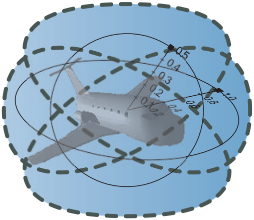
Differential Equation Invariance Axiomatization

André Platzer Yong Kiam Tan

Carnegie Mellon University

J. ACM **67**(1), 2020.



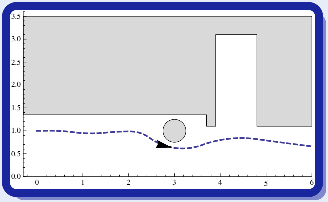
Outline

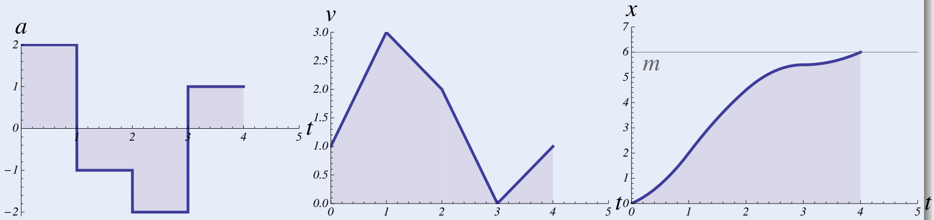
Hybrid Systems: Example Robot Control

Challenge (Hybrid Systems)

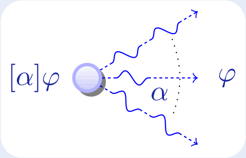
Fixed law describing state evolution with both

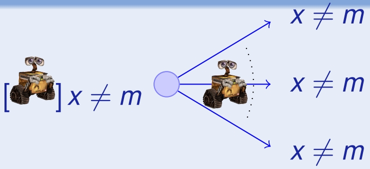
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)





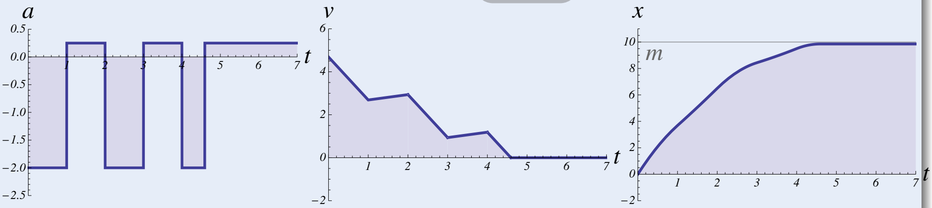
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)





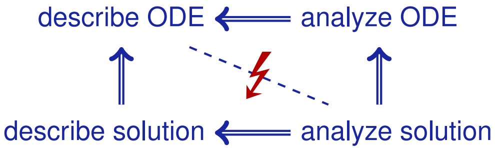
$$\underbrace{x \neq m \wedge b > 0}_{\text{init}} \rightarrow \Big[\big((\mathtt{if}(\mathrm{SB}(x,m))\, a := -b)\ ;\ x' = v, v' = a\big)^*\Big]\underbrace{x \neq m}_{\text{post}}$$

all runs



Contributions: Differential Equation Axiomatization

- 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
5. Decide invariance by proof

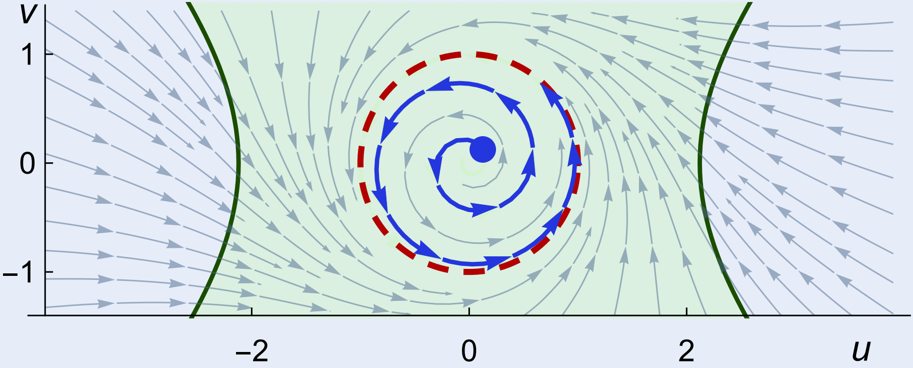
Outline

1. Differential Dynamic Logic
   - Syntax
   - Axiomatization
   - Relative Completeness / ODE
2. Proofs for Differential Equations
   - Differential Invariants / Cuts / Ghosts
3. Completeness for Differential Equation Invariants
   - Darboux are Differential Ghosts
   - Derived Differential Radical Invariants
   - Real Induction
   - Derived Local Progress
   - Completeness for Invariants
   - Completeness for Noetherian Functions
4. Summary

