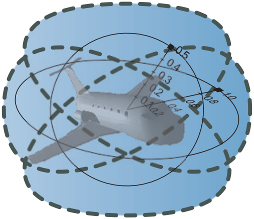
Differential Equation Axiomatization

The Impressive Power of Differential Ghosts

André Platzer
Joint work with Yong Kiam Tan

Carnegie Mellon University

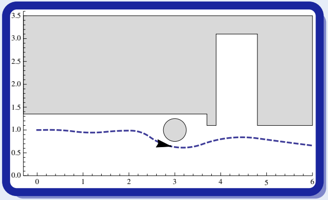


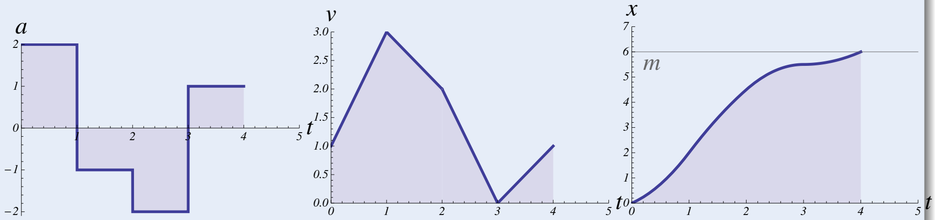
Outline

Challenge (Hybrid Systems)

Fixed law describing state evolution with both

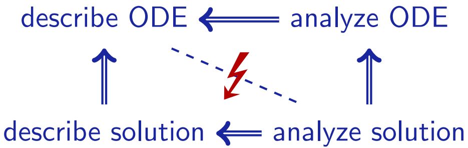
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)





Contributions

- Classical approach: ① given ODE ② solve ODE ③ analyze solution
- Descriptive power of ODEs: ODE much easier than its solution
- ↯ Analyzing ODEs via their solutions undoes their descriptive power!



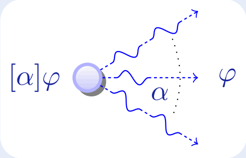
Poincaré 1881

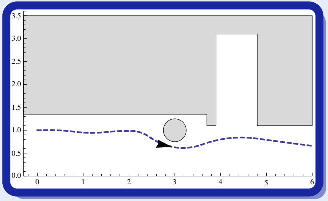
1. Now: Logical foundations of differential equation invariants
2. Identify axioms for differential equations
3. Completeness for differential equation invariants
4. Uniformly substitutable axioms, not infinite axiom schemata

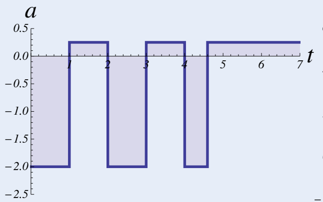
Outline

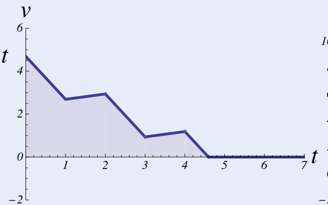
1. Differential Dynamic Logic
   - Semantics
   - Axiomatization
   - Relative Completeness / ODE
2. Proofs for Differential Equations
   - Differential Equation Axioms
   - Differential Invariants / Cuts / Ghosts
3. Completeness for Differential Equation Invariants
   - Derived Darboux
   - Semialgebraic Invariants
   - Real Induction
   - Local Progress
   - Completeness for Invariants
4. Summary

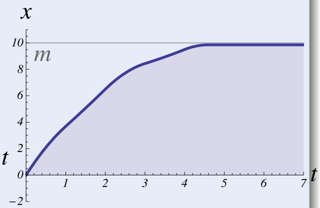
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



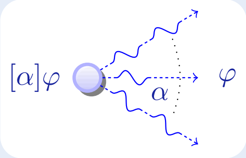


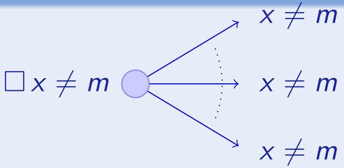


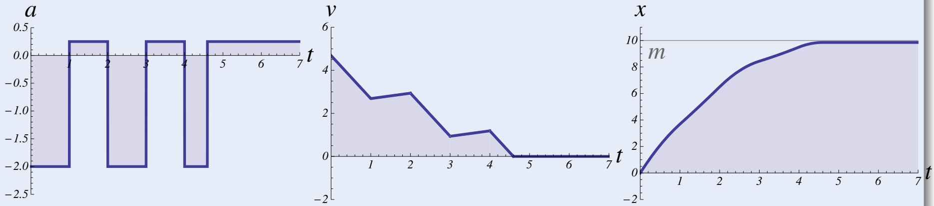




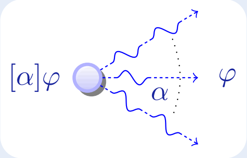
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

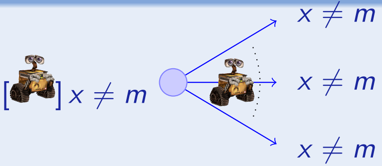


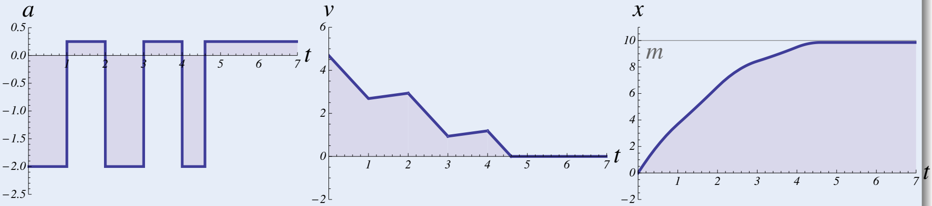




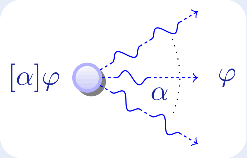
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

