Simulating and Verifying Cyber-Physical Systems: Current Challenges and Novel Research Directions

Khalil Ghorbal

INRIA, France

SCAV (CPSWeek)

Porto, Portugal

April 10th, 2018


visoterra

Hybrid Models: Discrete $\cup$ Continuous

Computer Science (Automata Theory)

Essentially **discrete**: finite set of modes with continuous evolution within modes. [Hybrid Automata, Alur et al. 1992]

Control (Differential Equations)

Essentially **continuous**: non-smooth (discontinuous) dynamics, differential inclusions, Filippov/Utkin regularization. [Mosterman 1998, Sanfelice 2003]

Define/Describe **Reactions** to **Events**

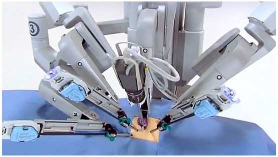
Events

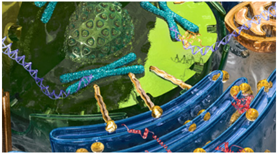
Model a simplified (often discrete) perception of the rich environment.

Reactions

Model how the system is supposed to react to an event so that it respects a set of constraints which are essentially physics laws and/or predefined requirements.

Convenient Model for a Large Class of Systems





Modeling is Instrumental to Master Complexity

Abstraction/Refinement Relationships

The molecular composition of the stratosphere has a minor impact on the Earth's orbit. Likewise, a galaxy is a dot in the Laniakea supercluster.

Compositionality and Reuse

Human beings are perhaps the most extreme example of both concepts: nature builds on top of what works to create new more complex structures.

Simulation (Time Travel)

A peek in the future (or the past) of a concrete model for a concrete initial (or final) condition. Essentially by "executing" the model step by step: only a **Local** recipe is needed.

Verification (Time Abstraction)

Qualitative analysis of the geometry (shape) of the state space as it captures **Global** properties.

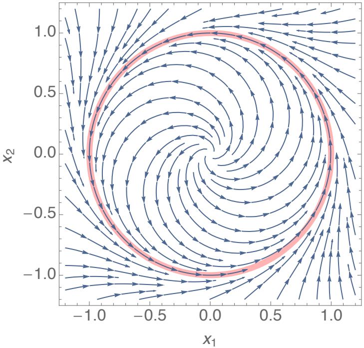
Local description defines the global properties which in turn benefit numerical approximations (eg. Geometrical Integration)

Outline

1. Introduction
2. Verification
3. Simulation
4. Challenges

If one regards a sorting algorithm as a discrete dynamical system acting on the given set, then the sorted list is an **invariant** or fixed point. It is an attractor that is reached from any initial position in finite time (# steps).

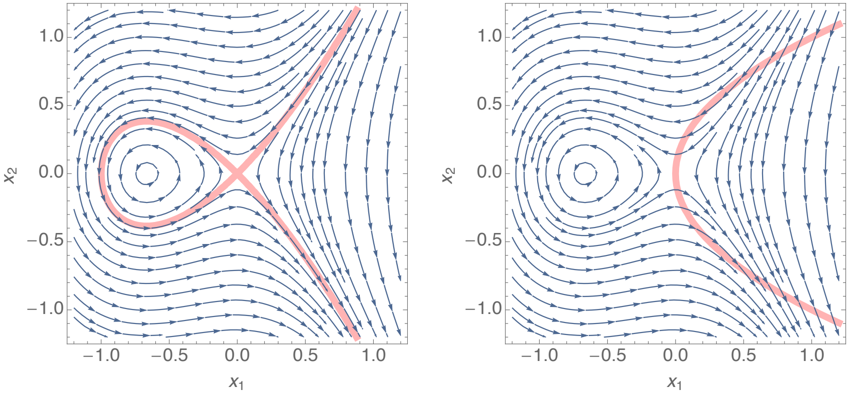
$$(\dot{x}_1, \dot{x}_2) = (x_1 - x_1^3 - x_2 - x_1 x_2^2, x_1 + x_2 - x_1^2 x_2 - x_2^3)$$



Algebraic Invariant Equation

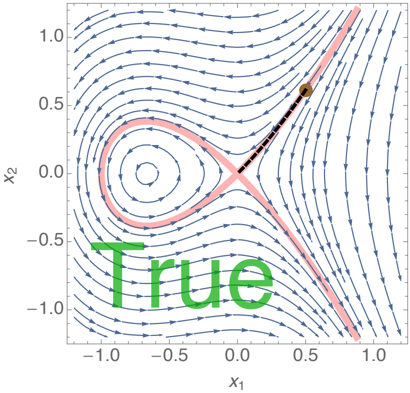
The solution for $\mathbf{x}_0 = (1, 0)$ respects $\boxed{x_1(t)^2 + x_2(t)^2 - 1 = 0}$ $\forall t$

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 ?