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

$$u^2 \le v^2 + \frac{9}{2} \to [u' = -v + \frac{u}{4}(1 - u^2 - v^2), v' = u + \frac{v}{4}(1 - u^2 - v^2)]\, u^2 \le v^2 + \frac{9}{2}$$

$$u^2 + v^2 = 1 \to [u' = -v + \frac{u}{4}(1 - u^2 - v^2), v' = u + \frac{v}{4}(1 - u^2 - v^2)]\, u^2 + v^2 = 1$$



Differential Dynamic Logic dL: Syntax

Definition (Hybrid program α)

$$\alpha, \beta \ ::= \ x := f(x) \mid ?Q \mid x' = f(x) \,\&\, Q \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^*$$

Definition (dL Formula P)

$$P, Q \ ::= \ e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid [\alpha] P \mid \langle \alpha \rangle P$$

JAR'08,LICS'12,JAR'17

Differential Dynamic Logic dL: Syntax

Discrete Assign | Test Condition | Differential Equation | Nondet. Choice | Seq. Compose | Nondet. Repeat

Definition (Hybrid program α)

$$\alpha, \beta ::= x := f(x) \mid ?Q \mid x' = f(x) \,\&\, Q \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^*$$

Definition (dL Formula P)

$$P, Q ::= e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid [\alpha]P \mid \langle\alpha\rangle P$$

All Reals | Some Reals | All Runs | Some Runs

JAR'08,LICS'12,JAR'17

equations of truth

[:=] $[x := e]p(x) \leftrightarrow p(e)$

[?] $[?Q]P \leftrightarrow (Q \rightarrow P)$

[′] $[x' = f(x)]p(x) \leftrightarrow \forall t \geq 0\, [x := y(t)]p(x)$ $\qquad (y'(t) = f(y))$

[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$

[;] $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

[*] $[\alpha^*]P \leftrightarrow P \wedge [\alpha][\alpha^*]P$

K $[\alpha](P \rightarrow Q) \rightarrow ([\alpha]P \rightarrow [\alpha]Q)$

I $[\alpha^*](P \rightarrow [\alpha]P) \rightarrow (P \rightarrow [\alpha^*]P)$

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

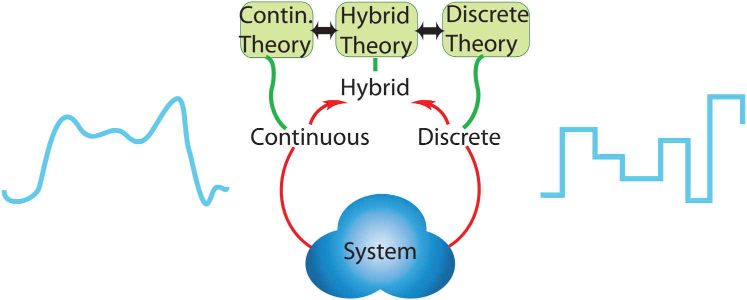
Complete Proof Theory of Hybrid Systems

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*** *relative to discrete dynamics.*

Corollary (Complete Proof-theoretical Bridge)

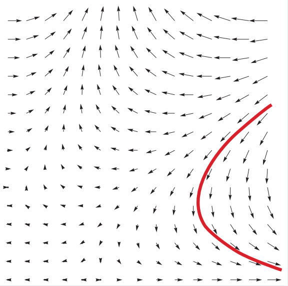
proving continuous = proving hybrid = proving discrete