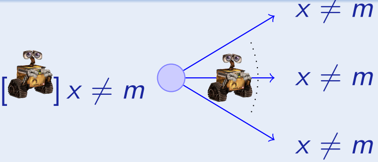




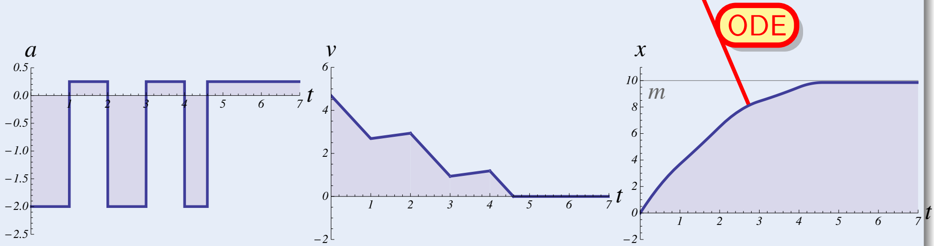


Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

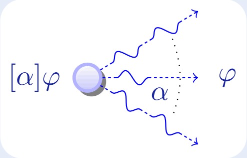


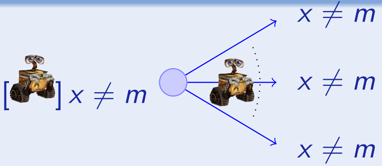


$$x' = v, v' = a$$

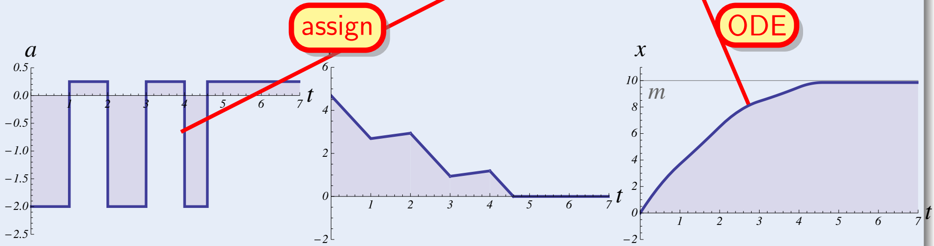


Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



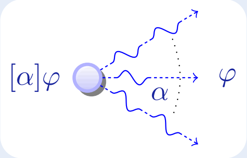


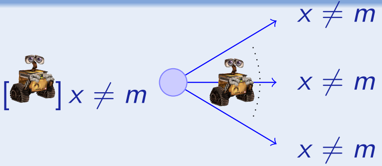
$a := -b$ $\quad x' = v, v' = a$



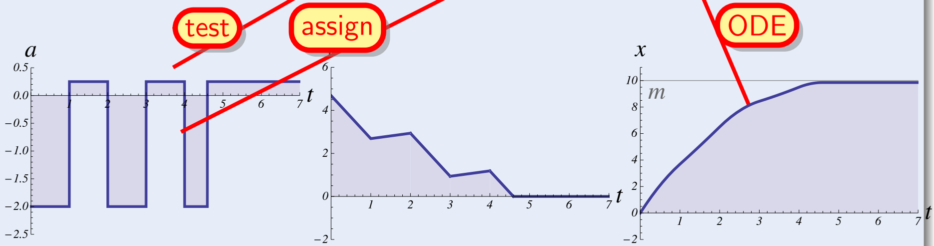
Hybrid Systems Analysis

Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



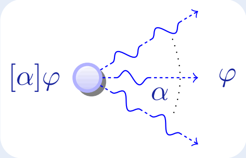


$(\texttt{if}(SB(x, m))\ a := -b)$ $x' = v, v' = a$



Hybrid Systems Analysis

Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



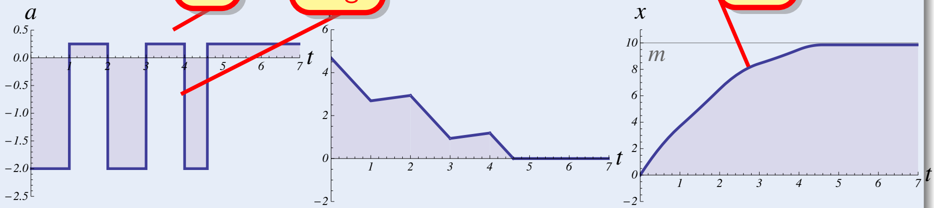
seq. compose

$$(\texttt{if}(SB(x, m))\ a := -b)\ ;\ x' = v, v' = a$$

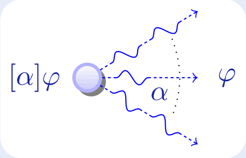
test

assign

ODE



Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



seq. compose

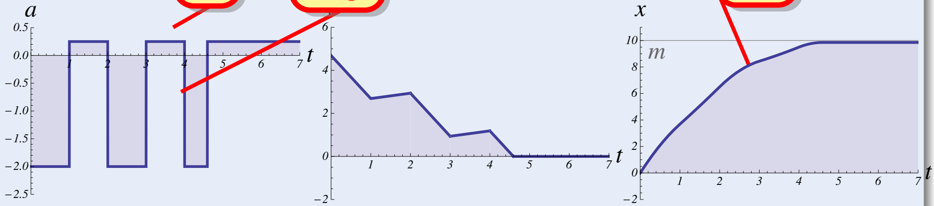
nondet. repeat

$$\big((\texttt{if}(SB(x,m))\ a := -b)\ ;\ x' = v, v' = a\big)^*$$

test

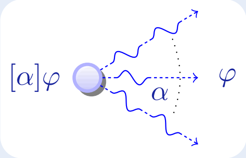
assign

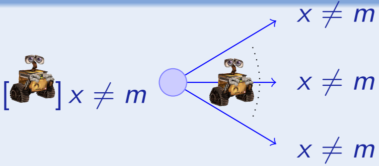
ODE



Hybrid Systems Analysis

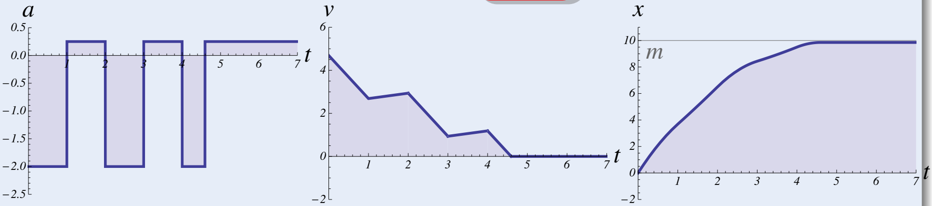
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)





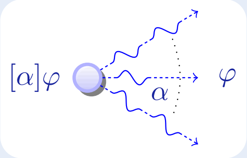
$$\Big[\Big(\big(\mathtt{if}(SB(x,m))\ a := -b\big)\ ;\ x' = v, v' = a\Big)^*\Big]\underbrace{x \neq m}_{\text{post}}$$

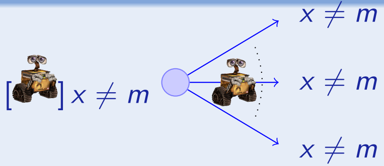
all runs



Hybrid Systems Analysis

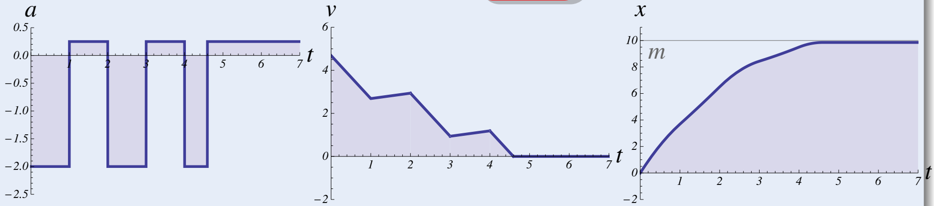
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)





$$\underbrace{x \neq m \land b > 0}_{\text{init}} \to \left[\left((\mathtt{if}(SB(x, m))\ a := -b)\ ;\ x' = v, v' = a\right)^*\right]\underbrace{x \neq m}_{\text{post}}$$

all runs



Differential Dynamic Logic dL: Semantics

Definition (Hybrid program semantics) $(\llbracket\cdot\rrbracket : \mathrm{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$

$$
\begin{aligned}
\llbracket x := e \rrbracket &= \{(\omega,\nu) : \nu = \omega \text{ except } \nu\llbracket x\rrbracket = \omega\llbracket e\rrbracket\} \\
\llbracket ?Q \rrbracket &= \{(\omega,\omega) : \omega \in \llbracket Q\rrbracket\} \\
\llbracket x' = f(x) \rrbracket &= \{(\varphi(0),\varphi(r)) : \varphi \models x' = f(x) \text{ for some duration } r\} \\
\llbracket \alpha \cup \beta \rrbracket &= \llbracket\alpha\rrbracket \cup \llbracket\beta\rrbracket \\
\llbracket \alpha ; \beta \rrbracket &= \llbracket\alpha\rrbracket \circ \llbracket\beta\rrbracket \\
\llbracket \alpha^* \rrbracket &= \llbracket\alpha\rrbracket^* = \bigcup_{n\in\mathbb{N}} \llbracket\alpha^n\rrbracket
\end{aligned}
$$

compositional semantics

Definition (dL semantics) $(\llbracket\cdot\rrbracket : \mathrm{Fml} \to \wp(\mathcal{S}))$

$$
\begin{aligned}
\llbracket e \geq \tilde{e} \rrbracket &= \{\omega : \omega\llbracket e\rrbracket \geq \omega\llbracket\tilde{e}\rrbracket\} \\
\llbracket \neg P \rrbracket &= \llbracket P\rrbracket^{\complement} \\
\llbracket P \wedge Q \rrbracket &= \llbracket P\rrbracket \cap \llbracket Q\rrbracket \\
\llbracket \langle\alpha\rangle P \rrbracket &= \llbracket\alpha\rrbracket \circ \llbracket P\rrbracket = \{\omega : \nu \in \llbracket P\rrbracket \text{ for some } \nu : (\omega,\nu) \in \llbracket\alpha\rrbracket\} \\
\llbracket [\alpha] P \rrbracket &= \llbracket \neg\langle\alpha\rangle\neg P\rrbracket = \{\omega : \nu \in \llbracket P\rrbracket \text{ for all } \nu : (\omega,\nu) \in \llbracket\alpha\rrbracket\} \\
\llbracket \exists x\, P \rrbracket &= \{\omega : \omega_x^r \in \llbracket P\rrbracket \text{ for some } r \in \mathbb{R}\}
\end{aligned}
$$

Differential Dynamic Logic: Axiomatization

equations of truth

$[:=]$	$[x := e]P(x) \leftrightarrow P(e)$
$[?]$	$[?Q]P \leftrightarrow (Q \rightarrow P)$
$[']$	$[x' = f(x)]P \leftrightarrow \forall t{\geq}0\,[x := x(t)]P \qquad (x'(t) = f(x))$
$[\cup]$	$[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$
$[;]$	$[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$
$[^*]$	$[\alpha^*]P \leftrightarrow P \wedge [\alpha][\alpha^*]P$
K	$[\alpha](P \rightarrow Q) \rightarrow ([\alpha]P \rightarrow [\alpha]Q)$
I	$[\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$
C	$[\alpha^*]\forall v{>}0\,(P(v) \rightarrow \langle\alpha\rangle P(v-1)) \rightarrow \forall v\,(P(v) \rightarrow \langle\alpha^*\rangle\exists v{\leq}0\,P(v))$

LICS'12,JAR'17

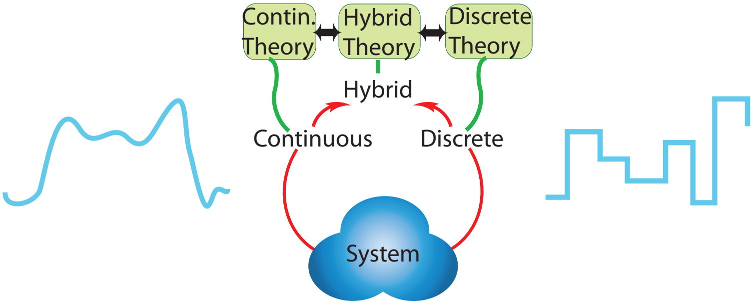
Complete Proof Theory of Hybrid Systems

Theorem (Sound & Complete) (JAR'08, LICS'12, JAR'17)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations* **or** *to discrete dynamics.*

Corollary (Complete Proof-theoretical Bridge)

proving continuous = proving hybrid = proving discrete



Outline

1. Differential Dynamic Logic
   - Semantics
   - Axiomatization
   - Relative Completeness / ODE
2. Proofs for Differential Equations
   - Differential Equation Axioms
   - Differential Invariants / Cuts / Ghosts
3. Completeness for Differential Equation Invariants
   - Derived Darboux
   - Semialgebraic Invariants
   - Real Induction
   - Local Progress
   - Completeness for Invariants
4. Summary

Differential Equation Axioms & Differential Axioms

DW $[x' = f(x) \,\&\, Q]Q$

DC $\big([x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x) \,\&\, Q \land C]P\big) \leftarrow [x' = f(x) \,\&\, Q]C$

DE $[x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x) \,\&\, Q][x' := f(x)]P$