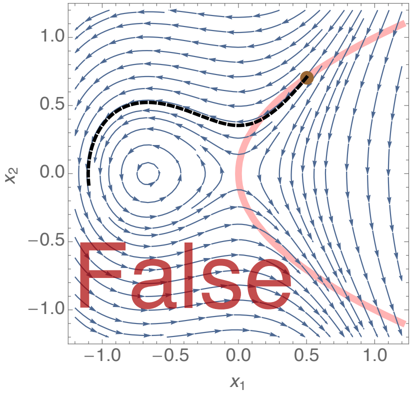


$p(x_1, x_2) = x_1^2 + x_1^3 - x_2^2$ $\qquad$ $p(x_1, x_2) = x_1 - x_2^2$

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 ?



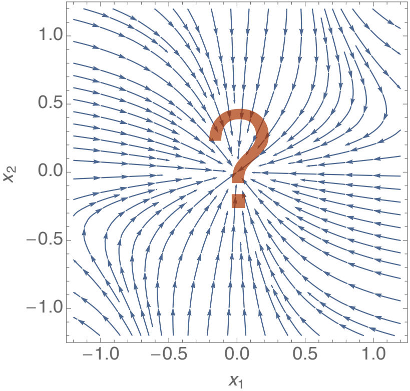
$p(x_1, x_2) = x_1^2 + x_1^3 - x_2^2$



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

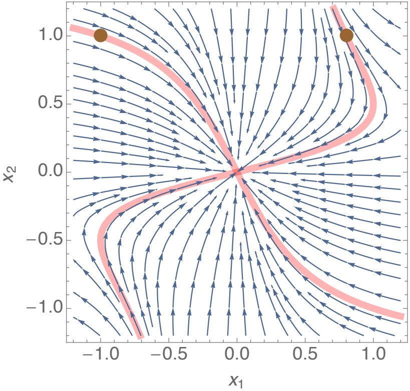
Problem II. *Generate Algebraic Invariant Equations*

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*

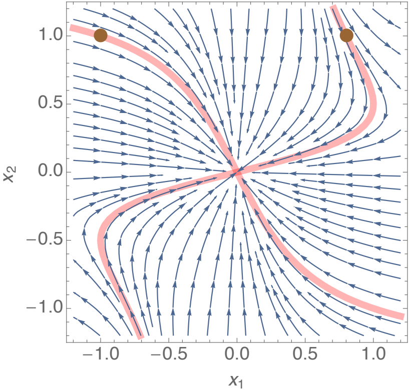
Given $\dot{\mathbf{x}} = (-x_1 + 2x_1^2 x_2, -x_2)$, how to generate p such that $p(\mathbf{x}(t)) = 0$?



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

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.

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 $\mathbf{f}$"

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

$$\equiv$$

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

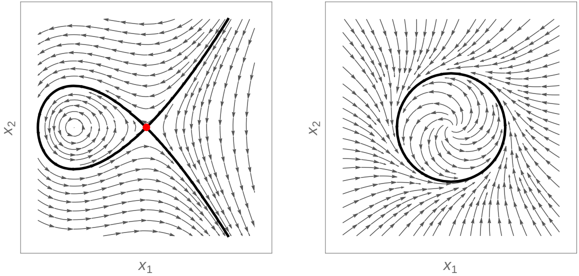
$$\equiv$$

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 $\{S\}\ \dot{\mathbf{x}} = \mathbf{f}\ \{S\}$.

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

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

Flow at singularities on the variety is directed into the variety

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

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

No flow in the problem variables at singularities on the variety

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

Flow at singularities on the variety is directed into the variety

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

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

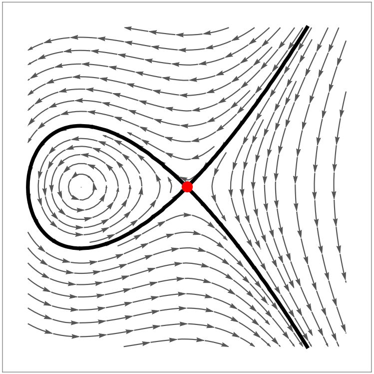
No flow in the problem variables at singularities on the variety

$$(\text{Lie}^\circ)\frac{p = 0 \to \big(\mathfrak{D}_{\mathbf{f}}(p) = 0 \land (\nabla p = \mathbf{0} \to \mathbf{f} = \mathbf{0})\big)}{(p = 0) \to [\dot{\mathbf{x}} = \mathbf{f}]\ (p = 0)}$$

Flow at singularities on the variety is directed into the variety

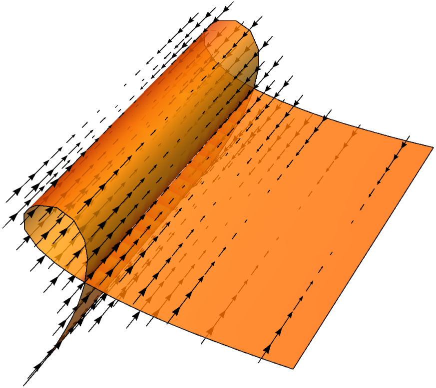
$$(\text{Lie}^*)\frac{p = 0 \to \big(\mathfrak{D}_{\mathbf{f}}(p) = 0 \land (\nabla p = \mathbf{0} \to p(\mathbf{x} + \lambda \mathbf{f}) = 0)\big)}{(p = 0) \to [\dot{\mathbf{x}} = \mathbf{f}]\ (p = 0)}\ .$$