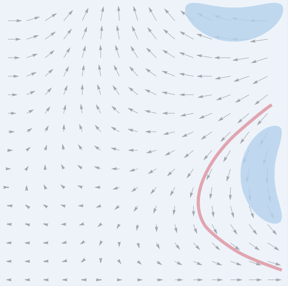
Outline

Differential Invariants for Differential Equations

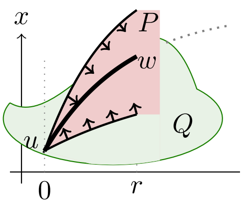
Differential Invariant



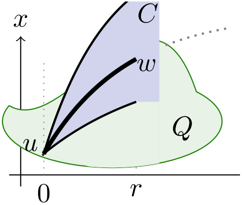
Differential Cut



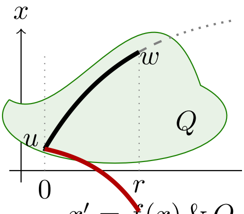
Differential Ghost



$x' = f(x)\,\&\,Q$

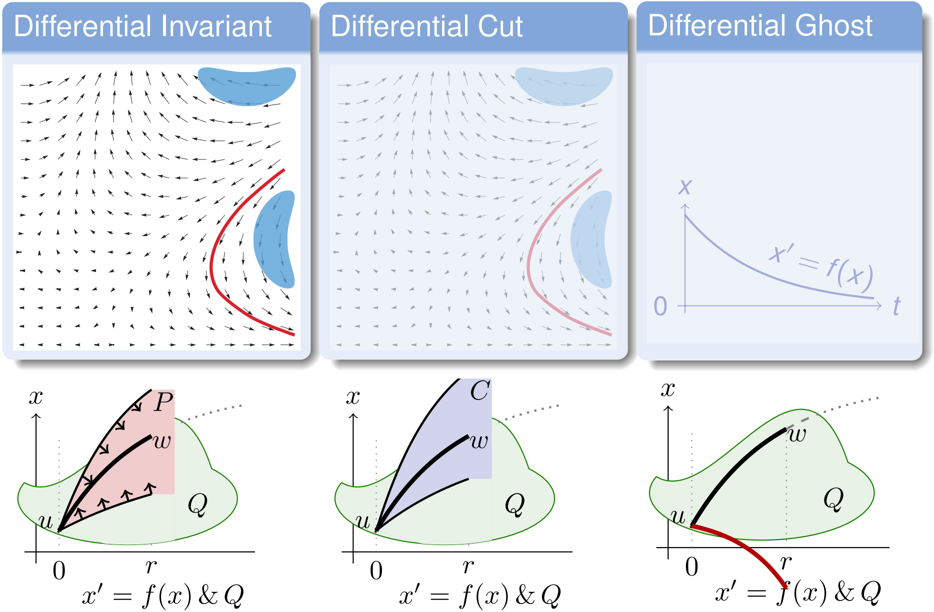


$x' = f(x)\,\&\,Q$



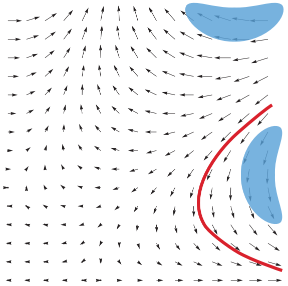
$x' = f(x)\,\&\,Q$

Differential Invariants for Differential Equations

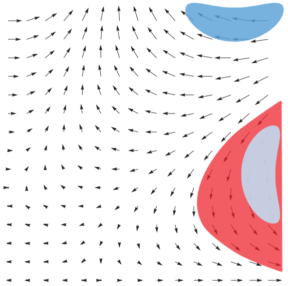


