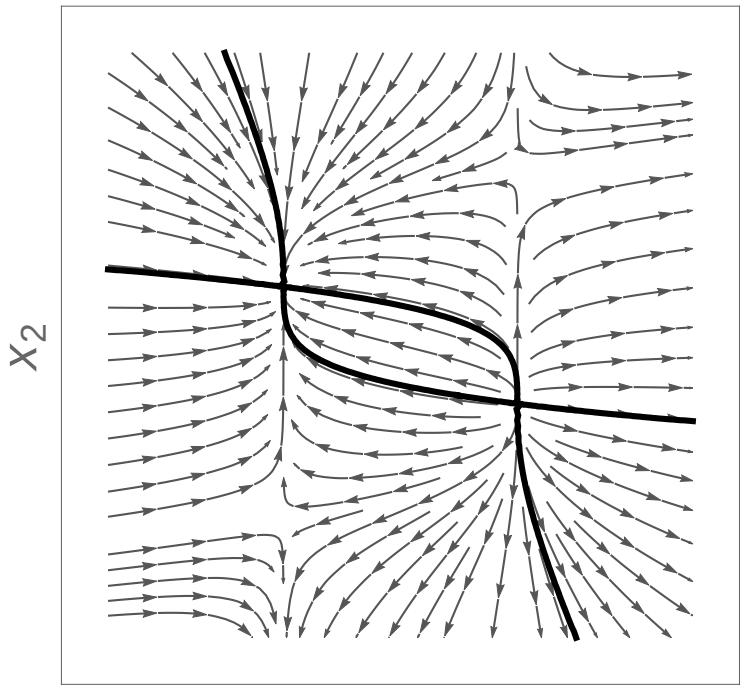
$$\text{(P-c)}\frac{\exists \lambda \in \mathbb{R}[\mathbf{x}],\ \mathfrak{D}_{\mathbf{f}}(p) = \lambda p}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}]\ (p = 0)}\ .$$

# Extensions of FI

[Sankaranarayanan et al., FMSD 2008]

$$\mathbf{f} = (3\left(x_1^2 - 4\right), -x_2^2 + x_1 x_2 + 3), \qquad p = x_2^4 + 2x_1 x_2^3 + 6x_2^2 + 2x_1 x_2 + x_1^2 + 3,$$

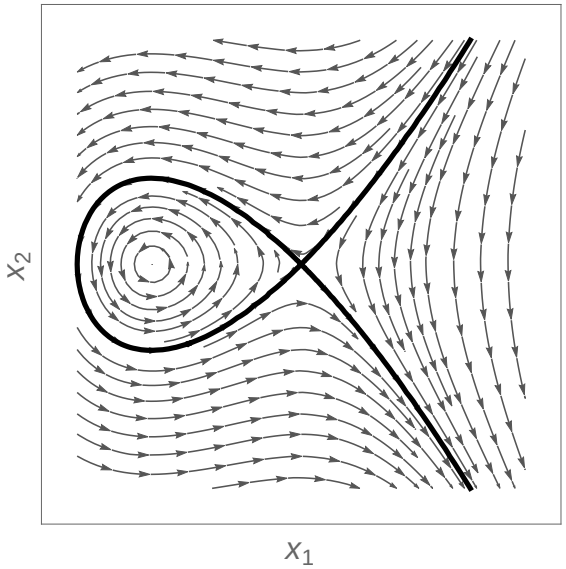
$$\mathfrak{D}_{\mathbf{f}}(p) = \underbrace{(6x_1 - 4x_2)}_{\lambda} p$$



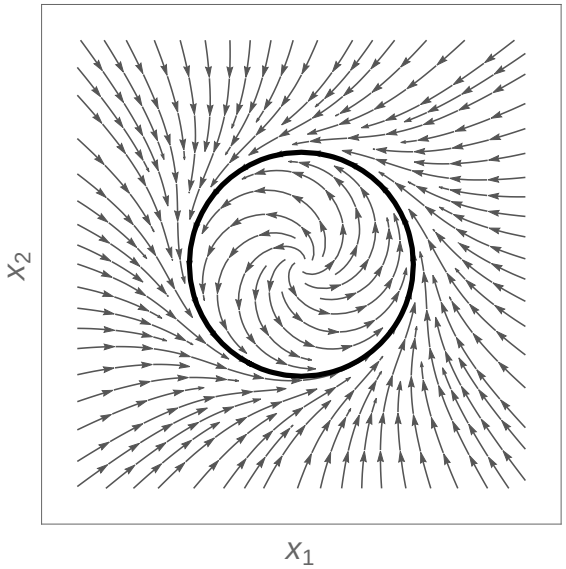

FI ✗ C-c ✗ P-c ✓

**Necessary and sufficient** for invariant varieties.

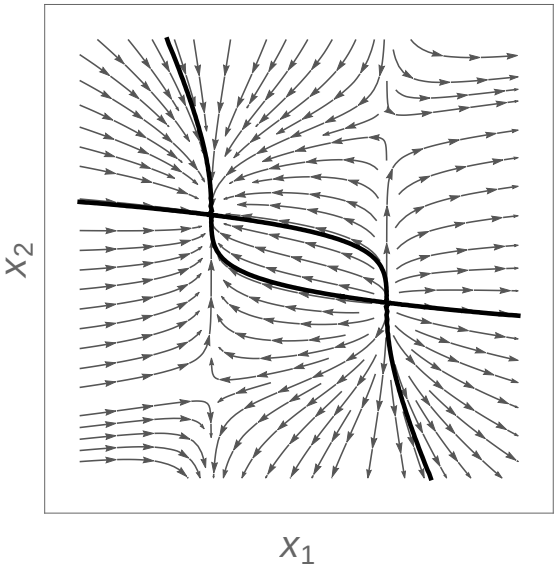
$$(\text{DRI})\frac{p = 0 \rightarrow \bigwedge_{i=0}^{N-1} \mathfrak{D}_{\mathbf{f}}^{(i)}(p) = 0}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}]\ (p = 0)}$$




✓




✓



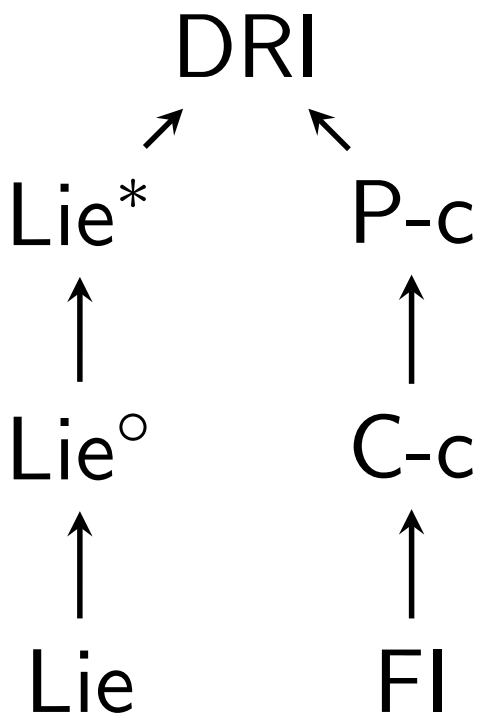

✓

$$(\mathrm{R}_A)\frac{A}{S_A : T_A \longrightarrow [\dot{\mathbf{x}} = \mathbf{f}]S_A : T_A} \qquad (\mathrm{R}_B)\frac{B}{S_B : T_B \longrightarrow [\dot{\mathbf{x}} = \mathbf{f}]S_B : T_B}$$