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



Lie ✗ Lie$^\circ$ ✓ Lie* ✓

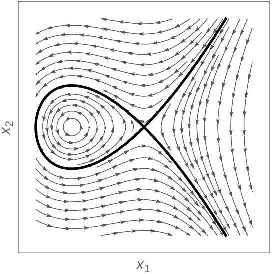
Handling certain **singularities** (points where $\nabla p = \mathbf{0}$)



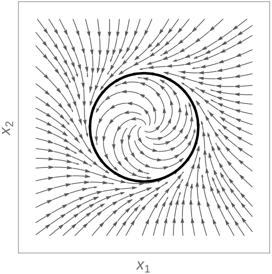
Lie ✗ Lie° ✗ Lie* ✓

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

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



p conserved ✓



p not conserved ✗

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

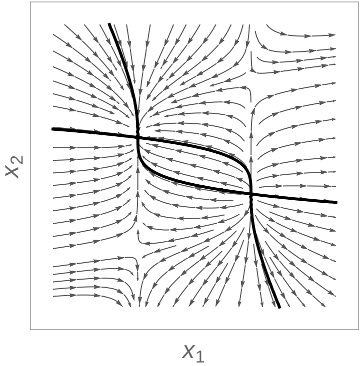
$$\text{(C-c)}\frac{\exists\lambda \in \mathbb{R},\ \mathfrak{D}_{\mathbf{f}}(p) = \lambda p}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}]\ (p = 0)},$$

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

[Sankaranarayanan et al., FMSD 2008]

$$\mathbf{f} = \left(3\left(x_1^2 - 4\right), -x_2^2 + x_1x_2 + 3\right), \qquad p = x_2^4 + 2x_1x_2^3 + 6x_2^2 + 2x_1x_2 + x_1^2 + 3,$$

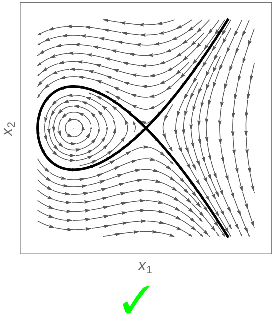
$$\mathfrak{D}_{\mathbf{f}}(p) = \underbrace{(6x_1 - 4x_2)}_{\lambda} p$$

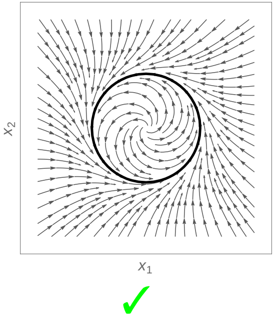


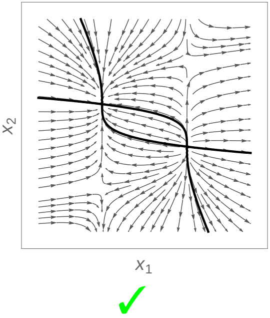
FI ✗ C-c ✗ P-c ✓

Necessary and sufficient for invariant varieties.

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





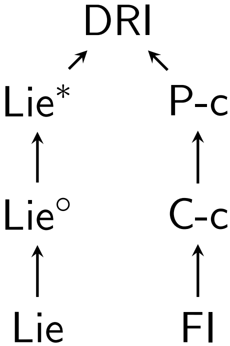


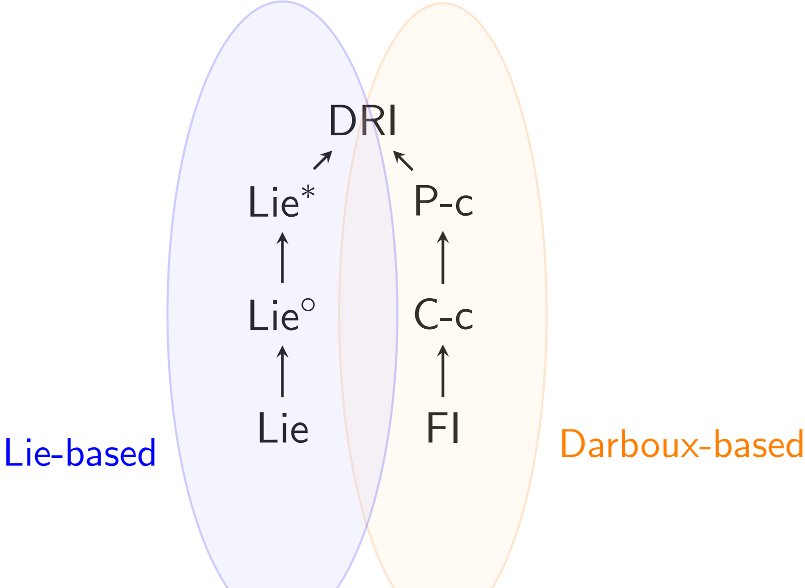
$$(\mathrm{R}_A)\frac{A}{S_A : T_A \longrightarrow [\dot{\mathbf{x}} = \mathbf{f}]S_A : T_A} \qquad (\mathrm{R}_B)\frac{B}{S_B : T_B \longrightarrow [\dot{\mathbf{x}} = \mathbf{f}]S_B : T_B}$$