Differential Invariants for Differential Equations

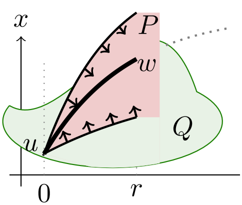
Differential Invariant



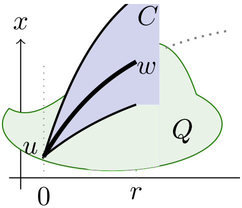
Differential Cut



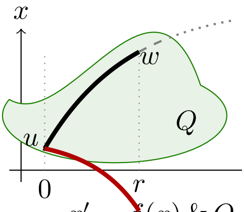
Differential Ghost



$x' = f(x) \,\&\, Q$

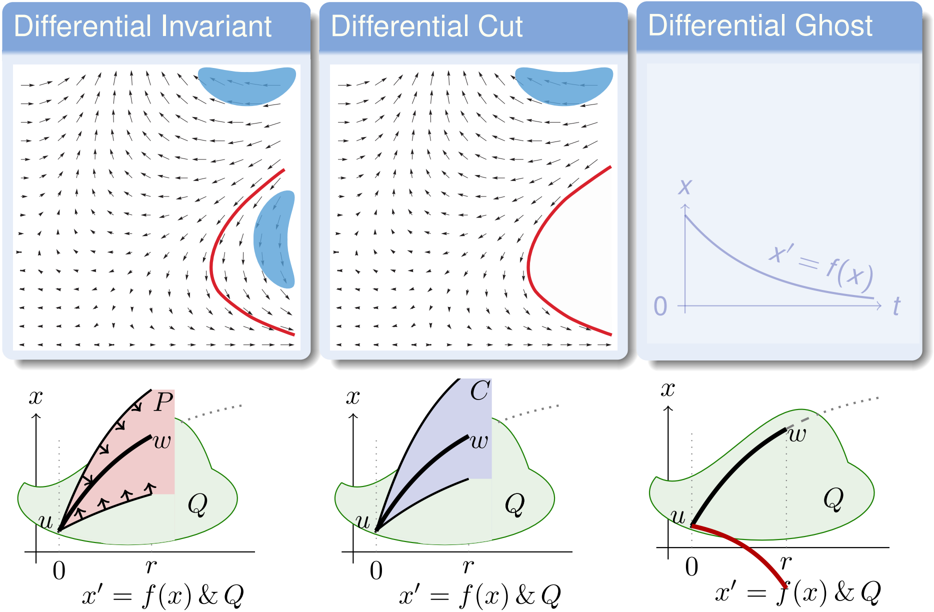


$x' = f(x) \,\&\, Q$



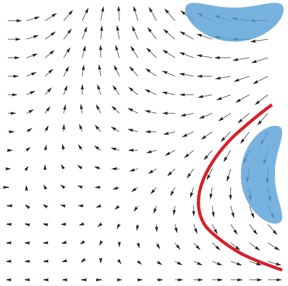
$x' = f(x) \,\&\, Q$

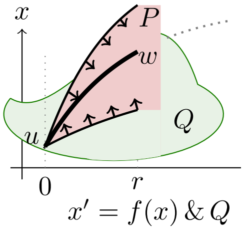
Differential Invariants for Differential Equations



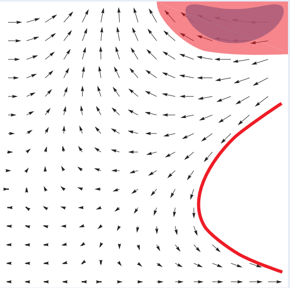
Differential Invariants for Differential Equations