DI $\big([x' = f(x) \,\&\, Q]P \leftrightarrow [?Q]P\big) \leftarrow [x' = f(x) \,\&\, Q](P)'$

DG $[x' = f(x) \,\&\, Q]P \leftrightarrow \exists y\, [x' = f(x), y' = a(x)y + b(x) \,\&\, Q]P$

DS $[x' = c() \,\&\, Q]P \leftrightarrow \forall t{\geq}0\, \big((\forall 0{\leq}s{\leq}t\, q(x{+}c()s)) \rightarrow [x := x{+}c()t]P\big)$

$+'$ $(e + k)' = (e)' + (k)'$

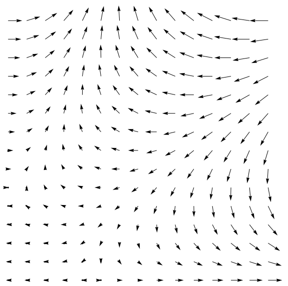
$\cdot'$ $(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$

$\circ'$ $[y := g(x)][y' := 1]\big((f(g(x)))' = (f(y))' \cdot (g(x))'\big)$

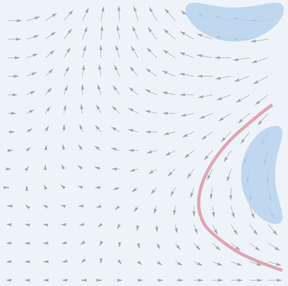
JAR'17

Differential Invariants for Differential Equations

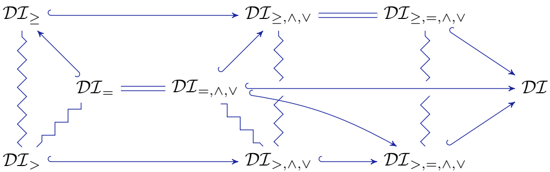
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability theory

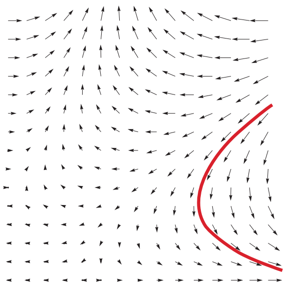
Math

Characteristic PDE

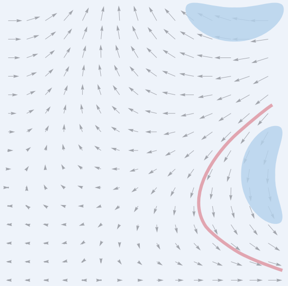
JLogComput'10,CAV'08,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17

Differential Invariants for Differential Equations

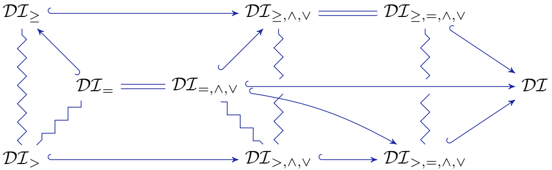
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability theory

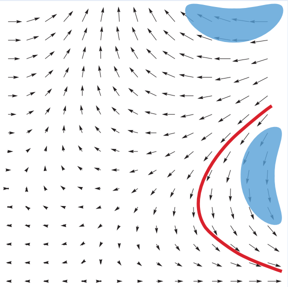
Math

Character-istic PDE

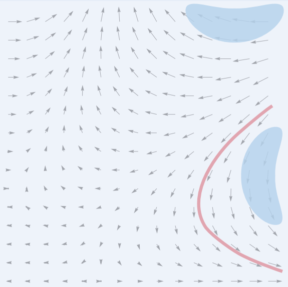
JLogComput'10,CAV'08,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17

Differential Invariants for Differential Equations

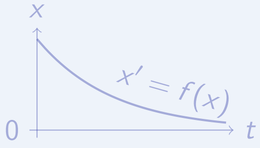
Differential Invariant

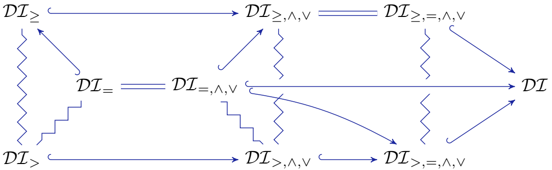


Differential Cut



Differential Ghost





Logic

Provability theory

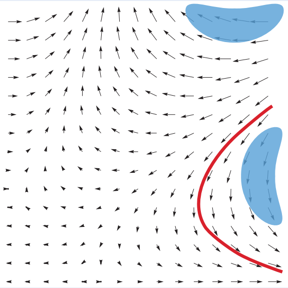
Math

Character-istic PDE

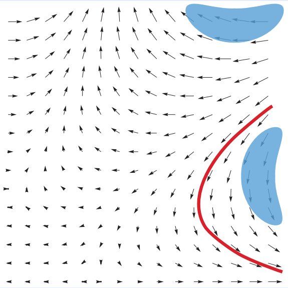
JLogComput'10,CAV'08,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17

Differential Invariants for Differential Equations

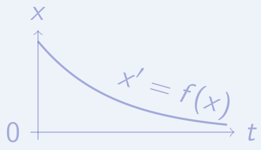
Differential Invariant

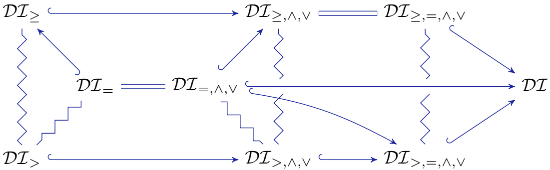


Differential Cut



Differential Ghost





Logic

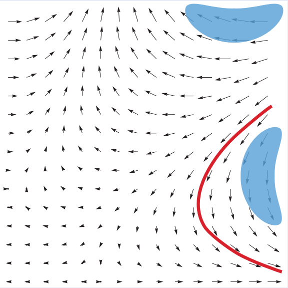
Provability theory

Math

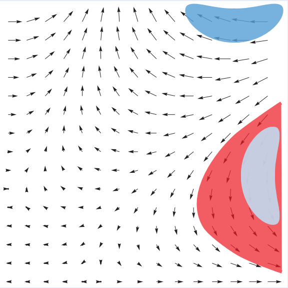
Characteristic PDE

JLogComput'10,CAV'08,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17

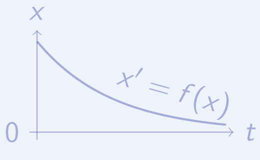
Differential Invariant

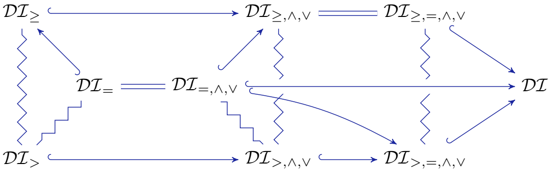


Differential Cut



Differential Ghost





Logic

Provability theory

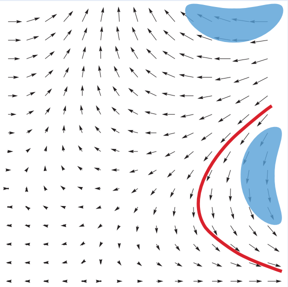
Math

Characteristic PDE

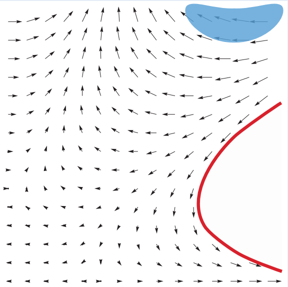
JLogComput'10,CAV'08,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17

Differential Invariants for Differential Equations

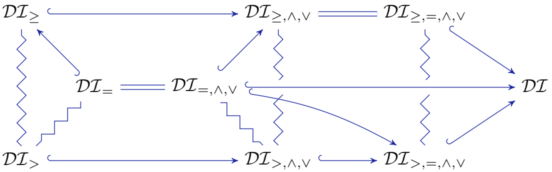
Differential Invariant



Differential Cut



Differential Ghost



Logic

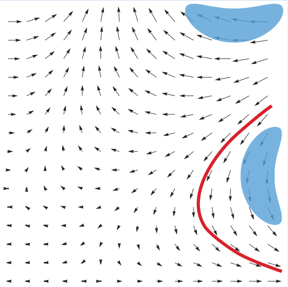
Provability theory

Math

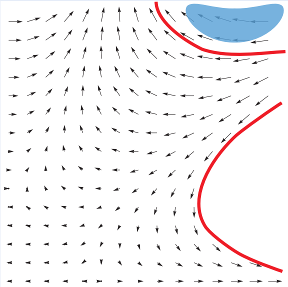
Characteristic PDE

JLogComput'10,CAV'08,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17

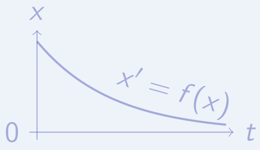
Differential Invariant

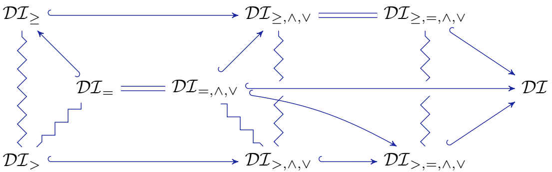


Differential Cut



Differential Ghost





Logic

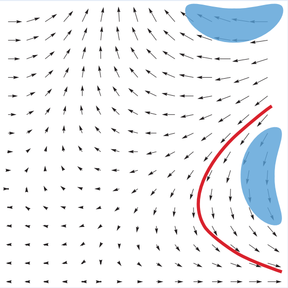
Provability theory

Math

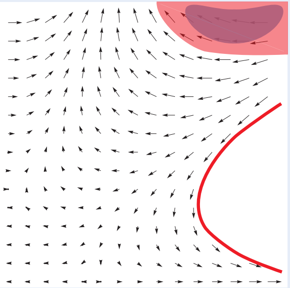
Characteristic PDE

JLogComput'10,CAV'08,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17

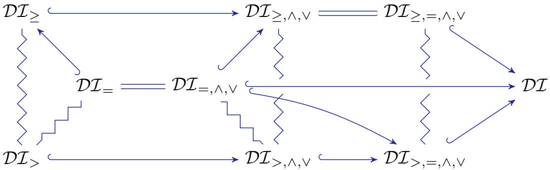
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability theory