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


DRI
Lie*
P-c
Lie°
C-c
Lie
FI


DRI
Lie*
P-c
Lie°
C-c
Lie
FI
Lie-based
Darboux-based

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

(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 ✗

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

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)

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

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

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

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

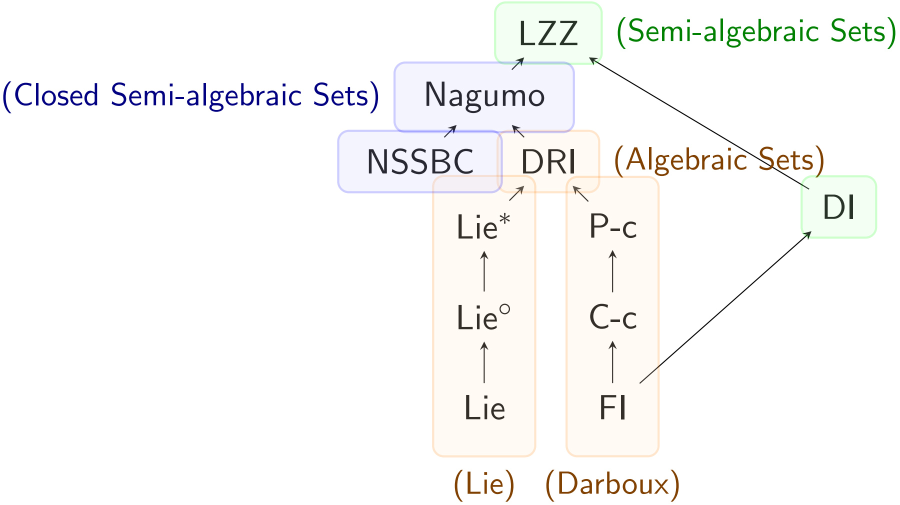
An arbitrary set $S \subset \mathbb{R}^n$ is a positive invariant for $\mathbf{f}$ if and only if

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

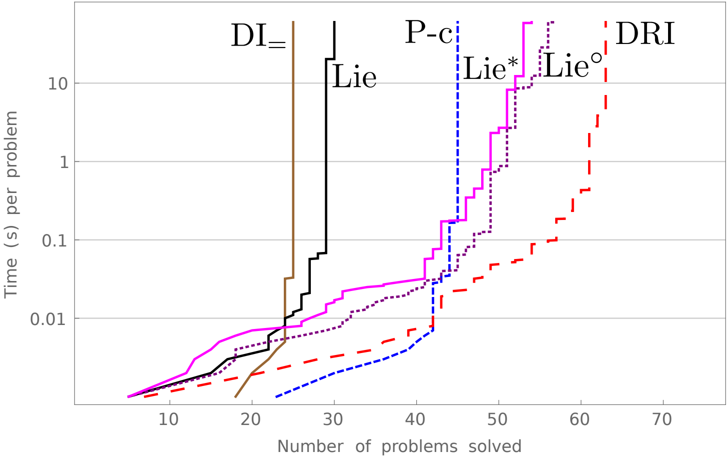
or equivalently

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

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


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

Experimental Performance: Algebraic Sets



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 $(\dot{x}_1, \dot{x}_2) = (x_1, x_2)$

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

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 $N = 1$

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

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

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

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

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

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

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

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

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

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

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 $M(\beta)$

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

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

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 $M(\beta)$

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

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

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 $M(\beta)$

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

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

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

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

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

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

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

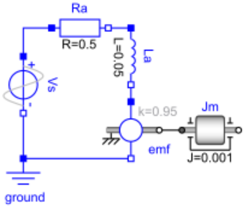
Simulation (Time Travel)

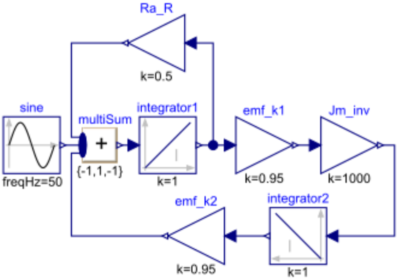
A peek in the future (or the past) of a concrete model for a concrete initial (or final) condition. Essentially by "executing" the model step by step: only a **Local** recipe is needed.

Verification (Time Abstraction)

Qualitative analysis of the geometry (shape) of the state space as it captures **Global** properties.