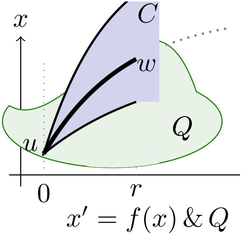
Differential Invariant



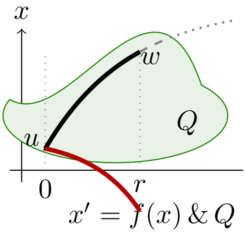


Differential Cut



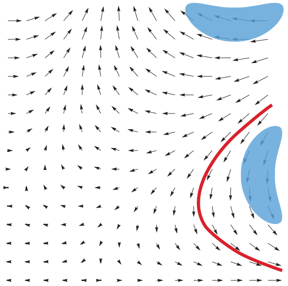


Differential Ghost

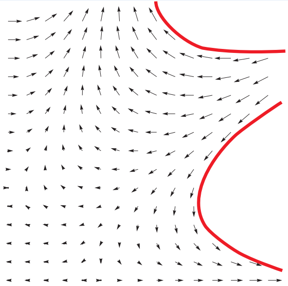


Differential Invariants for Differential Equations

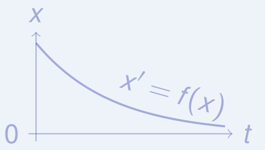
Differential Invariant

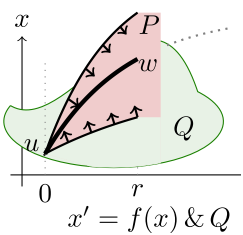


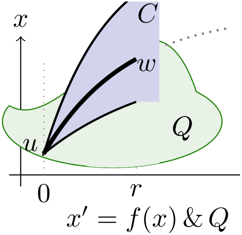
Differential Cut

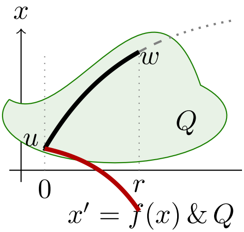


Differential Ghost



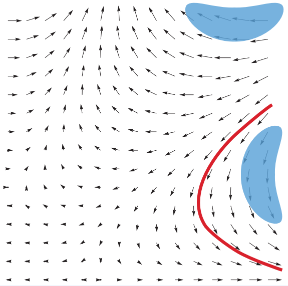




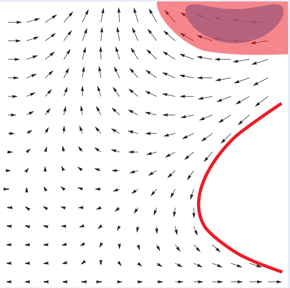


Differential Invariants for Differential Equations

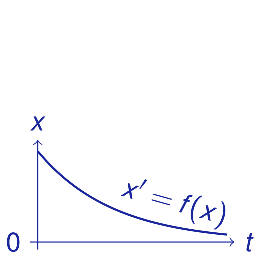
Differential Invariant

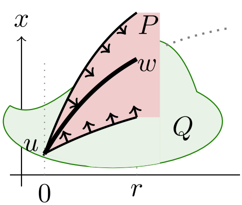


Differential Cut

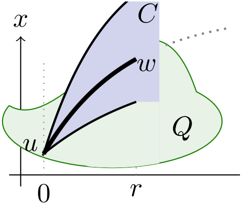


Differential Ghost

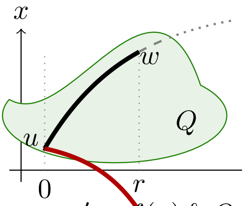




$x' = f(x) \,\&\, Q$

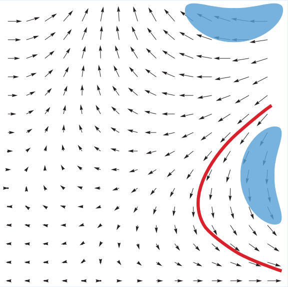


$x' = f(x) \,\&\, Q$

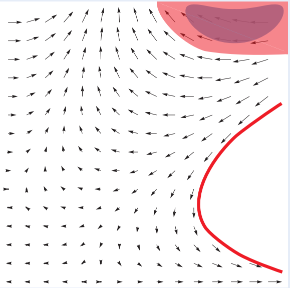


$x' = f(x) \,\&\, Q$

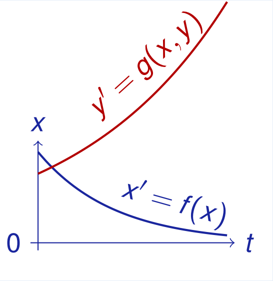
Differential Invariant

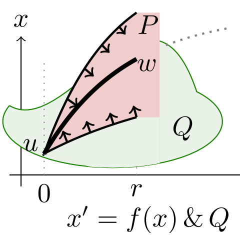


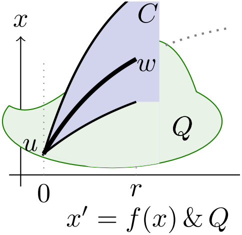
Differential Cut

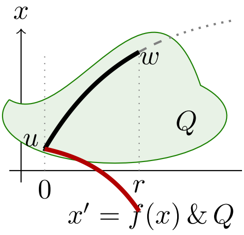


Differential Ghost



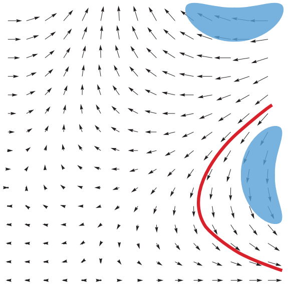




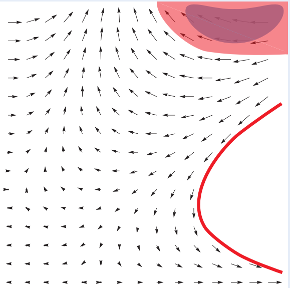


Differential Invariants for Differential Equations