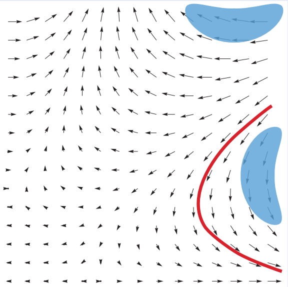
Math

Characteristic PDE

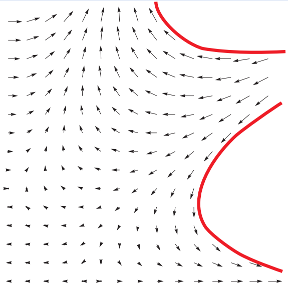
JLogComput'10,CAV'08,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17

Differential Invariants for Differential Equations

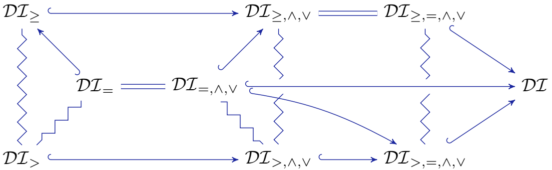
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability theory

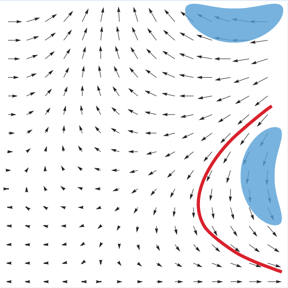
Math

Character-istic PDE

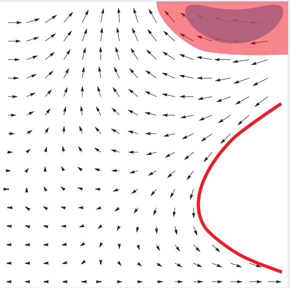
JLogComput'10,CAV'08,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17

Differential Invariants for Differential Equations

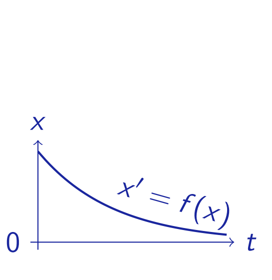
Differential Invariant

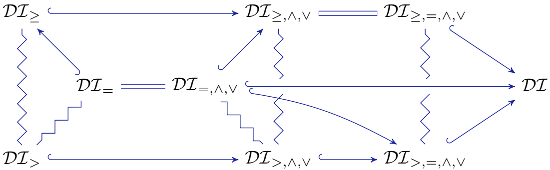


Differential Cut



Differential Ghost





Logic

Provability theory

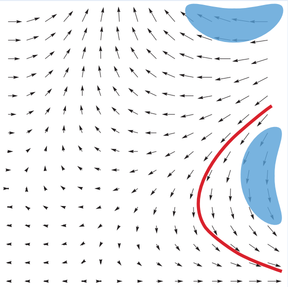
Math

Character-istic PDE

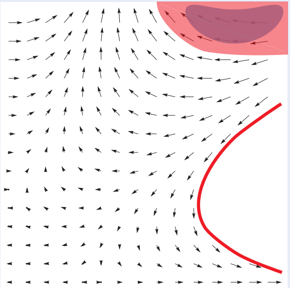
JLogComput'10,CAV'08,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17

Differential Invariants for Differential Equations

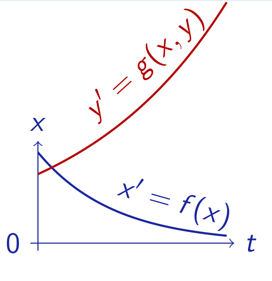
Differential Invariant

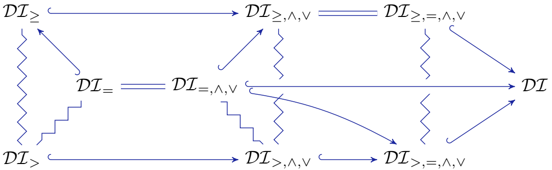


Differential Cut



Differential Ghost





Logic

Provability theory

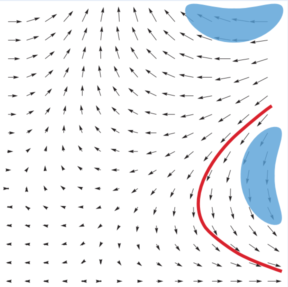
Math

Character-istic PDE

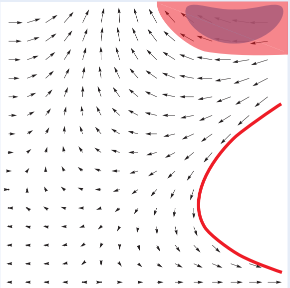
JLogComput'10,CAV'08,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17

Differential Invariants for Differential Equations

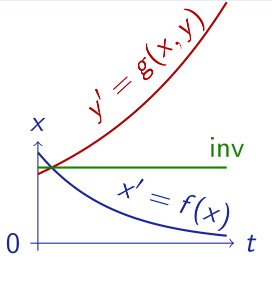
Differential Invariant

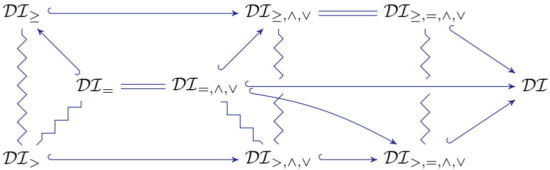


Differential Cut



Differential Ghost





Logic

Provability theory

Math

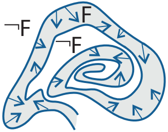
Character-istic PDE

JLogComput'10,CAV'08,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17

Differential Invariants for Differential Equations

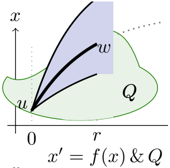
Differential Invariant

$$\frac{Q \vdash [x' := f(x)]{\color{red}(P)'}}{P \vdash [x' = f(x)\,\&\,Q]P}$$



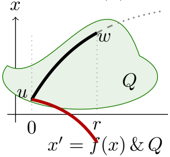
Differential Cut

$$\frac{P \vdash [x' = f(x)\,\&\,Q]{\color{red}C} \qquad P \vdash [x' = f(x)\,\&\,Q \land {\color{red}C}]P}{P \vdash [x' = f(x)\,\&\,Q]P}$$



Differential Ghost

$$\frac{P \leftrightarrow \exists y\, {\color{green}G} \qquad {\color{green}G} \vdash [x' = f(x), {\color{red}y' = g(x,y)}\,\&\,Q]{\color{green}G}}{P \vdash [x' = f(x)\,\&\,Q]P}$$



JLogComput'10,LMCS'12, LICS'12,JAR'17

Differential Invariants for Differential Equations

Differential Invariant

$$\frac{Q \vdash [x' := f(x)](P)'}{P \vdash [x' = f(x) \,\&\, Q]P}$$

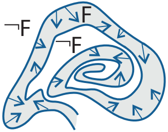
Differential Cut

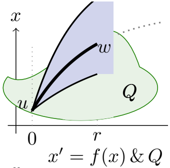
$$\frac{P \vdash [x' = f(x) \,\&\, Q]C \quad P \vdash [x' = f(x) \,\&\, Q \wedge C]P}{P \vdash [x' = f(x) \,\&\, Q]P}$$

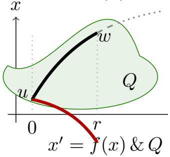
Differential Ghost

$$\frac{P \leftrightarrow \exists y\, G \quad G \vdash [x' = f(x), y' = g(x,y) \,\&\, Q]G}{P \vdash [x' = f(x) \,\&\, Q]P}$$

DI $\prec$ DI+DC $\prec$ DI+DC+DG deductive strength







JLogComput'10,LMCS'12, LICS'12,JAR'17

Differential Invariants for Differential Equations

Differential Invariant

$$\frac{Q \vdash [x' := f(x)](P)'}{P \vdash [x' = f(x) \,\&\, Q]P}$$

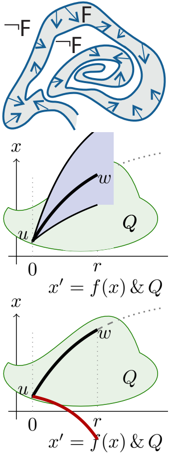
Differential Cut

$$\frac{P \vdash [x' = f(x) \,\&\, Q]C \qquad P \vdash [x' = f(x) \,\&\, Q \land C]P}{P \vdash [x' = f(x) \,\&\, Q]P}$$

Differential Ghost

$$\frac{P \leftrightarrow \exists y\, G \qquad G \vdash [x' = f(x), y' = g(x,y) \,\&\, Q]G}{P \vdash [x' = f(x) \,\&\, Q]P}$$

if new $y' = g(x,y)$ has a global solution



JLogComput'10,LMCS'12, LICS'12,JAR'17

Outline

Differential Equation Axiomatization

Theorem (Algebraic Completeness) (LICS'18)

dL *calculus is a sound & complete axiomatization of algebraic invariants of polynomial differential equations, which are decidable*