Local description defines the global properties which in turn benefit numerical approximations (eg. Geometrical Integration)

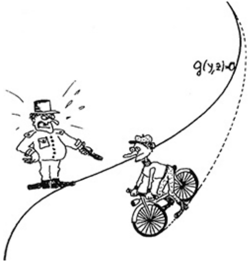

Ra
R=0.5
L=0.05
La
Vs
k=0.95
Jm
emf
J=0.001
ground


Ra_R
k=0.5
sine
multiSum
integrator1
emf_k1
Jm_inv
freqHz=50
{-1,1,-1}
k=1
k=0.95
k=1000
emf_k2
integrator2
k=0.95
k=1

Differential-Algebraic Equations (DAE)

- Verification and Faithful Simulation for cyber-physical systems with 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

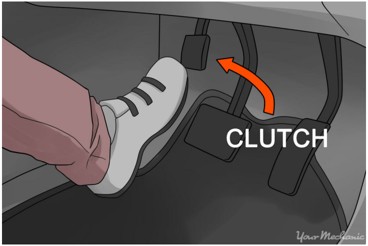
`if` **Guard** `do` **Differential Equation**

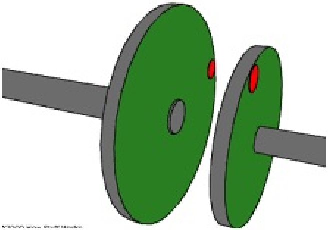
- **Guard**: predicate in the state variables and their **time derivatives**.
- **Differential Equation**: equation, **implicit** or explicit, in the state variables and their time derivatives.

if **Guard** do **Differential Equation**

- **Guard**: predicate in the state variables and their **time derivatives**.
- **Differential Equation**: equation, **implicit** or explicit, in the state variables and their time derivatives.

When a guard holds, its equation is enforced.


CLUTCH
YourMechanic



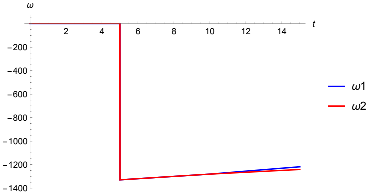
$$
\begin{array}{rll}
\texttt{if t} & \texttt{do} & J_1\dot{\omega}_1 = \tau_1 \qquad (e_1)\\
\texttt{if t} & \texttt{do} & J_2\dot{\omega}_2 = \tau_2 \qquad (e_2)\\
\texttt{if } \gamma & \texttt{do} & \omega_1 - \omega_2 = 0 \qquad (e_3)\\
\texttt{if } \gamma & \texttt{do} & \tau_1 + \tau_2 = 0 \qquad (e_4)\\
\texttt{if } \neg\gamma & \texttt{do} & \tau_1 = 0 \qquad (e_5)\\
\texttt{if } \neg\gamma & \texttt{do} & \tau_2 = 0 \qquad (e_6)
\end{array}
$$

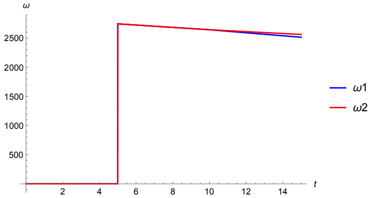
- **State Variables**: the angular velocities ω_1 and ω_2
- γ is an input signal modelling the pedal's position

$$
\begin{array}{rlll}
\texttt{if t} & \texttt{do} & J_1\dot{\omega}_1 = \tau_1 & (e_1) \\
\texttt{if t} & \texttt{do} & J_2\dot{\omega}_2 = \tau_2 & (e_2) \\
\texttt{if } \gamma & \texttt{do} & \omega_1 - \omega_2 = 0 & (e_3) \\
\texttt{if } \gamma & \texttt{do} & \tau_1 + \tau_2 = 0 & (e_4) \\
\texttt{if } \neg\gamma & \texttt{do} & \tau_1 = 0 & (e_5) \\
\texttt{if } \neg\gamma & \texttt{do} & \tau_2 = 0 & (e_6)
\end{array}
$$

if t	do	$J_1\dot{\omega}_1 = \tau_1$	(e_1)
if t	do	$J_2\dot{\omega}_2 = \tau_2$	(e_2)
if γ	do	$\omega_1 - \omega_2 = 0$	(e_3)
if γ	do	$\tau_1 + \tau_2 = 0$	(e_4)
if $\neg\gamma$	do	$\tau_1 = 0$	(e_5)
if $\neg\gamma$	do	$\tau_2 = 0$	(e_6)

- Dymola **crashes** with a division by zero
- Mathematica treats resets as initializations (nondeterministic behavior)





The solution may be discontinuous when $\gamma : \mathrm{f} \to \mathrm{t}$ because of the additional constraint $\omega_1 - \omega_2 = 0$

Problem 1 How to handle overdetermined systems ?

- The angular velocities ω_1 and ω_2 are **known**
- γ switches to t (the driver engages the clutch)

$\omega_1 - \omega_2 = 0$ is **enforced**

- The system **becomes** overdetermined
- The solution is not smooth and even discontinuous

Problem 2 What is the meaning of the derivatives ?

Some equations must hold for $\gamma = \mathsf{t}$ and $\gamma = \mathsf{f}$.

$$\begin{array}{lll} \texttt{if t} & \texttt{do} & J_1\dot{\omega}_1 = \tau_1 \qquad (e_1) \\ \texttt{if t} & \texttt{do} & J_2\dot{\omega}_2 = \tau_2 \qquad (e_2) \end{array}$$

- What is the **meaning** of derivatives when $\gamma : \mathsf{f} \to \mathsf{t}$?
- How to compute the **reset values** ?