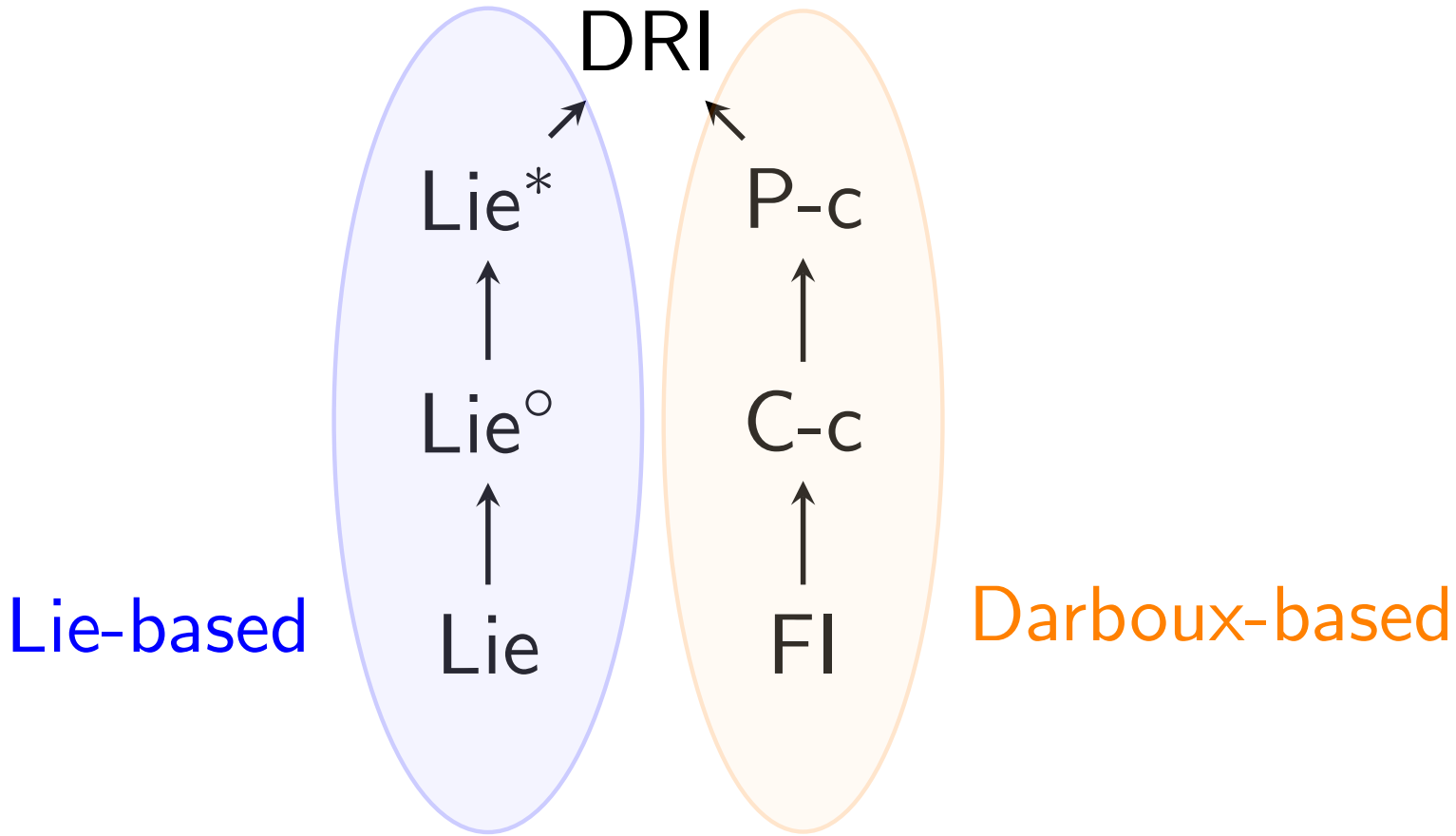
## Partial Order

$\mathrm{R}_A \preccurlyeq \mathrm{R}_B$ if and only if $A \implies B$ and $T_A$ is a "subtype" of $T_B$ .

- $\mathrm{R}_A \sim \mathrm{R}_B$ ($\mathrm{R}_A \preccurlyeq \mathrm{R}_B$ and $\mathrm{R}_A \succcurlyeq \mathrm{R}_B$) **Equivalence**.
- $\mathrm{R}_A \prec \mathrm{R}_B$ ($\mathrm{R}_A \preccurlyeq \mathrm{R}_B$ and $\mathrm{R}_A \not\succcurlyeq \mathrm{R}_B$) **Strict increase** of deductive power




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




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

*Square-free reduction* of a polynomial

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

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

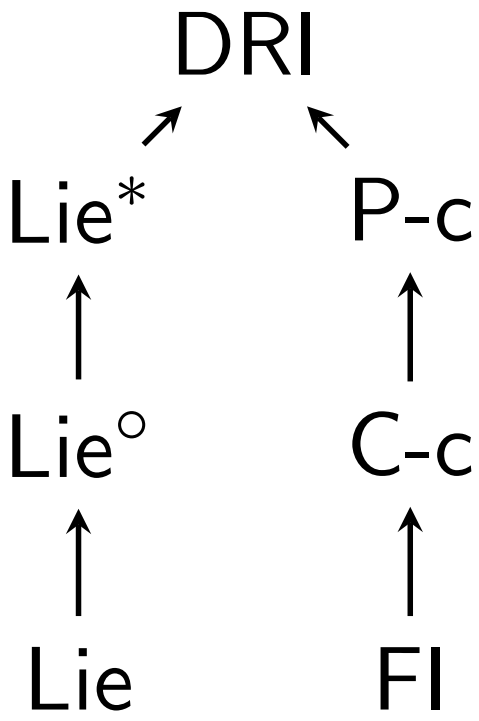
- SF **automated pre-processing** step in **computer algebra** systems
- Is it a "good idea" to apply SF for invariance checking ?

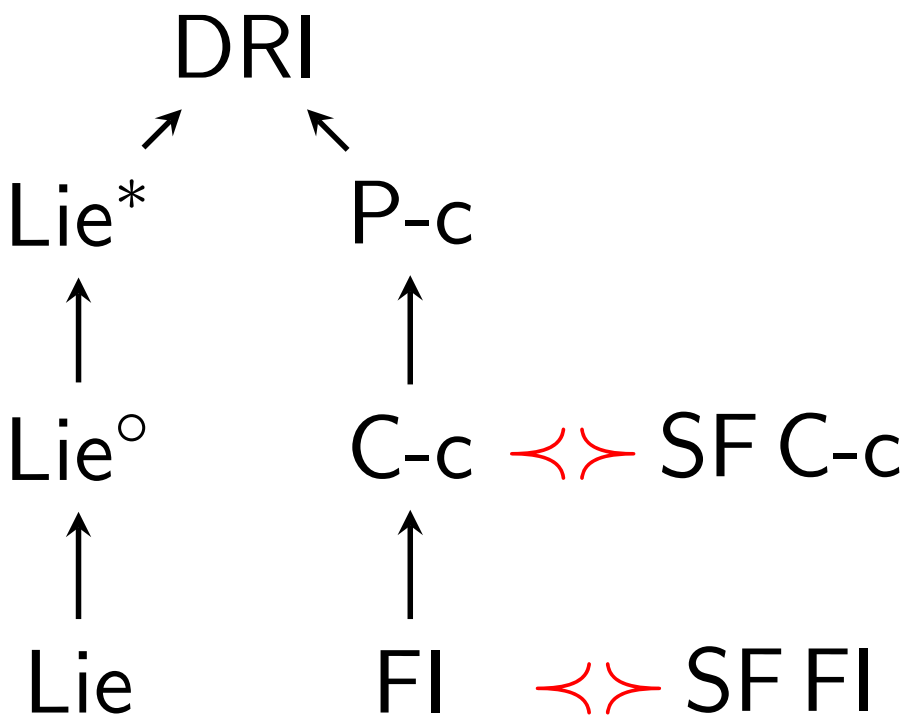
*Square-free reduction* of a polynomial

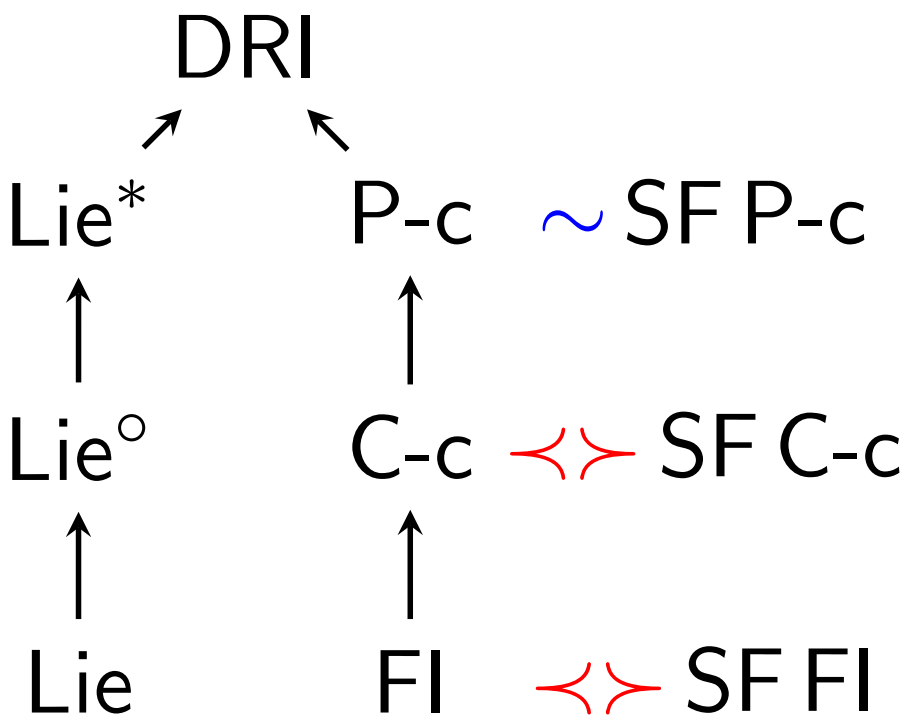
$$\mathrm{SF}(h) = h_1^{\alpha_1} h_2^{\alpha_2} \cdots h_k^{\alpha_k}$$