Theorem (Semialgebraic Completeness) (LICS'18)

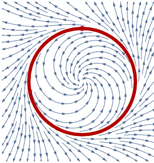
dL *calculus with RI is a sound & complete axiomatization of semialgebraic invariants of differential equations, which are decidable*

ODE Axiomatization: Derived Darboux Rules

Gaston Darboux 1878

Darboux equalities are DG

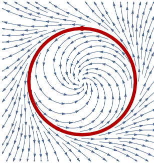
$$\frac{Q \vdash p' = gp}{p = 0 \vdash [x' = f(x) \,\&\, Q]p = 0} \quad (g \in \mathbb{R}[x])$$

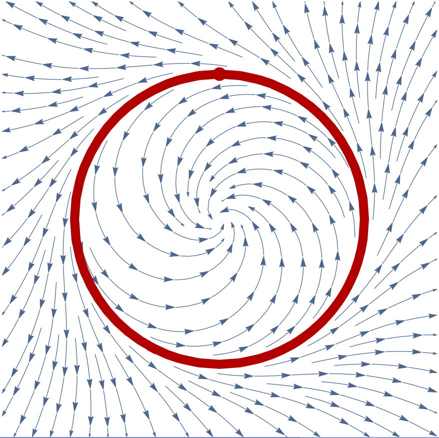


ODE Axiomatization: Derived Darboux Rules

Darboux equalities are DG

$$\frac{Q \vdash p' = gp}{p = 0 \vdash [x' = f(x) \,\&\, Q]p = 0} \quad (g \in \mathbb{R}[x])$$



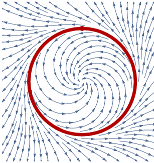


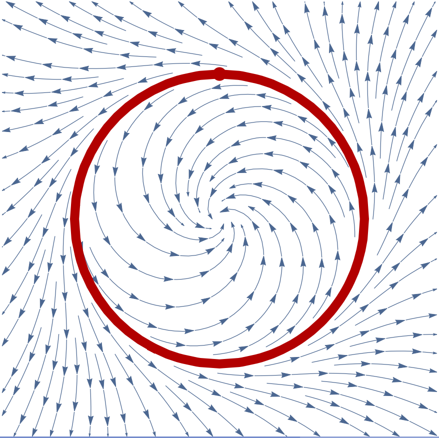
$$\frac{\vdash 2xx' + 2yy' = \qquad (x^2+y^2-1)}{.. \vdash \begin{bmatrix} x' = -y-x+x^3+xy^2 \\ y' = x-y+x^2y+y^3 \end{bmatrix} x^2+y^2-1=0}$$

ODE Axiomatization: Derived Darboux Rules

Darboux equalities are DG

$$\frac{Q \vdash p' = gp}{p = 0 \vdash [x' = f(x) \,\&\, Q]p = 0} \quad (g \in \mathbb{R}[x])$$



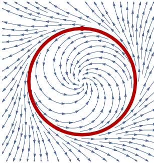


$$\frac{\vdash 2xx' + 2yy' = 2(x^2+y^2)(x^2+y^2-1)}{.. \vdash \begin{bmatrix} x' = -y - x + x^3 + xy^2 \\ y' = x - y + x^2y + y^3 \end{bmatrix} x^2+y^2-1=0}$$

ODE Axiomatization: Derived Darboux Rules

Darboux equalities are DG

$$\frac{Q \vdash p' = gp}{p = 0 \vdash [x' = f(x) \,\&\, Q]p = 0} \quad (g \in \mathbb{R}[x])$$

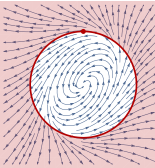


Proof Idea.

1. DG counterweight $y' = -gy$ to reduce $p = 0$ to $py = 0 \wedge y \neq 0$.
2. DG counter-counterweight $z' = gz$ to reduce $y \neq 0$ to $yz = 1$.
3. $py = 0$ and $yz = 1$ are now differential invariants by construction. □

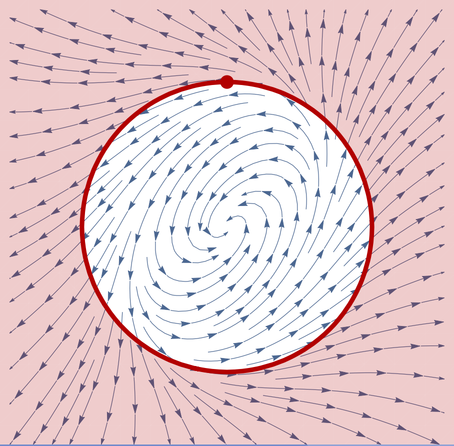
ODE Axiomatization: Derived Darboux Rules

Thomas Hakon Grönwall 1919



Darboux inequalities are DG

$$\frac{Q \vdash p' \geq gp}{p \gtrsim 0 \vdash [x' = f(x) \,\&\, Q] p \gtrsim 0} \quad (g \in \mathbb{R}[x])$$

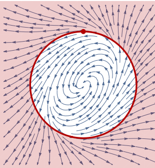


$$\frac{\vdash 2xx' + 2yy' \geq 2(x^2+y^2)(x^2+y^2-1)}{.. \vdash [x' = -y - x + x^3 + xy^2 + x, \; y' = x - y + x^2y + y^3]\, x^2+y^2-1 \geq 0}$$

ODE Axiomatization: Derived Darboux Rules

Darboux inequalities are DG

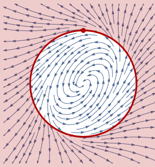
$$\frac{Q \vdash p' \geq gp}{p \gtrsim 0 \vdash [x' = f(x) \,\&\, Q] p \gtrsim 0} \quad (g \in \mathbb{R}[x])$$



Proof Idea.

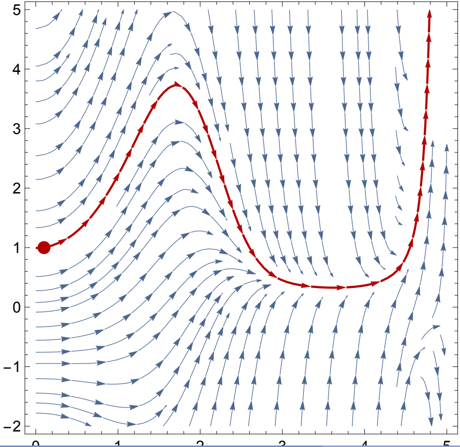
1. DG counterweight $y' = -gy$ to reduce $p \gtrsim 0$ to $py \gtrsim 0 \land y > 0$.
2. DG counter-counterweight $z' = \frac{g}{2} z$ to reduce $y > 0$ to $yz^2 = 1$.
3. $yz^2 = 1$ and (after DC with $y > 0$) $py \gtrsim 0$ are differential invariants by construction as $(py)' = p'y - gyp \geq 0$ from premise since $y > 0$. □

ODE Axiomatization: Derived Darboux Rules



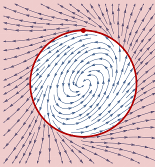
Darboux inequalities are DG

$$\frac{Q \vdash p' \geq gp}{p \gtrsim 0 \vdash [x' = f(x) \,\&\, Q]p \gtrsim 0} \quad (g \in \mathbb{R}[x])$$



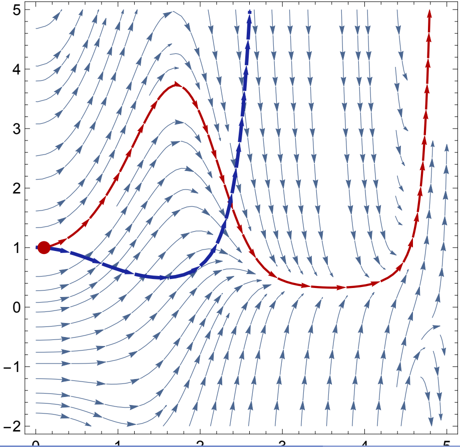
$$\frac{x' \geq (-t^3 + u - 1)x}{x \geq 0 \vdash \left[\begin{array}{l} x' = -t^3x + (u-1)x + t \\ u' = u \\ t' = 1 \end{array}\right] x \geq 0}$$

ODE Axiomatization: Derived Darboux Rules



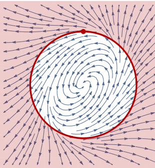
Darboux inequalities are DG

$$\frac{Q \vdash p' \geq gp}{p \gtrsim 0 \vdash [x' = f(x) \,\&\, Q]p \gtrsim 0} \quad (g \in \mathbb{R}[x])$$



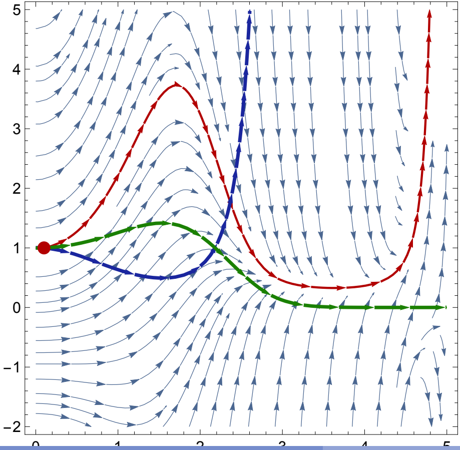
$$\frac{x' \geq (-t^3 + u - 1)x}{x \geq 0 \vdash \begin{bmatrix} x' = -t^3x + (u-1)x + t \\ u' = u \\ t' = 1 \\ y' = -(-t^3 + u - 1)y \end{bmatrix} x \geq 0}$$