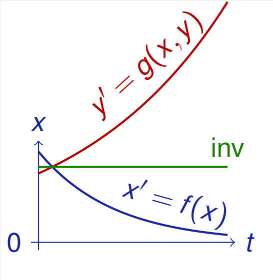
Differential Invariant

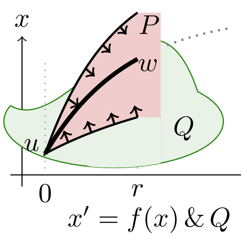


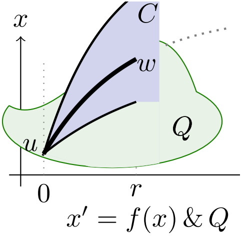
Differential Cut

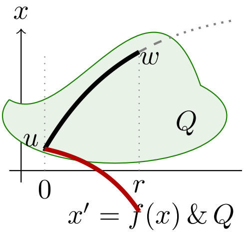


Differential Ghost









Differential Invariant

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

Differential Cut

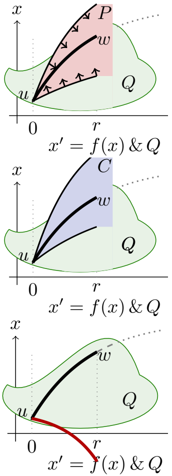
$$\frac{P \to [x' = f(x) \,\&\, Q]C \quad P \to [x' = f(x) \,\&\, Q \wedge C]P}{P \to [x' = f(x) \,\&\, Q]P}$$

Differential Ghost

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

deductive power added DI $\prec$ DI+DC $\prec$ DI+DC+DG

$$[\![(e)']\!]_v = \sum_x v(x') \frac{\partial [\![e]\!]}{\partial x}(v)$$

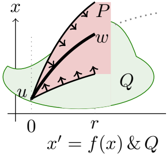


Springer'10, LMCS'12, LICS'12,JAR'17,LICS'18,JACM'20

Differential Invariants for Differential Equations

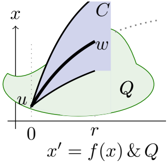
Differential Invariant

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



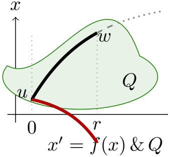
Differential Cut

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



Differential Ghost

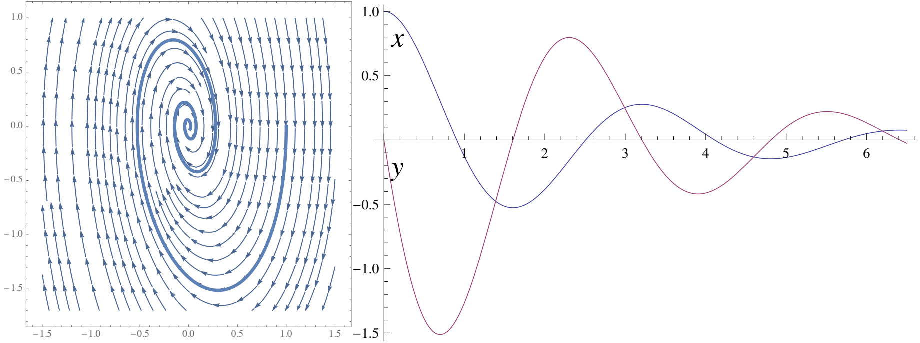
$$\frac{P \leftrightarrow \exists y\, \color{green}{G} \quad \color{green}{G} \rightarrow [x' = f(x), \color{red}{y' = g(x,y)} \,\&\, Q]\color{green}{G}}{P \rightarrow [x' = f(x) \,\&\, Q]P}$$



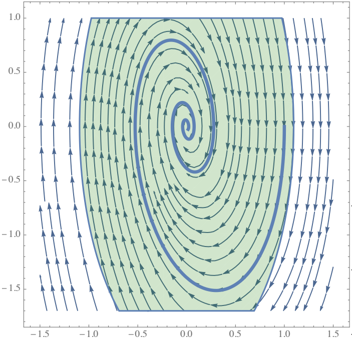
if $\color{red}{g(x,y) = a(x)y + b(x)}$, so has long solution!