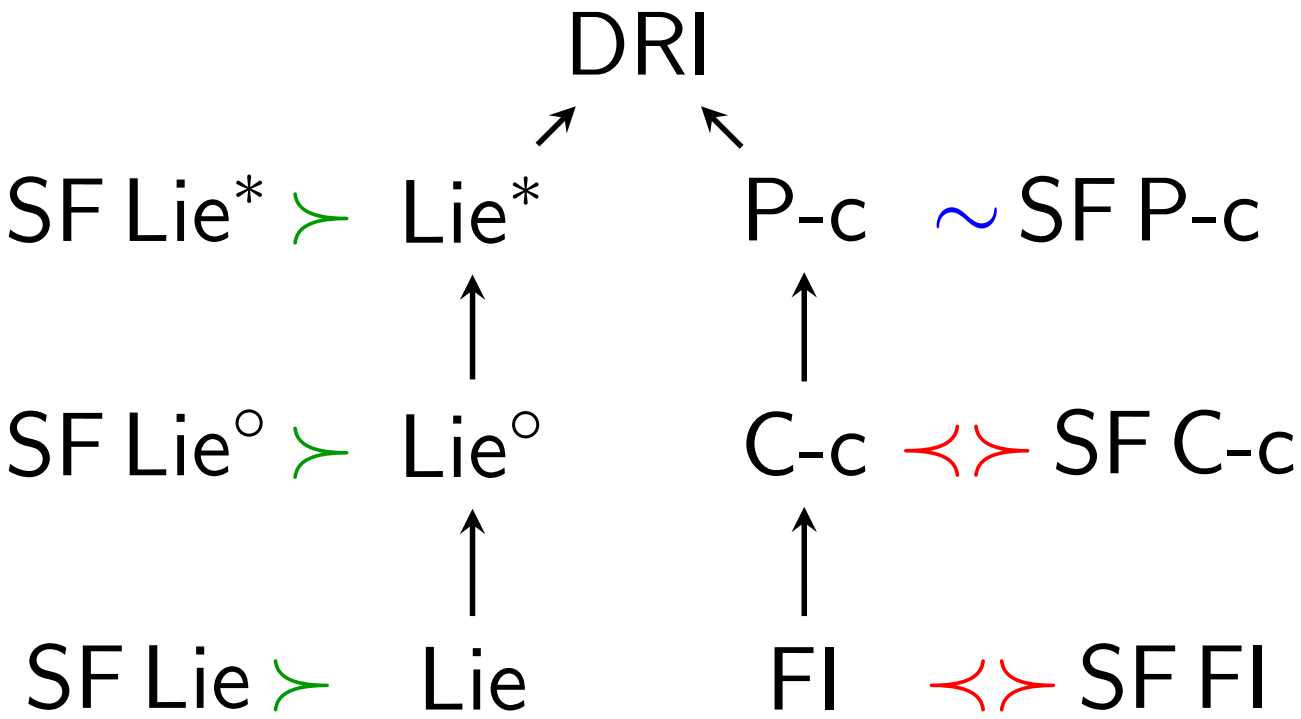
Geometrically $V_{\mathbb{R}}(h) \equiv_{\mathbb{R}} V_{\mathbb{R}}(\mathrm{SF}(h))$.

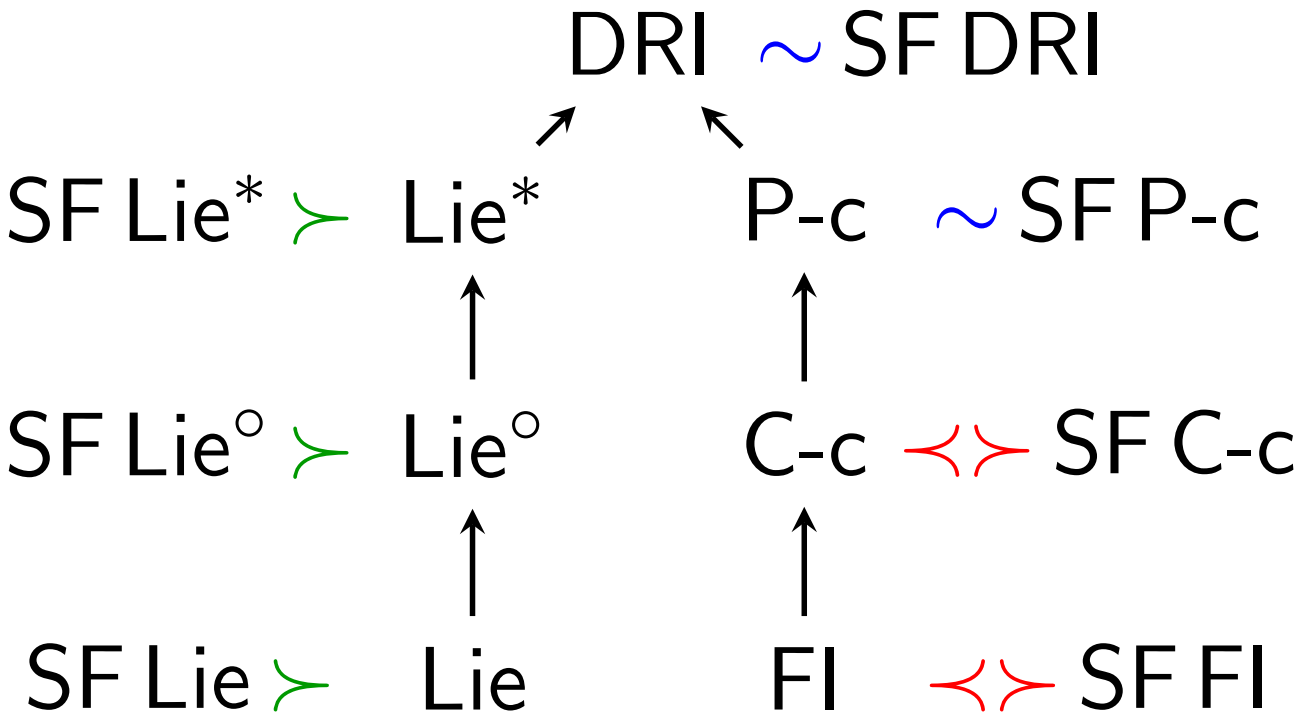
- SF **automated pre-processing** step in **computer algebra** systems
- Is it a "good idea" to apply SF for invariance checking ?


DRI
Lie*
P-c
Lie°
C-c
Lie
FI


DRI
Lie*
P-c
Lie°
C-c
SF C-c
Lie
FI
SF FI


DRI
Lie*
P-c
∼ SF P-c
Lie°
C-c
≺≻ SF C-c
Lie
FI
≺≻ SF FI


DRI
SF Lie*
Lie*
P-c
SF P-c
SF Lie°
Lie°
C-c
SF C-c
SF Lie
Lie
FI
SF FI


DRI ∼ SF DRI
SF Lie* ≻ Lie*
P-c ∼ SF P-c
SF Lie° ≻ Lie°
C-c ≺≻ SF C-c
SF Lie ≻ Lie
FI ≺≻ SF FI

So far we have only seen **algebraic** sets: $p = 0$

- For $\wedge_i p_i = 0$, we can rewrite using $\sum_i p_i^2 = 0$
- We can do better [SAS'14]

What about **semi-algebraic** sets:

- Sets of the form $p \leq 0$
- Closed Sets
- Arbitrary Sets: boolean formulae with polynomial equalities and inequalities

## Sub-tangent Vector

A vector $\mathbf{v} \in \mathbb{R}^n$ is sub-tangential to a set $S \subseteq \mathbb{R}^n$ at $\mathbf{x} \in S$ if

$$\liminf_{\lambda \to 0^+} \frac{\text{dist}\,(S, \mathbf{x} + \lambda \mathbf{v})}{\lambda} = 0. \quad (\text{dist}(S, \mathbf{x}) \equiv \inf_{\mathbf{y} \in S} \|\mathbf{x} - \mathbf{y}\|_1)$$