$xy \geq 0 \leftarrow t \geq 0$



Darboux inequalities are DG

$$\frac{Q \vdash p' \geq gp}{p \gtrsim 0 \vdash [x' = f(x) \,\&\, Q]p \gtrsim 0} \quad (g \in \mathbb{R}[x])$$



$$\frac{x' \geq (-t^3 + u - 1)x}{x \geq 0 \vdash \big[x' = -t^3 x + (u-1)x + t,\; u' = u,\; t' = 1,\; y' = -(-t^3 + u - 1)y,\; z' = \frac{-t^3+u-1}{2} z\big]\; x \geq 0}$$

$xy \geq 0 \leftarrow t \geq 0$

$yz^2 = 1$

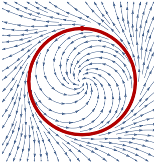
Darboux Inequalities are Differential Ghosts: Details

$$
\cfrac{
  \cfrac{
    \cfrac{
      \cfrac{*}{Q \vdash (-gy)z^2 + y(2z(\frac{g}{2}z)) = 0}
    }{yz^2 = 1 \vdash [x' = f(x), y' = -gy, z' = \frac{g}{2}z \,\&\, Q]yz^2 = 1}\ \text{DI}
  }{y > 0 \vdash \exists z\, [x' = f(x), y' = -gy, z' = \frac{g}{2}z \,\&\, Q]\, y > 0}\ \text{M,}\exists\text{R}
}{y > 0 \vdash [x' = f(x), y' = -gy \,\&\, Q]\, y > 0}\ \text{DG}
$$

$$
\cfrac{
  \cfrac{
    \cfrac{
      \cfrac{
        \cfrac{Q \vdash p' \geq gp \qquad \cfrac{*}{p' \geq gp, y > 0 \vdash p'y - gyp \geq 0}}{Q, y > 0 \vdash p'y - gyp \geq 0}\ \text{cut}
      }{p \gtrsim 0, y > 0 \vdash [x' = f(x), y' = -gy \,\&\, Q \wedge y > 0] py \gtrsim 0 \quad \triangleright}\ \text{DI}
    }{p \gtrsim 0, y > 0 \vdash [x' = f(x), y' = -gy \,\&\, Q](y > 0 \wedge py \gtrsim 0)}\ \text{DC}
  }{p \gtrsim 0 \vdash \exists y\, [x' = f(x), y' = -gy \,\&\, Q] p \gtrsim 0}\ \text{M,}\exists\text{R}
}{p \gtrsim 0 \vdash [x' = f(x) \,\&\, Q] p \gtrsim 0}\ \text{DG}
$$

P.S. $z' = \frac{g}{2}z$ superfluous for open inequalities $p > 0$ and $p \neq 0$.

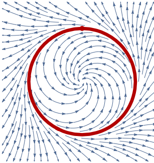
ODE Axiomatization: Derived Darboux Rules



Vectorial Darboux are VDG

$$\frac{Q \vdash \mathbf{p}' = G\mathbf{p}}{\mathbf{p} = 0 \vdash [x' = f(x) \,\&\, Q]\mathbf{p} = 0} \quad (G \in \mathbb{R}[x]^{n \times n})$$

ODE Axiomatization: Derived Darboux Rules



Vectorial Darboux are VDG

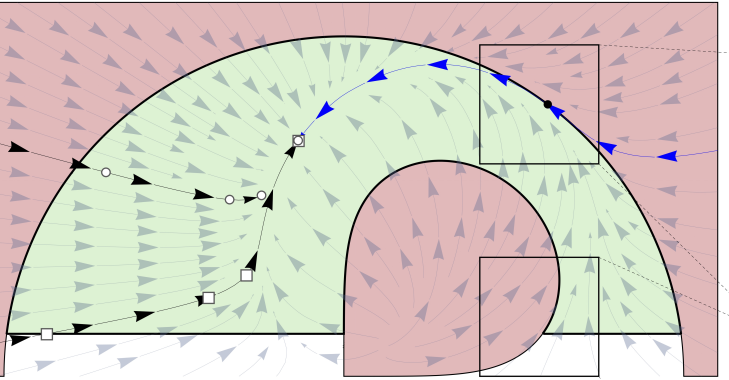
$$\frac{Q \vdash \mathbf{p}' = G\mathbf{p}}{\mathbf{p} = 0 \vdash [x' = f(x) \,\&\, Q]\mathbf{p} = 0} \quad (G \in \mathbb{R}[x]^{n \times n})$$

Proof Idea.

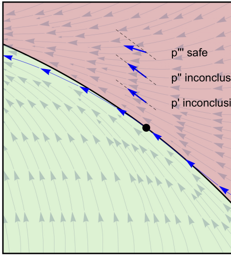
1. DG counterweight $\mathbf{y}' = -G\mathbf{y}$ to change $\mathbf{p} = 0$ to $\mathbf{p} \cdot \mathbf{y} = 0$.
2. But: $\mathbf{p} \cdot \mathbf{y} = 0 \not\Rightarrow \mathbf{p} = 0$ even if $\mathbf{y} \neq 0$.
3. Redo: time-varying orthogonal basis $Y' = -YG$ of DGs with $Y\mathbf{p} = 0$.
4. $Y\mathbf{p} = 0 \Rightarrow \mathbf{p} = 0$ if $\det Y \neq 0$. $\quad Y\,\mathrm{adj}(Y) = \det(Y)I$
5. DC $\det Y \neq 0$ which proves by dbx using Abel-Liouville identity $\det(Y)' = \mathrm{tr}(\mathrm{adj}(Y)Y') = \mathrm{tr}\left(\mathrm{adj}(Y)(-YG)\right) = -\mathrm{tr}(G)\det(Y)$
6. Continuous change of basis Y^{-1} such that $\mathbf{p}$ becomes constant.
7. Continuous change to new variables is sound by DG.

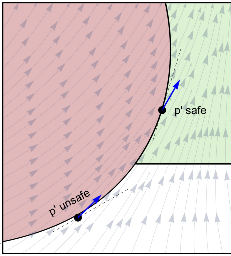
□

Time is defined so that motion looks simple ≈Poincaré

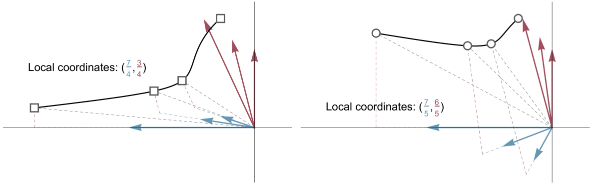


Proofs with higher Lie derivatives





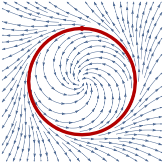
Sound and complete ODE invariance proofs



Proofs use continuously changing basis to keep invariants at constant local coordinates

Vectorial Darboux are VDG

$$\frac{Q \vdash \mathbf{p}' = G\mathbf{p}}{\mathbf{p} = 0 \vdash [x' = f(x) \,\&\, Q]\mathbf{p} = 0}$$

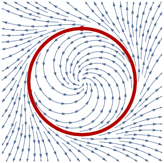


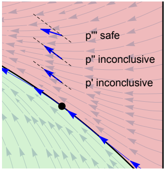
Vectorial Darboux are VDG

$$\frac{Q \vdash \mathbf{p}' = G\mathbf{p}}{\mathbf{p} = 0 \vdash [x' = f(x) \,\&\, Q]\mathbf{p} = 0}$$

Differential radical invariants are vdbx

$$\frac{\Gamma, Q \vdash \bigwedge_{i=0}^{N-1} p^{(i)} = 0 \quad Q \vdash p^{(N)} = \sum_{i=0}^{N-1} g_i p^{(i)}}{\Gamma \vdash [x' = f(x) \,\&\, Q]p = 0}$$





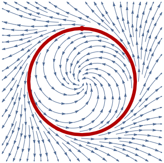
ODE Axiomatization: Derived Invariant Rules

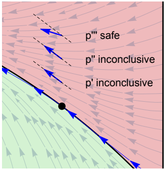
Vectorial Darboux are VDG

$$\frac{Q \vdash \mathbf{p}' = G\mathbf{p}}{\mathbf{p} = 0 \vdash [x' = f(x) \,\&\, Q]\mathbf{p} = 0}$$

Differential radical invariants are vdbx

$$\frac{\Gamma, Q \vdash \bigwedge_{i=0}^{N-1} p^{(i)} = 0 \quad Q \vdash p^{(N)} = \sum_{i=0}^{N-1} g_i p^{(i)}}{\Gamma \vdash [x' = f(x) \,\&\, Q]p = 0}$$





Proof Idea.

by vdbx with $G = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & 1 \\ g_0 & g_1 & \dots & g_{N-2} & g_{N-1} \end{pmatrix}$, $\mathbf{p} = \begin{pmatrix} p \\ p^{(1)} \\ p^{(2)} \\ \vdots \\ p^{(N-1)} \end{pmatrix}$

ODE Axiomatization: Derived Invariant Rules

Vectorial Darboux are VDG

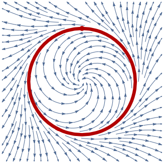
$$\frac{Q \vdash \mathbf{p}' = G\mathbf{p}}{\mathbf{p} = 0 \vdash [x' = f(x) \,\&\, Q]\mathbf{p} = 0}$$

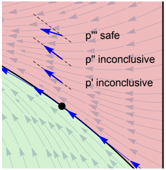
Differential radical invariants are vdbx