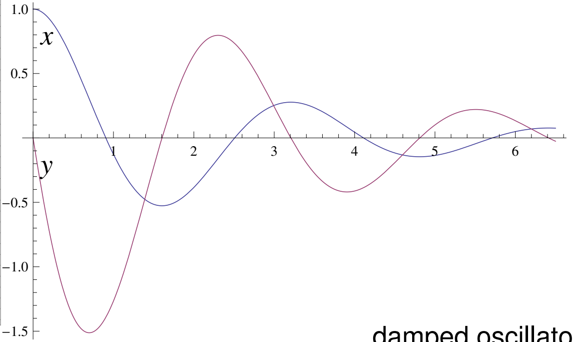
Springer'10, LMCS'12, LICS'12,JAR'17,LICS'18,JACM'20

$$\frac{}{\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, \omega \geq 0 \land d \geq 0]\, \omega^2 x^2 + y^2 \leq c^2}$$



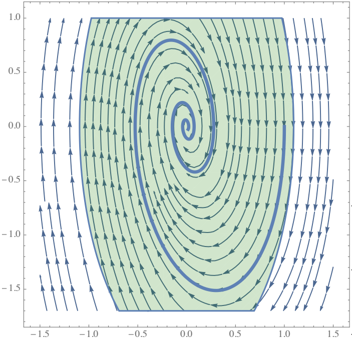
$$\omega^2x^2+y^2\le c^2 \rightarrow [x'=y, y'=-\omega^2x-2d\omega y\ \&\ \omega\ge 0\wedge d\ge 0]\,\omega^2x^2+y^2\le c^2$$

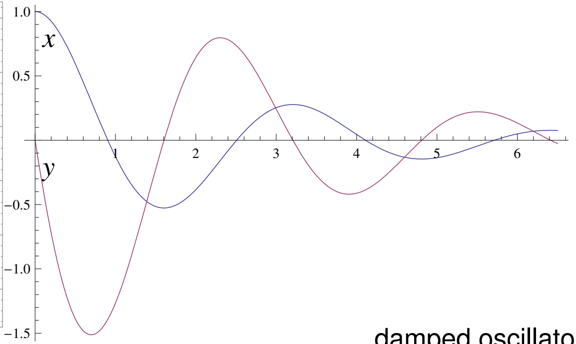




damped oscillator

$$\frac{\omega \geq 0 \land d \geq 0 \rightarrow [x' := y][y' := -\omega^2 x - 2d\omega y]\, 2\omega^2 x x' + 2 y y' \leq 0}{\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, \omega \geq 0 \land d \geq 0]\, \omega^2 x^2 + y^2 \leq c^2}$$



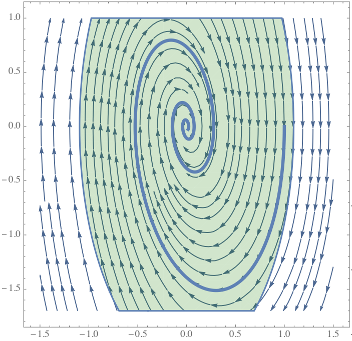


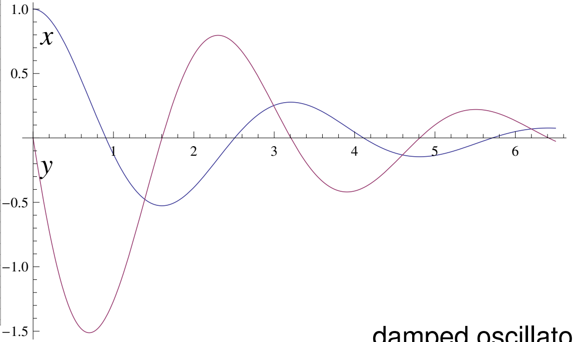
damped oscillator

$$\omega\geq 0 \land d\geq 0 \rightarrow 2\omega^2 x y + 2y(-\omega^2 x - 2d\omega y) \leq 0$$

$$\omega\geq 0 \land d\geq 0 \rightarrow [x':=y][y':=-\omega^2 x - 2d\omega y]\, 2\omega^2 x x' + 2y y' \leq 0$$