## Contingent Cone

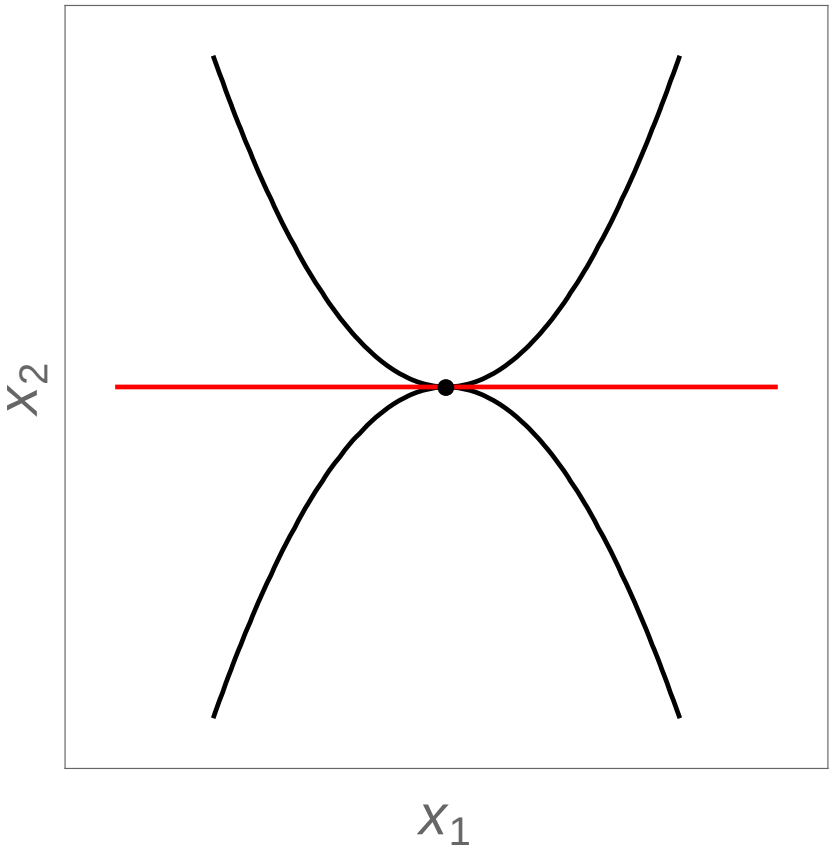
$K_{\mathbf{x}}(S)$: the set of all sub-tangent vectors to a set $S$ at $\mathbf{x} \in S$.

## Nagumo's Theorem

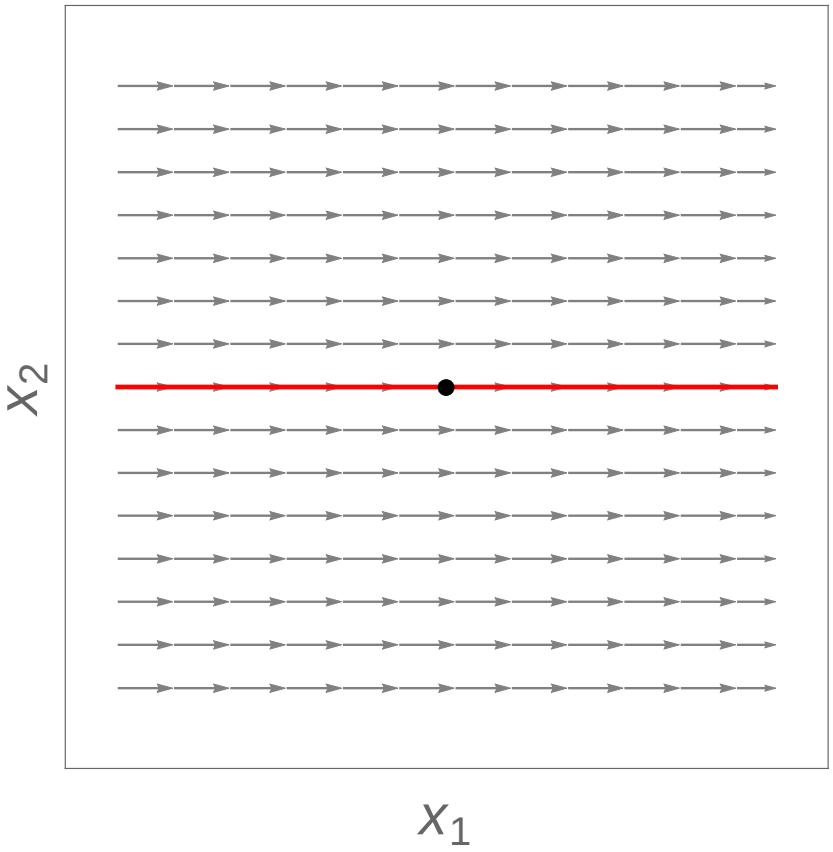
A **closed** set $S \subset \mathbb{R}^n$ is **positively invariant** under the flow of the system if and only if $\mathbf{f}(\mathbf{x}) \in K_{\mathbf{x}}(S)$ for all $\mathbf{x} \in \text{bdr}(S)$ (boundary of $S$).

# Contingent Cone of Boolean Formulae

$K_x(S_1) \cap K_x(S_2) \supset K_x(S_1 \cap S_2)$




$$x_2 + x_1^2 = 0 \wedge x_2 - x_1^2 = 0$$




$$\dot{x}_1 = 1, \dot{x}_2 = 0$$

## (Non-strict) Barrier Certificate ✓

$$(\forall \mathbf{x} \in \mathbb{R}^n, \mathfrak{D}_{\mathbf{f}}(p) \leq 0) \longrightarrow p \leq 0 \text{ is a positive invariant}$$

## Unsound Barrier Certificate ✗

$$(\forall \mathbf{x}\, s.t.\, \mathbf{p(x) = 0}, \mathfrak{D}_{\mathbf{f}}(p) \leq 0) \longrightarrow p \leq 0 \text{ is a positive invariant}$$

## **Strict** Barrier Certificate ✓

$$(\forall \mathbf{x}\, s.t.\, p(\mathbf{x}) = 0, \mathfrak{D}_{\mathbf{f}}(\mathbf{p}) < \mathbf{0}) \longrightarrow p \leq 0 \text{ is a positive invariant}$$

## Differential Invariants (DI)

$$(\mathrm{DI})\frac{D(S)^{\mathbf{f}}_{\dot{\mathbf{x}}}}{S \to [\dot{\mathbf{x}} = \mathbf{f}]\ S},$$

$D(S)^{\mathbf{f}}_{\dot{\mathbf{x}}}$: substitute each $\dot{\mathbf{x}}_i$ in $D(S)$ with $\mathbf{f}_i(\mathbf{x})$

$$\begin{aligned}
D(r) &= 0 \quad \text{for numbers,}\\
D(x) &= \dot{x} \quad \text{for variables,}\\
D(a+b) &= D(a) + D(b),\\
D(a \cdot b) &= D(a) \cdot b + a \cdot D(b),\\
D(a \le b) &\equiv D(a) \le D(b), \quad \text{accordingly for } \ge, >, <\ . \ \textbf{(BC)}\\
D(S_1 \wedge S_2) &\equiv D(S_1) \wedge D(S_2),\\
D(S_1 \vee S_2) &\equiv D(S_1) \wedge D(S_2), \ \textbf{($\wedge$ here is important for soundness)}
\end{aligned}$$

## Apply Strict Barrier Certificate on Active Boundaries

$$\text{(NSSBC)}\quad \frac{\left(\min_{i=1,\ldots,k}\max_{j=1,\ldots,m(i)} p_{ij}=0\right)\rightarrow \mathfrak{D}_{\mathbf{f}}\left(\min_{i=1,\ldots,k}\max_{j=1,\ldots,m(i)} p_{ij}\right)<0}{\left(\bigvee_{i=1}^{k}\bigwedge_{j=1}^{m(i)} p_{ij}\leq 0\right)\rightarrow [\dot{\mathbf{x}}=\mathbf{f}]\left(\bigvee_{i=1}^{k}\bigwedge_{j=1}^{m(i)} p_{ij}\leq 0\right)}.$$

## Check Invariance of $p_1 \leq 0 \vee p_2 \leq 0$

| NSSBC | | DI |
|---|---|---|
| | $(p_1 < p_2 \wedge p_1 = 0 \rightarrow \mathfrak{D}_{\mathbf{f}}(p_1) < 0)$ | |
| $\wedge$ | $(p_1 > p_2 \wedge p_2 = 0 \rightarrow \mathfrak{D}_{\mathbf{f}}(p_2) < 0)$ | $\mathfrak{D}_{\mathbf{f}}(p_1) \leq 0 \wedge \mathfrak{D}_{\mathbf{f}}(p_2) \leq 0$ |
| $\wedge$ | $(p_1 = p_2 = 0 \rightarrow \mathfrak{D}_{\mathbf{f}}(p_1) < 0 \vee \mathfrak{D}_{\mathbf{f}}(p_2) < 0)$ | |

# Liu, Zhan, Zhao (LZZ) Characterization [EMSOFT'2011]

## Definitions

$$\mathrm{In}_f(S) \equiv \{\mathbf{x} \in \mathbb{R}^n \mid \exists\ \epsilon > 0.\ \forall\ t \in (0, \epsilon).\ \mathbf{x}(t) \in S\},$$
$$\mathrm{In}_{(-f)}(S) \equiv \{\mathbf{x} \in \mathbb{R}^n \mid \exists\ \epsilon > 0.\ \forall\ t \in (0, \epsilon).\ \mathbf{x}(-t) \in S\},$$