Causality Principle

The additional constraints are

- **caused** by (consequence of) the **current** status, and
- **enforced** at the **immediate next** instant

Causality Principle

The additional constraints are

- **caused** by (consequence of) the **current** status, and
- **enforced** at the **immediate next** instant

t : **present**

$$\omega_1(t) - \omega_2(t) \neq 0$$

$$\omega_1(t+\delta) - \omega_2(t+\delta) = 0$$

$t + \delta\ ,\ 0 < \delta << 1$: **immediate future**

Causality Principle

The additional constraints are

- **caused** by (consequence of) the **current** status, and
- **enforced** at the **immediate next** instant

t : **present**

$\omega_1(t) - \omega_2(t) \neq 0$

$\omega_1(t+\delta) - \omega_2(t+\delta) = 0$

$t + \delta\ ,\ 0 < \delta << 1$: **immediate future**

$\delta \in {}^\star\mathbb{R}$ is a **positive infinitesimal**

- $\delta = \langle \delta_1, \delta_2, \ldots \rangle$
- $\delta_i \in \mathbb{R}$
- Not necessarily convergent
- $\langle 1, \frac{1}{2}, \frac{1}{3}, \ldots \rangle$ is a (positive) infinitesimal
- $r = \langle r, r, r, \ldots \rangle$, $r \in \mathbb{R}$
- Functions over the reals can be *internalized*
- $x(\langle t_1, t_2, \ldots \rangle) = \langle x(t_1), x(t_2), \ldots \rangle$

- $\delta = \langle \delta_1, \delta_2, \ldots \rangle$
- $\delta_i \in \mathbb{R}$
- Not necessarily convergent
- $\langle 1, \frac{1}{2}, \frac{1}{3}, \ldots \rangle$ is a (positive) infinitesimal
- $r = \langle r, r, r, \ldots \rangle$, $r \in \mathbb{R}$
- Functions over the reals can be *internalized*
- $x(\langle t_1, t_2, \ldots \rangle) = \langle x(t_1), x(t_2), \ldots \rangle$

- $\delta = \langle \delta_1, \delta_2, \ldots \rangle$
- $\delta_i \in \mathbb{R}$
- Not necessarily convergent
- $\langle 1, \frac{1}{2}, \frac{1}{3}, \ldots \rangle$ is a (positive) infinitesimal
- $r = \langle r, r, r, \ldots \rangle$, $r \in \mathbb{R}$
- Functions over the reals can be *internalized*
- $x(\langle t_1, t_2, \ldots \rangle) = \langle x(t_1), x(t_2), \ldots \rangle$

- $\delta = \langle \delta_1, \delta_2, \ldots \rangle$
- $\delta_i \in \mathbb{R}$
- Not necessarily convergent
- $\langle 1, \frac{1}{2}, \frac{1}{3}, \ldots \rangle$ is a (positive) infinitesimal
- $r = \langle r, r, r, \ldots \rangle$, $r \in \mathbb{R}$
- Functions over the reals can be *internalized*
- $x(\langle t_1, t_2, \ldots \rangle) = \langle x(t_1), x(t_2), \ldots \rangle$

Let $\delta \in {}^\star\mathbb{R}$ be a non zero infinitesimal.

$$\frac{x(t+\delta) - x(t)}{\delta}$$

Proposition

A real function x is differentiable at t if and only if there exists a real number b such that

$$\frac{x(t+\epsilon) - x(t)}{\epsilon} \sim b$$

for any non zero infinitesimal ϵ.

$$\dot{x} \text{ is replaced by } \frac{x(t+\delta) - x(t)}{\delta} = \frac{x^{\bullet} - x}{\delta}$$

- **Shift forward** (when needed)
- **Formal substitution** of time derivatives into difference quotient.

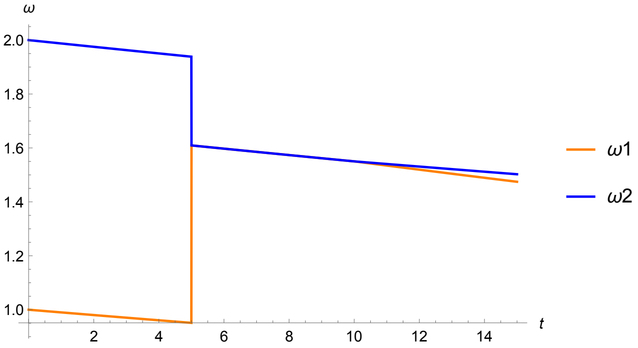
$$
\begin{array}{rlll}
\texttt{if t} & \texttt{do} & J_1\dot{\omega}_1 = \tau_1 & (e_1) \\
\texttt{if t} & \texttt{do} & J_2\dot{\omega}_2 = \tau_2 & (e_2) \\
\texttt{if } \gamma & \texttt{do} & \omega_1 - \omega_2 = 0 & (e_3) \\
\texttt{if } \gamma & \texttt{do} & \tau_1 + \tau_2 = 0 & (e_4) \\
\texttt{if } \neg\gamma & \texttt{do} & \tau_1 = 0 & (e_5) \\
\texttt{if } \neg\gamma & \texttt{do} & \tau_2 = 0 & (e_6)
\end{array}
\qquad
\begin{array}{rlll}
\texttt{if t} & \texttt{do} & J_1\frac{\omega_1^\bullet - \omega_1}{\delta} = \tau_1 & (e_1^\delta) \\
\texttt{if t} & \texttt{do} & J_2\frac{\omega_2^\bullet - \omega_2}{\delta} = \tau_2 & (e_2^\delta) \\
\texttt{if } \gamma & \texttt{do} & \omega_1^\bullet - \omega_2^\bullet = 0 & (e_3^\bullet) \\
\texttt{if } \gamma & \texttt{do} & \tau_1 + \tau_2 = 0 & (e_4) \\
\texttt{if } \neg\gamma & \texttt{do} & \tau_1 = 0 & (e_5) \\
\texttt{if } \neg\gamma & \texttt{do} & \tau_2 = 0 & (e_6)
\end{array}
$$