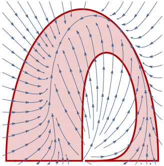
$$\frac{\Gamma, Q \vdash \bigwedge_{i=0}^{N-1} p^{(i)} = 0 \quad Q \vdash p^{(N)} = \sum_{i=0}^{N-1} g_i p^{(i)}}{\Gamma \vdash [x' = f(x) \,\&\, Q]p = 0}$$

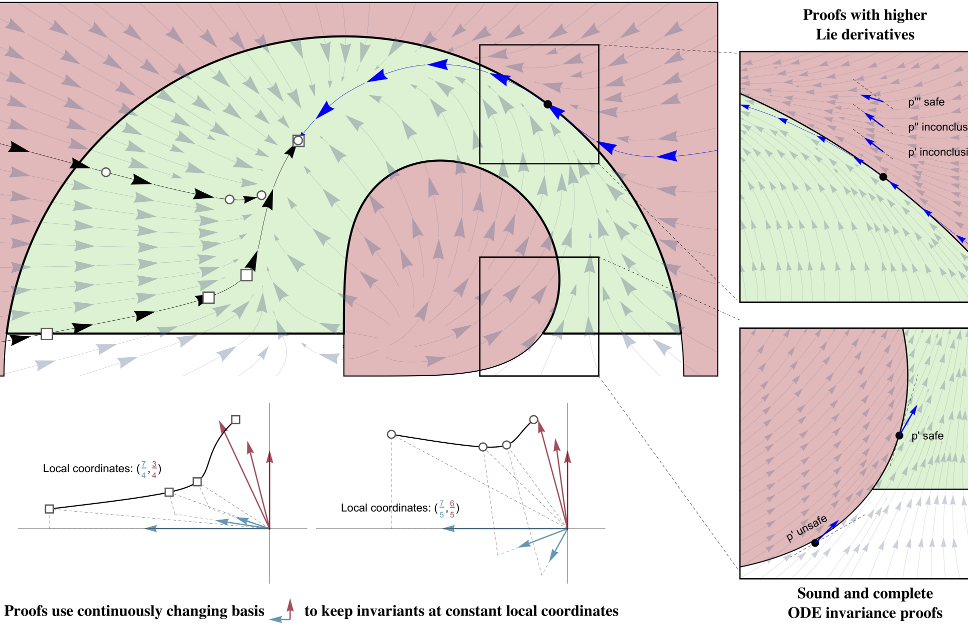
Semialgebraic invariants are derived

$$\frac{p{=}0 \vdash p'{\geq}0 \quad .. \quad p{=}0{\wedge}..{\wedge}p^{(N-2)}{=}0 \vdash p^{(N-1)}{\geq}0}{p \geq 0 \vdash [x' = f(x)]p \geq 0}$$









Proofs use continuously changing basis to keep invariants at constant local coordinates

ODE Axiomatization: Derived Semialgebraic Rules

Semialgebraic invariants are derived

$$\frac{P \vdash \bigwedge_{i=0}^{M} \big(\bigvee_{j=0}^{m(i)} p_{ij}{'^{*}}{=}0 \lor \bigvee_{j=0}^{n(i)} q_{ij}{'^{*}}{>}0 \big) \quad \neg P \vdash \bigwedge_{i=0}^{N} \big(\bigvee_{j=0}^{a(i)} r_{ij}{'^{*-}}{=}0 \lor \bigvee_{j=0}^{b(i)} s_{ij}{'^{*-}}{>}0 \big)}{P \vdash [x' = f(x)]P}$$

$$P \equiv \bigwedge_{i=0}^{M} \big(\bigvee_{j=0}^{m(i)} p_{ij} = 0 \lor \bigvee_{j=0}^{n(i)} q_{ij} > 0 \big) \quad \neg P \equiv \bigwedge_{i=0}^{N} \big(\bigvee_{j=0}^{a(i)} r_{ij} = 0 \lor \bigvee_{j=0}^{b(i)} s_{ij} > 0 \big)$$

$$p{'^{*}}{=}0 \equiv \bigwedge_{i=0}^{N-1} p^{(i)} = 0 \quad \text{where } p^{(N)} = \sum_{i=0}^{N-1} g_i p^{(i)}$$

$$q{'^{*}}{>}0 \equiv q \geq 0 \land \big(q = 0 \rightarrow q' \geq 0\big) \land \big(q = 0 \land q' = 0 \rightarrow q^{(2)} \geq 0\big) \land \dots$$
$$\land \big(q = 0 \land q' = 0 \land \dots \land q^{(N-2)} = 0 \rightarrow q^{(N-1)} > 0\big)$$

Definable $p{'^{*-}}$ for *all/most significant* Lie derivatives w.r.t. backwards ODE

ODE Axiomatization: Derived Semialgebraic Rules

Semialgebraic inva…

$P \vdash \bigwedge_{i=0}^{M} \big(\bigvee_{j=0}^{m(i)} p_{ij}'^{*}$ … $=0 \lor \bigvee_{j=0}^{b(i)} s_{ij}'^{*-}>0 \big)$

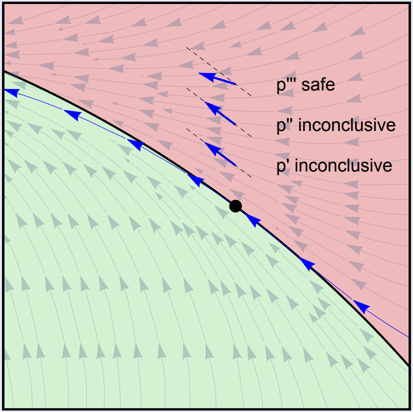
$P \equiv \bigwedge_{i=0}^{M} \big(\bigvee_{j=0}^{m(i)} p$ … $r_{ij} = 0 \lor \bigvee_{j=0}^{b(i)} s_{ij} > 0 \big)$

$p'^{*}=0 \equiv \bigwedge_{i=0}^{N-1} p^{(i)} =$ …

$q'^{*}>0 \equiv q \geq 0 \land \big($ … $\to q^{(2)} \geq 0 \big) \land \dots$

$\land \big(q = 0 \land q$ … $> 0 \big)$

Seriously?



Fortunately, it's just a derived rule!

Definable p'^{*-} for *all/most significant* Lie derivatives w.r.t. backwards ODE

Extended Axiomatization for Semialgebraics

Real Induction

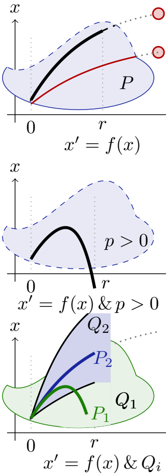
$$\frac{P \vdash \langle x'=f(x)\,\&\,P\rangle\circ \quad \neg P \vdash \langle x'=-f(x)\,\&\,\neg P\rangle\circ}{P \vdash [x'=f(x)]P}$$

Continuous Existence

$$p > 0 \rightarrow \langle x' = f(x)\,\&\,p > 0\rangle\circ$$

Unique Solutions

$$\langle x' = f(x)\,\&\,Q_1\rangle P_1 \wedge \langle x' = f(x)\,\&\,Q_2\rangle P_2 \\ \rightarrow \langle x' = f(x)\,\&\,Q_1 \wedge Q_2\rangle(P_1 \vee P_2)$$



Extended Axiomatization for Semialgebraics

Real Induction

$$\frac{P \vdash \langle x'=f(x) \,\&\, P\rangle\circ \quad \neg P \vdash \langle x'=-f(x) \,\&\, \neg P\rangle\circ}{P \vdash [x' = f(x)]P}$$

Continuous Existence

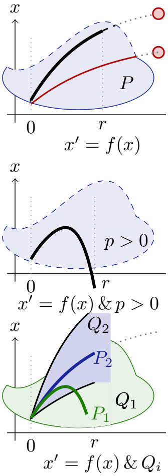
$$p > 0 \rightarrow \langle x' = f(x) \,\&\, p > 0\rangle\circ$$

Unique Solutions

$$\langle x' = f(x) \,\&\, Q_1\rangle P_1 \wedge \langle x' = f(x) \,\&\, Q_2\rangle P_2 \\ \rightarrow \langle x' = f(x) \,\&\, Q_1 \wedge Q_2\rangle(P_1 \vee P_2)$$

$P \vdash \langle x'=f(x) \,\&\, P\rangle\circ$ by Cont,Uniq for open P

$\neg P \vdash \langle x'=-f(x) \,\&\, \neg P\rangle\circ$ by Cont,Uniq for closed P



ODE Axiomatization: Derived Local Progress Rules

Equality Progress

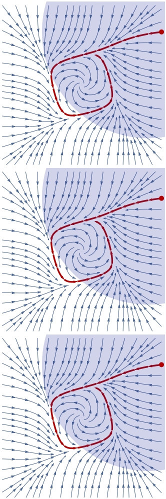
$$\big(p = 0 \rightarrow \langle x' = f(x) \,\&\, p = 0\rangle\circ\big) \leftarrow p'^{*} = 0$$

Inequality Progress

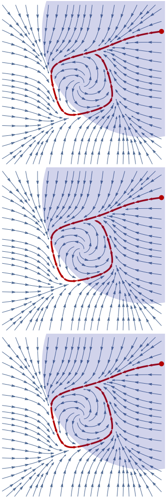
$$p > q \;\lor\; p = q \land \langle x' = f(x) \,\&\, p' \geq q'\rangle\circ \\ \rightarrow \langle x' = f(x) \,\&\, p \geq q\rangle\circ$$

Mixed Progress

$$\big(p{=}0 \rightarrow \langle x' = f(x) \,\&\, p{=}0 \lor q{>}0\rangle\circ\big) \leftarrow q'^{*} > 0$$