## Characterization

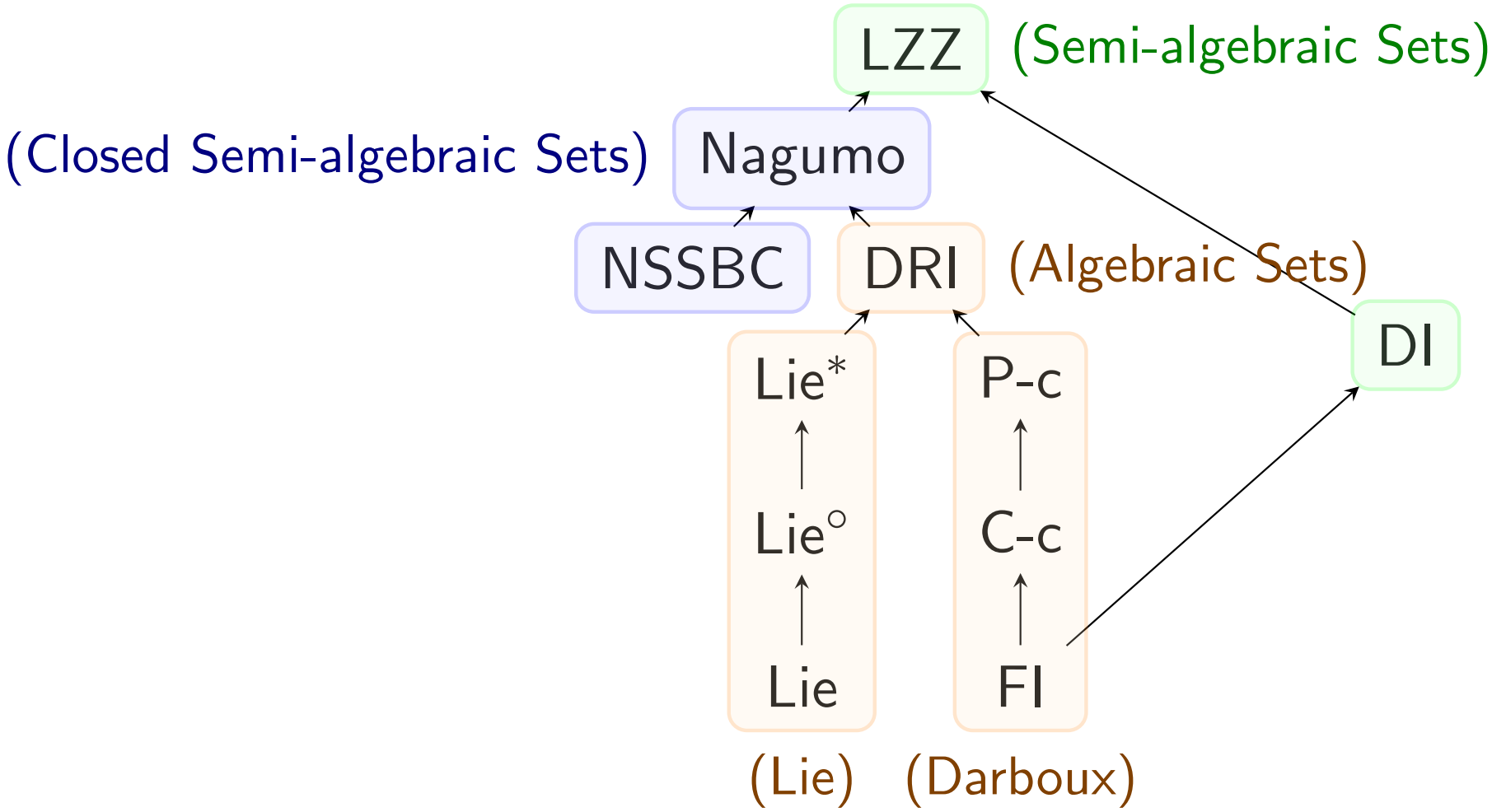
An arbitrary set $S \subset \mathbb{R}^n$ is a positive invariant for $\mathbf{f}$ if and only if

$$S \subseteq \mathrm{In}_f(S) \text{ and } S^c \subseteq \mathrm{In}_{(-f)}(S^c)$$

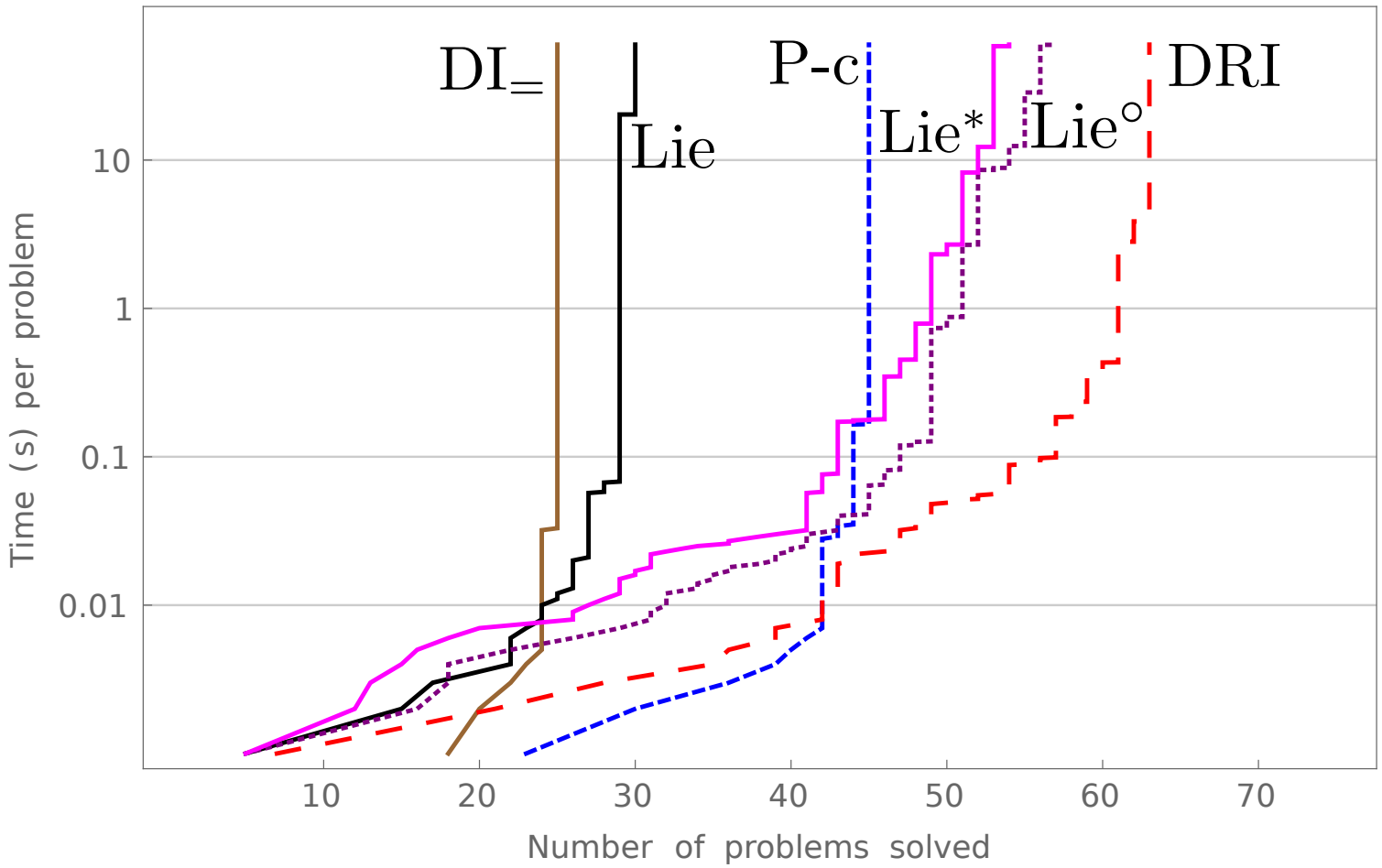
or equivalently

$$\mathrm{In}_{(-f)}(S) \subseteq S \subseteq \mathrm{In}_f(S)$$

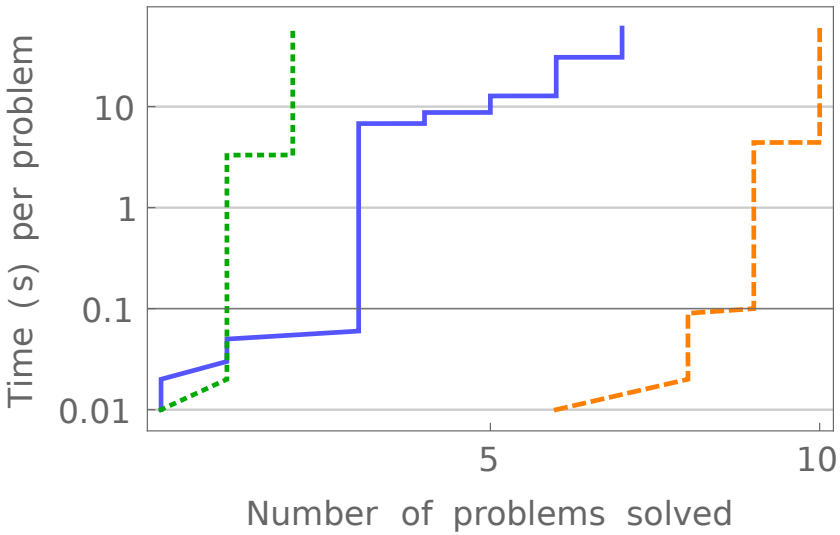
- $\mathrm{In}_f(S)$ can be computed using high-order Lie derivatives !