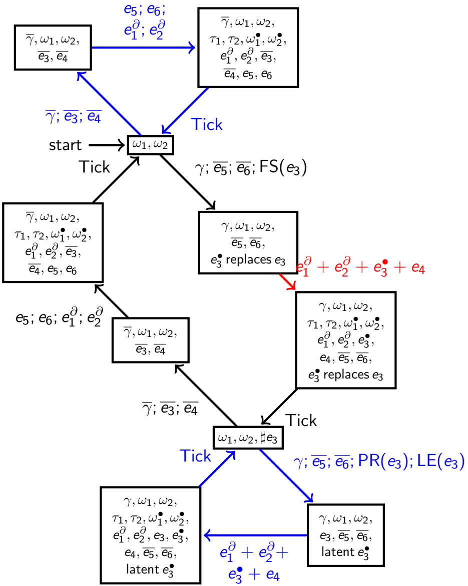
$$
\begin{array}{llll}
\texttt{if t} & \texttt{do} & J_1 \frac{\omega_1^\bullet - \omega_1}{\delta} = \tau_1 & (e_1^\delta) \\
\texttt{if t} & \texttt{do} & J_2 \frac{\omega_2^\bullet - \omega_2}{\delta} = \tau_2 & (e_2^\delta) \\
\texttt{if } \gamma & \texttt{do} & \omega_1^\bullet - \omega_2^\bullet = 0 & (e_3^\bullet) \\
\texttt{if } \gamma & \texttt{do} & \tau_1 + \tau_2 = 0 & (e_4) \\
\texttt{if } \neg\gamma & \texttt{do} & \tau_1 = 0 & (e_5) \\
\texttt{if } \neg\gamma & \texttt{do} & \tau_2 = 0 & (e_6)
\end{array}
$$

$$\omega_1^\bullet = \omega_2^\bullet = \frac{J_1\omega_1 + J_2\omega_2}{J_1 + J_2}$$

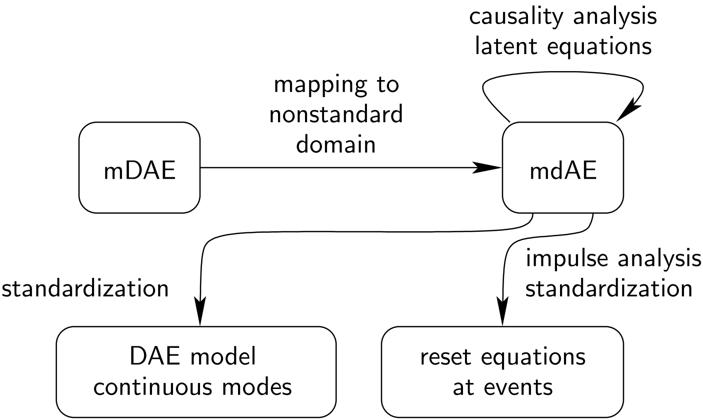
Standardization

- Automated procedure for a class of systems
- Generalization remains a challenge