ODE Axiomatization: Derived Local Progress Rules



Equality Progress

$$\left(p = 0 \rightarrow \langle x' = f(x) \,\&\, p = 0 \rangle \circ\right) \leftarrow p'^{*} = 0$$

Inequality Progress

$$p > q \;\lor\; p = q \land \langle x' = f(x) \,\&\, p' \geq q' \rangle \circ \\ \rightarrow \langle x' = f(x) \,\&\, p \geq q \rangle \circ$$

Mixed Progress

$$\left(p{=}0 \rightarrow \langle x' = f(x) \,\&\, p{=}0 \lor q{>}0 \rangle \circ\right) \leftarrow q'^{*} > 0$$

Relate most significant Lie derivatives from sAI
to local progress in rI, stitch together by Cont,Uniq

Differential Equation Axiomatization

Theorem (Algebraic Completeness) (LICS'18)

dL *calculus is a sound & complete axiomatization of algebraic invariants of polynomial differential equations, which are decidable*

Theorem (Semialgebraic Completeness) (LICS'18)

dL *calculus with RI is a sound & complete axiomatization of semialgebraic invariants of differential equations, which are decidable*

Differential Equation Axiomatization

Theorem (Algebraic Completeness) (LICS'18)

dL *calculus is a sound & complete axiomatization of algebraic invariants of polynomial differential equations, which are decidable with a derived axiom (on open Q for completeness):*

$$(DRI)\quad [x' = f(x)\,\&\,Q]p = 0 \leftrightarrow \big(Q \to p'^{*} = 0\big)$$

Theorem (Semialgebraic Completeness) (LICS'18)

dL *calculus with RI is a sound & complete axiomatization of semialgebraic invariants of differential equations, which are decidable with a derived rule:*

$$(sAI)\quad \frac{\dots p'^{*} = 0 \dots p'^{*} > 0 \dots}{P \vdash [x' = f(x)\,\&\,Q]P}$$

Definable p'^{*} is short for *all/most significant* Lie derivatives w.r.t. ODE

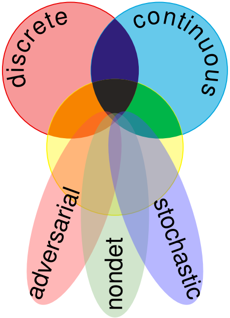
Outline

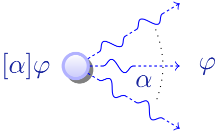
1. Differential Dynamic Logic
   - Semantics
   - Axiomatization
   - Relative Completeness / ODE
2. Proofs for Differential Equations
   - Differential Equation Axioms
   - Differential Invariants / Cuts / Ghosts
3. Completeness for Differential Equation Invariants
   - Derived Darboux
   - Semialgebraic Invariants
   - Real Induction
   - Local Progress
   - Completeness for Invariants
4. Summary

Logical Foundation for Differential Equation Invariants

differential dynamic logic

dL = DL + HP





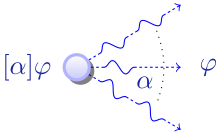
1. Poincaré: qualitative ODE
2. Complete axiomatization
3. Algebraic ODE invariants
4. Semialgebraic ODE invariants
5. Algebraic hybrid systems
6. Local ODE progress
7. Decidable by dL proof
8. Uniform substitution axioms

1. Differential invariants
2. Differential cuts
3. Differential ghosts
4. Real induction
5. Continuous existence
6. Unique solutions

Impressive power of differential ghosts

differential dynamic logic

dL = DL + HP



1. Poincaré: qualitative ODE
2. Complete axiomatization
3. Algebraic ODE invariants
4. Semialgebraic ODE invariants
5. Algebraic hybrid systems
6. Local ODE progress
7. Decidable by dL proof
8. Uniform substitution axioms

1. MVT
2. Prefix
3. Picard-Lind
4. $\mathbb{R}$-complete
5. Existence
6. Uniqueness

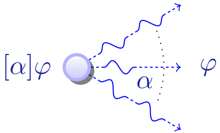
1. Differential invariants
2. Differential cuts
3. Differential ghosts
4. Real induction
5. Continuous existence
6. Unique solutions

Impressive power of differential ghosts

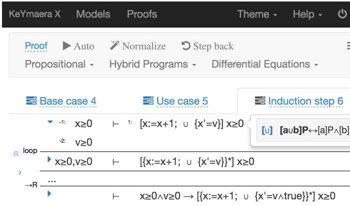
Logical Foundation for Differential Equation Invariants

differential dynamic logic

dL = DL + HP



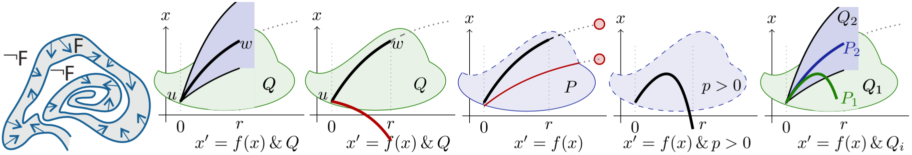
KeYmaera X

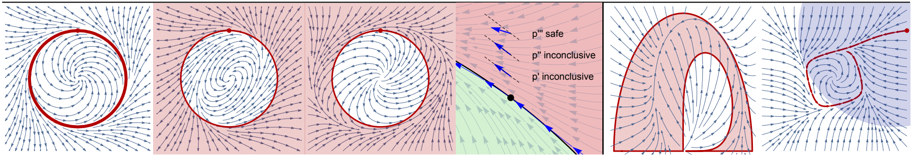


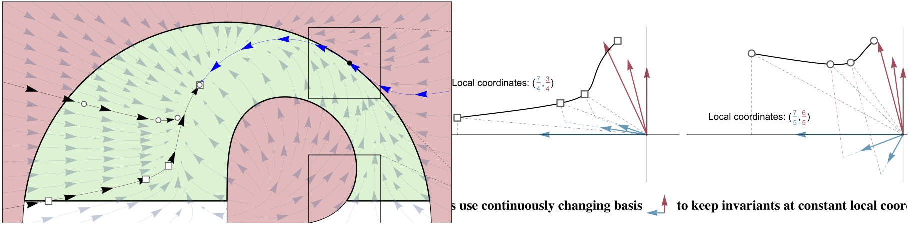
1. Poincaré: qualitative ODE
2. Complete axiomatization
3. Algebraic ODE invariants
4. Semialgebraic ODE invariants
5. Algebraic hybrid systems
6. Local ODE progress
7. Decidable by dL proof
8. Uniform substitution axioms

Impressive power of differential ghosts

Differential Equation Axiomatization vs. Derived Rules







A. Platzer. *Logical Foundations of Cyber-Physical Systems.* Springer 2018

I Part: Elementary Cyber-Physical Systems

1. Differential Equations & Domains
2. Choice & Control
3. Safety & Contracts
4. Dynamical Systems & Dynamic Axioms
5. Truth & Proof
6. Control Loops & Invariants
7. Events & Responses
8. Reactions & Delays

II Part: Differential Equations Analysis

9. Differential Equations & Differential Invariants
10. Differential Equations & Proofs
11. Ghosts & Differential Ghosts
12. Differential Invariants & Proof Theory

III Part: Adversarial Cyber-Physical Systems

13-16. Hybrid Systems & Hybrid Games

IV Part: Comprehensive CPS Correctness

images/lfcps-flyer.png

André Platzer and Yong Kiam Tan.
Differential equation axiomatization: The impressive power of differential ghosts.
In Anuj Dawar and Erich Grädel, editors, *LICS*, New York, 2018. ACM.
doi:10.1145/3209108.3209147.

André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.
doi:10.1007/s10817-008-9103-8.

André Platzer.
Logics of dynamical systems.
In LICS [12], pages 13–24.
doi:10.1109/LICS.2012.13.

André Platzer.
A complete uniform substitution calculus for differential dynamic logic.

J. Autom. Reas., 59(2):219–265, 2017.
doi:10.1007/s10817-016-9385-1.

André Platzer.
The complete proof theory of hybrid systems.
In LICS [12], pages 541–550.
doi:10.1109/LICS.2012.64.

André Platzer.
A uniform substitution calculus for differential dynamic logic.
In Amy Felty and Aart Middeldorp, editors, *CADE*, volume 9195 of *LNCS*, pages 467–481, Berlin, 2015. Springer.
doi:10.1007/978-3-319-21401-6_32.

André Platzer.
Differential-algebraic dynamic logic for differential-algebraic programs.
J. Log. Comput., 20(1):309–352, 2010.
doi:10.1093/logcom/exn070.

André Platzer and Edmund M. Clarke.
Computing differential invariants of hybrid systems as fixedpoints.

Form. Methods Syst. Des., 35(1):98–120, 2009.
Special issue for selected papers from CAV'08.
doi:10.1007/s10703-009-0079-8.

André Platzer.
The structure of differential invariants and differential cut elimination.
Log. Meth. Comput. Sci., 8(4:16):1–38, 2012.
doi:10.2168/LMCS-8(4:16)2012.

André Platzer.
A differential operator approach to equational differential invariants.
In Lennart Beringer and Amy Felty, editors, *ITP*, volume 7406 of *LNCS*, pages 28–48, Berlin, 2012. Springer.
doi:10.1007/978-3-642-32347-8_3.

André Platzer.
Logical Foundations of Cyber-Physical Systems.
Springer, Switzerland, 2018.
URL: http://www.springer.com/978-3-319-63587-3.

Logic in Computer Science (LICS), 2012 27th Annual IEEE Symposium on, Los Alamitos, 2012. IEEE.