LZZ
(Semi-algebraic Sets)
(Closed Semi-algebraic Sets)
Nagumo
NSSBC
DRI
(Algebraic Sets)
DI
Lie*
Lie°
Lie
P-c
C-c
FI
(Lie)
(Darboux)

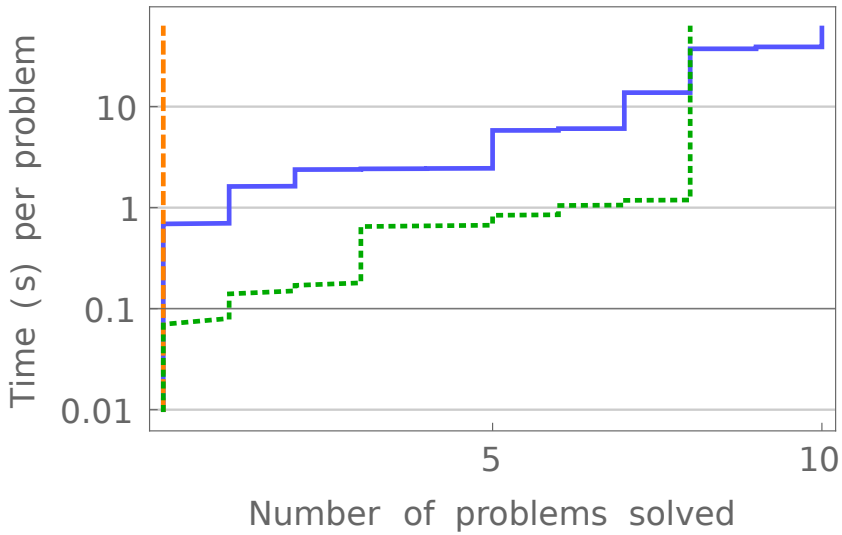
# Experimental Performance: Algebraic Sets



# Experimental Performance: Semi-algebraic Sets




LZZ vs DI




LZZ vs NSSBC

LZZ DI NSSBC

# Outline


1. Context
2. The Checking Problem
3. The Generation Problem
4. Future Avenues

## Template-Based

- Fix a template: generic polynomials with symbolic coefficients
- Use sufficient conditions to derive constraints over the coefficients
- Solve the system
- In practice:
  - templates of the form $p = 0$ (algebraic sets) with Darboux condition ($\mathfrak{D}_{\mathbf{f}}(p) \in \langle p \rangle$) work for $n \leq 10$ and $d \leq 3$.
  - templates of the form $p \leq 0$ relying on Barrier Certificates (SOSTools)

## Discrete Abstraction

- Discrete the space with the signs of a given set of polynomials
- Relies on sufficient conditions to remove spurious transitions
- Issue: How to populate and eventually refine the initial set of polynomials

# Matrix Representation: Intuition

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

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

# 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 $N = 1$

# 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: $\mathfrak{D}_{\mathbf{f}}(h) = \beta h$

# 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: $\mathfrak{D}_{\mathbf{f}}(h) = \beta h$

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

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: $\mathfrak{D}_{\mathbf{f}}(h) = \beta h$

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

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

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: $\mathfrak{D}_{\mathbf{f}}(h) = \beta h$

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

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

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

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

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

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 $M(\beta)$

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

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

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 $M(\beta)$

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

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

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 $M(\beta)$

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

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

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 $M(\beta) \quad \rightsquigarrow$ **NP-hard** [Buss et al. 1999]

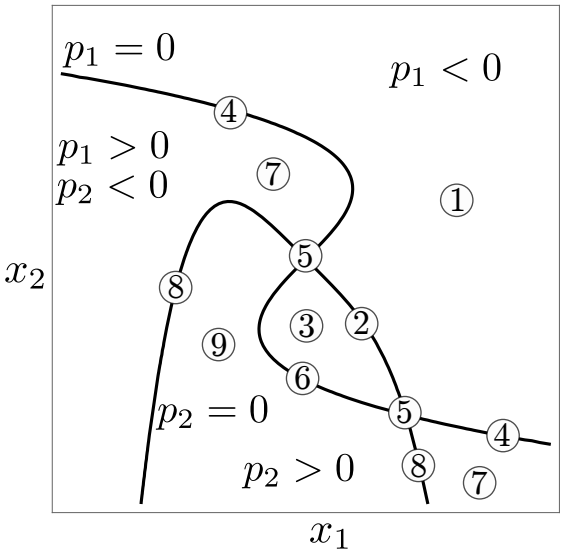
$$h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$$

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

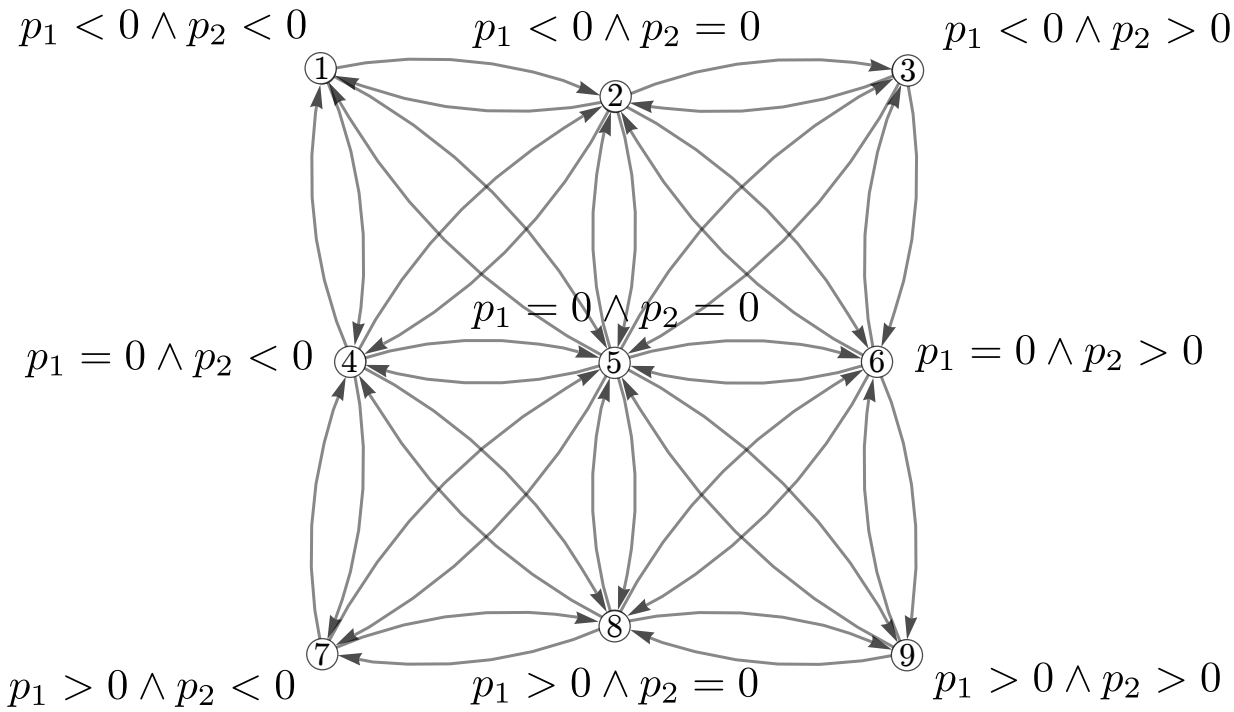
Study the **null space** (kernel) of $M(\beta)$

- 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 $M(\beta) \quad \rightsquigarrow$ **NP-hard** [Buss et al. 1999]