ω
2.0
1.8
1.6
1.4
1.2
1.0
2
4
6
8
10
12
14
t
ω1
ω2


$\overline{\gamma}, \omega_1, \omega_2, \overline{e_3}, \overline{e_4}$
$e_5; e_6; e_1^\partial; e_2^\partial$
$\overline{\gamma}, \omega_1, \omega_2, \tau_1, \tau_2, \omega_1^\bullet, \omega_2^\bullet, e_1^\partial, e_2^\partial, \overline{e_3}, \overline{e_4}, e_5, e_6$
$\overline{\gamma}; \overline{e_3}; \overline{e_4}$
Tick
start
ω_1, ω_2
Tick
$\gamma; \overline{e_5}; \overline{e_6}; \mathsf{FS}(e_3)$
$\overline{\gamma}, \omega_1, \omega_2, \tau_1, \tau_2, \omega_1^\bullet, \omega_2^\bullet, e_1^\partial, e_2^\partial, \overline{e_3}, \overline{e_4}, e_5, e_6$
$\gamma, \omega_1, \omega_2, \overline{e_5}, \overline{e_6}$, $e_3^\bullet$ replaces e_3
$e_1^\partial + e_2^\partial + e_3^\bullet + e_4$
$e_5; e_6; e_1^\partial; e_2^\partial$
$\overline{\gamma}, \omega_1, \omega_2, \overline{e_3}, \overline{e_4}$
$\gamma, \omega_1, \omega_2, \tau_1, \tau_2, \omega_1^\bullet, \omega_2^\bullet, e_1^\partial, e_2^\partial, e_3^\bullet, e_4, \overline{e_5}, \overline{e_6}$, $e_3^\bullet$ replaces e_3
$\overline{\gamma}; \overline{e_3}; \overline{e_4}$
Tick
$\omega_1, \omega_2, \sharp e_3$
Tick
$\gamma; \overline{e_5}; \overline{e_6}; \mathsf{PR}(e_3); \mathsf{LE}(e_3)$
$\gamma, \omega_1, \omega_2, \tau_1, \tau_2, \omega_1^\bullet, \omega_2^\bullet, e_1^\partial, e_2^\partial, e_3, e_3^\bullet, e_4, \overline{e_5}, \overline{e_6}$, latent $e_3^\bullet$
$e_1^\partial + e_2^\partial + e_3^\bullet + e_4$
$\gamma, \omega_1, \omega_2, e_3, \overline{e_5}, \overline{e_6}$, latent $e_3^\bullet$

Unifying Discrete and Continuous Dynamics



Challenges

Combining Static Analysis and Symbolic Computation

Invariants Generation

- Extends previous work (algebraic approach)
- **Approximate** exact computations to scale

Simulation of multi-mode DAE

- 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

- Extends previous work (algebraic approach)
- **Approximate** exact computations to scale

Simulation of multi-mode DAE

- 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

- Extends previous work (algebraic approach)
- **Approximate** exact computations to scale

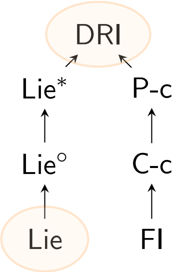
Simulation of multi-mode DAE

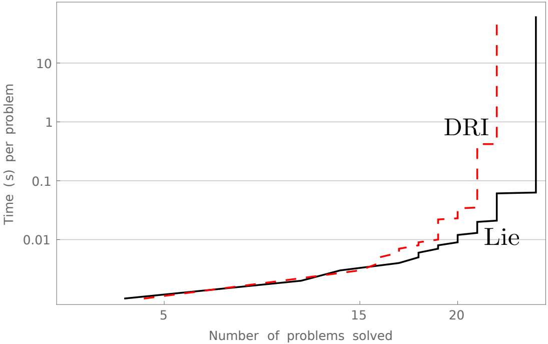
- Well-founded operational semantics (compilation, index reduction)
- Preserve composionality in presence of mode changes
- Proper handling of zero-crossing (detection and consistent initialization)
- Cascades of zero-crossings (sliding modes)

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

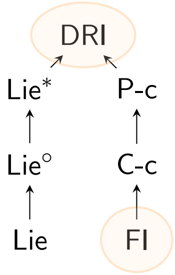
Thanks for your attention !

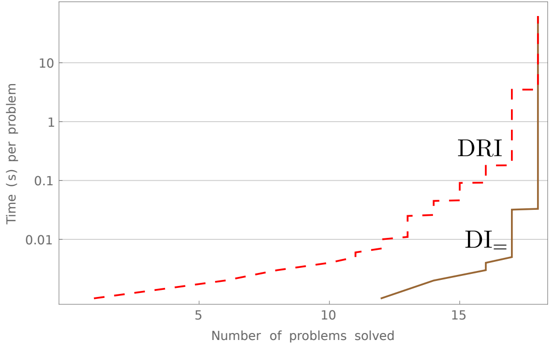
Lie and DRI **decide** invariance for **smooth invariant manifolds**.





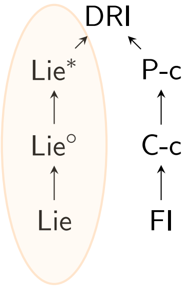
$\mathrm{DI}_=$ and DRI **decide** invariance of varieties of **conserved quantities**.

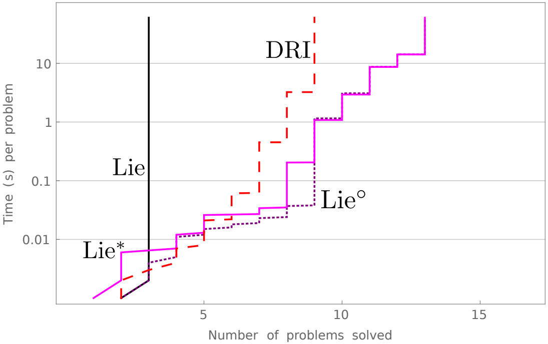




Singularities at Equilibria (Lie, Lie$^\circ$ & Lie* vs DRI)

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





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

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