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




Discretization




Transition system

# Outline


1. Context
2. The Checking Problem
3. The Generation Problem
4. Future Avenues

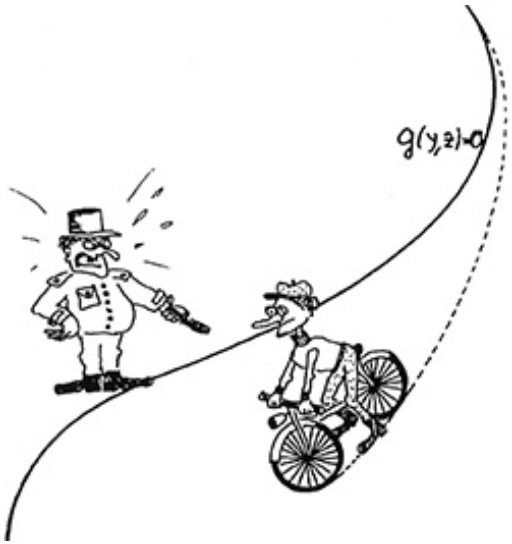
# Challenges

# Differential-Algebraic Equations (DAE)

- Verification and Faithful Simulation for cyber-physical systems with DAE

# Differential-Algebraic Equations (DAE)

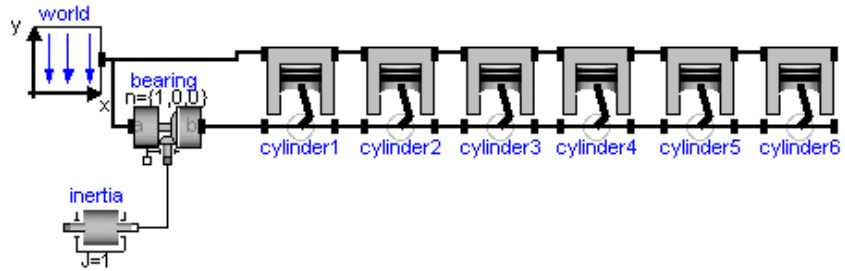
- Verification and Faithful Simulation for cyber-physical systems with DAE



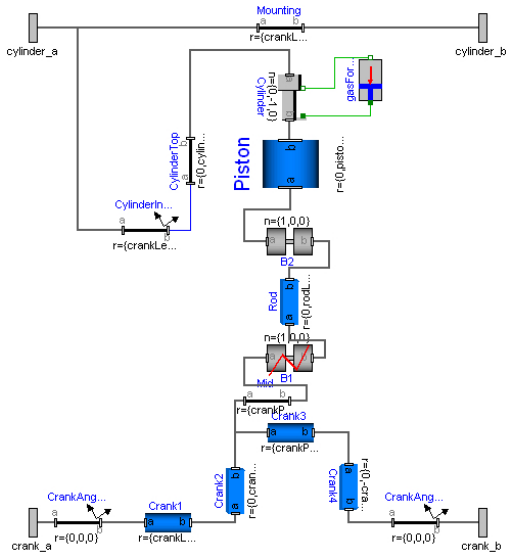

- $\mathbf{0} = \mathbf{F}(\mathbf{x}, \dot{\mathbf{x}}, t)$
- $\begin{cases} \dot{\mathbf{x}} = \mathbf{f}(\mathbf{y}, \mathbf{x}) \\ \mathbf{0} = \mathbf{g}(\mathbf{y}, \mathbf{x}) \end{cases}$
- Compositional design
- Tools: Dymola (Dassault Systèmes), Modelica

# V6 Engine Simple Combustion Model (Modelica)

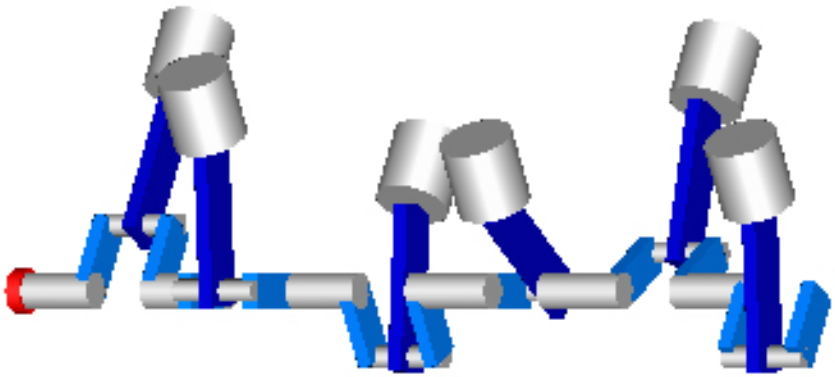
## Engine




## Cylinder




## Simulation



# Combining Static Analysis and Symbolic Computation

## Invariants Generation for DAE

- Extends previous work (algebraic approach)
- Semi-explicit form of index 1 (specific class of DAE)

## Hybrid Simulation is Hard

- Well-founded operational semantics (compilation, index reduction)
- Preserve composionality in presence of mode changes
- Proper handling of zero-crossing
  (detection and consistent initialization)
- Cascades of zero-crossings (sliding modes)

↣ Investigate the use of **static analysis** and **symbolic computation**

# Combining Static Analysis and Symbolic Computation

## Invariants Generation for DAE

- Extends previous work (algebraic approach)
- Semi-explicit form of index 1 (specific class of DAE)

## Hybrid Simulation is Hard

- Well-founded operational semantics (compilation, index reduction)
- Preserve composionality in presence of mode changes
- Proper handling of zero-crossing
  (detection and consistent initialization)
- Cascades of zero-crossings (sliding modes)

↠ Investigate the use of **static analysis** and **symbolic computation**

# Combining Static Analysis and Symbolic Computation

## Invariants Generation for DAE

- Extends previous work (algebraic approach)
- Semi-explicit form of index 1 (specific class of DAE)

## Hybrid Simulation is Hard

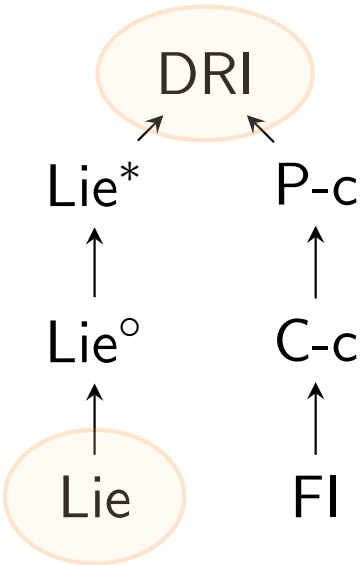
- Well-founded operational semantics (compilation, index reduction)
- Preserve composionality in presence of mode changes
- Proper handling of zero-crossing
  (detection and consistent initialization)
- Cascades of zero-crossings (sliding modes)

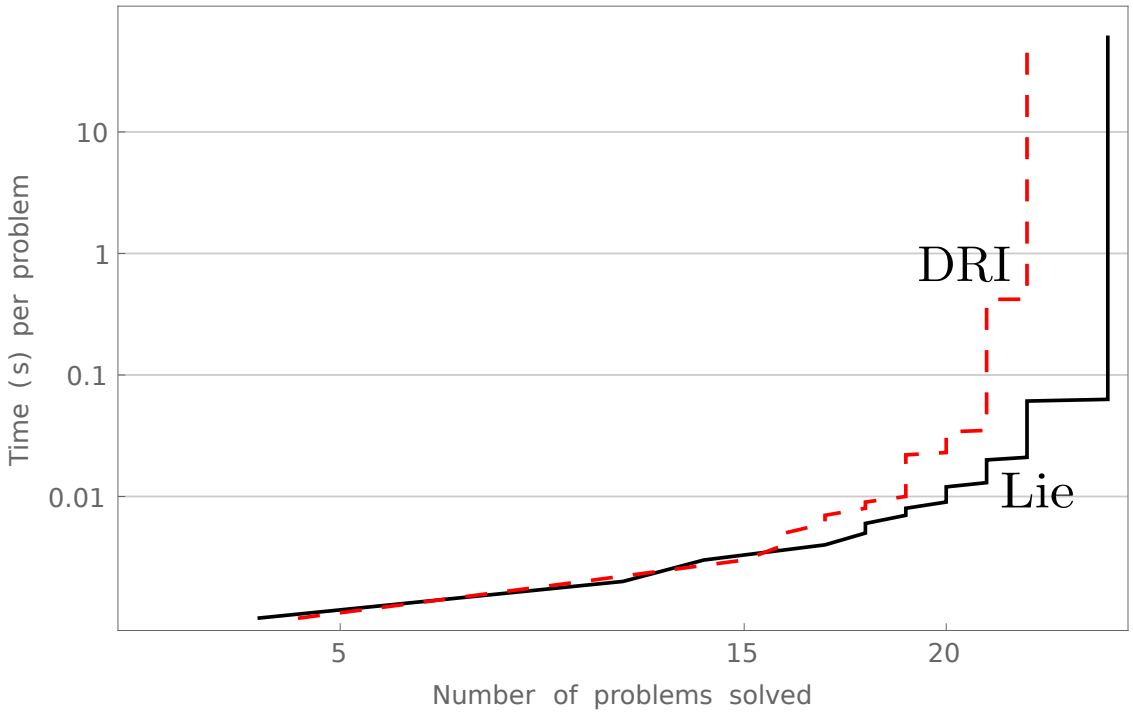
↠ Investigate the use of **static analysis** and **symbolic computation**

# Thanks for your attention !

# Smooth invariant manifolds (Lie vs DRI)

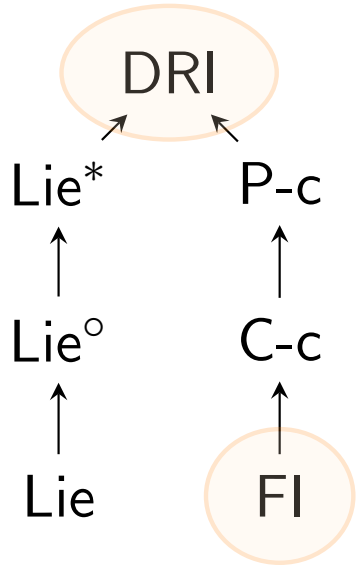
Lie and DRI **decide** invariance for **smooth invariant manifolds**.

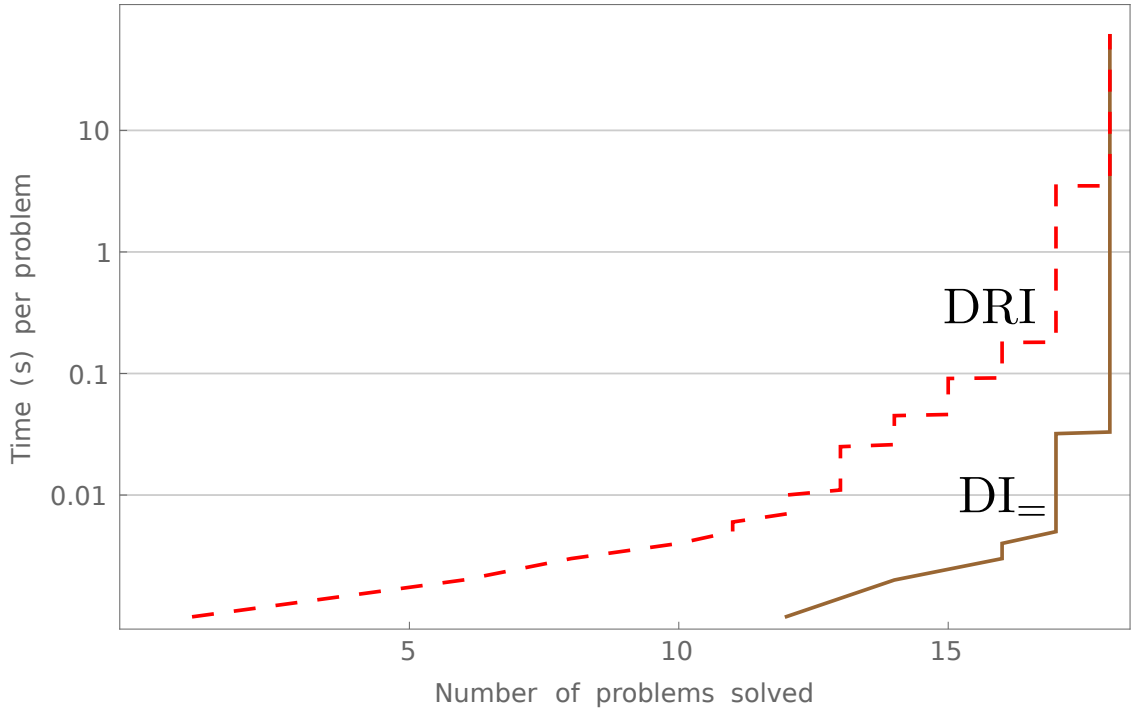


# Functional invariants (DI vs DRI)

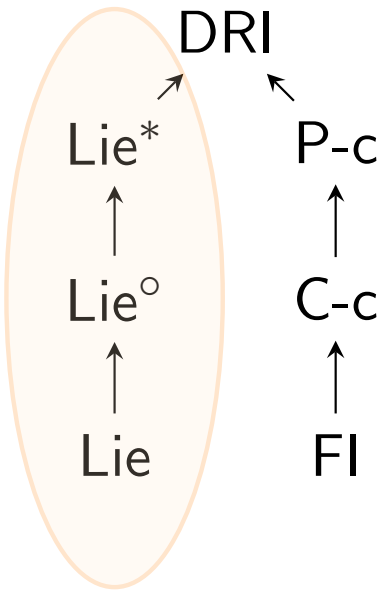
$DI_=$ and DRI **decide** invariance of varieties of **conserved quantities**.

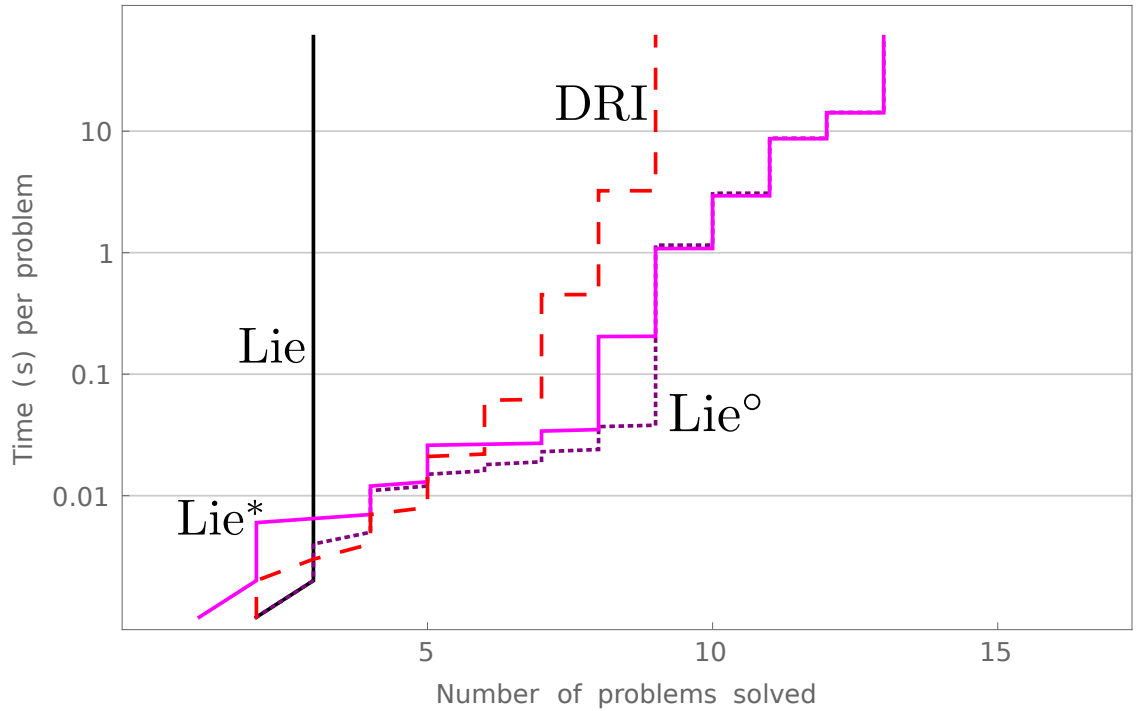


# Singularities at Equilibria (Lie, Lie$^\circ$ & Lie$^*$ vs DRI)

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



$$
\begin{array}{ll}
 & (h_1 > \max(h_2, \ldots, h_m) \rightarrow \mathfrak{D}_{\mathbf{f}}(h_1) < 0) \\
\wedge & (h_1 < \max(h_2, \ldots, h_m) \rightarrow \mathfrak{D}_{\mathbf{f}}(\max(h_2, \ldots, h_m)) < 0) \\
\wedge & (h_1 = \max(h_2, \ldots, h_m) \rightarrow \mathfrak{D}_{\mathbf{f}}(h_1) < 0 \wedge \mathfrak{D}_{\mathbf{f}}(\max(h_2, \ldots, h_m)) < 0)
\end{array}
$$

$$
\begin{array}{ll}
 & (g_1 < \min(g_2, \ldots, g_m) \rightarrow \mathfrak{D}_{\mathbf{f}}(g_1) < 0) \\
\wedge & (g_1 > \min(g_2, \ldots, g_m) \rightarrow \mathfrak{D}_{\mathbf{f}}(\min(g_2, \ldots, g_m)) < 0) \\
\wedge & (g_1 = \min(g_2, \ldots, g_m) \rightarrow \mathfrak{D}_{\mathbf{f}}(g_1) < 0 \vee \mathfrak{D}_{\mathbf{f}}(\min(g_2, \ldots, g_m)) < 0)
\end{array}
\quad .
$$