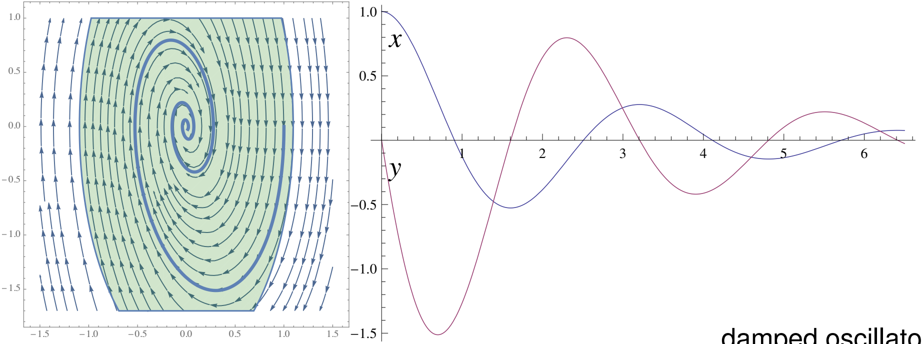
$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, \omega\geq 0 \land d\geq 0]\, \omega^2 x^2 + y^2 \leq c^2$$





damped oscillator

$$\frac{\frac{\frac{*}{\omega\geq 0 \land d\geq 0 \rightarrow 2\omega^2 xy + 2y(-\omega^2 x - 2d\omega y) \leq 0}}{\omega\geq 0 \land d\geq 0 \rightarrow [x':=y][y':=-\omega^2 x - 2d\omega y]\, 2\omega^2 x x' + 2yy' \leq 0}}{\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, \omega\geq 0 \land d\geq 0]\, \omega^2 x^2 + y^2 \leq c^2}$$



damped oscillator

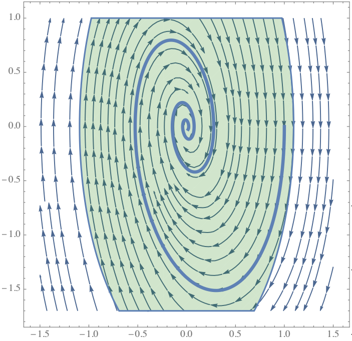
$$*$$

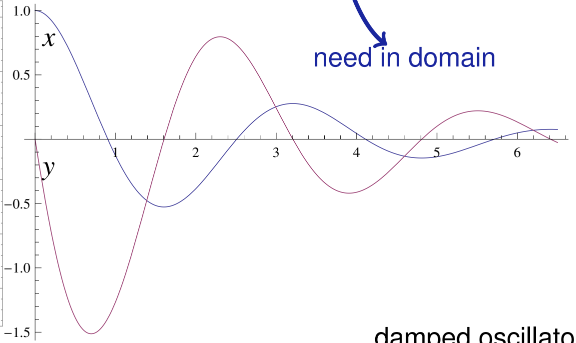
$$\omega\geq 0 \land d\geq 0 \rightarrow 2\omega^2 xy + 2y(-\omega^2 x - 2d\omega y) \leq 0$$

$$\omega\geq 0 \land d\geq 0 \rightarrow [x':=y][y':=-\omega^2 x - 2d\omega y]\, 2\omega^2 xx' + 2yy' \leq 0$$

$$\omega^2x^2+y^2\leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, \omega\geq 0 \land d\geq 0]\, \omega^2x^2+y^2\leq c^2$$

need in domain

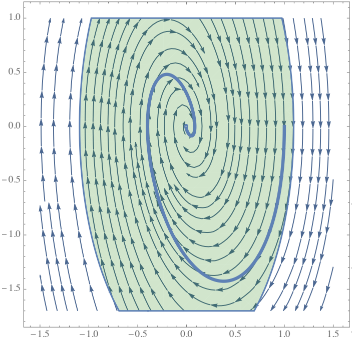


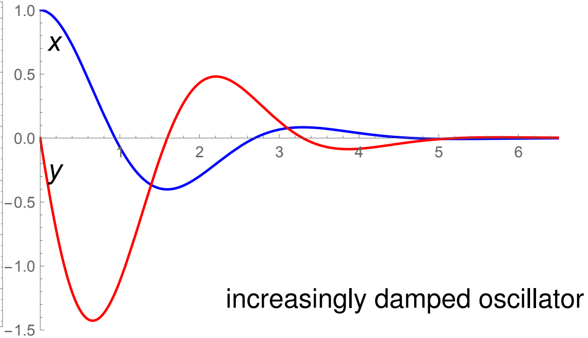


damped oscillator

$$\overline{\omega^2 x^2 + y^2 \le c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d'=7 \,\&\, \omega \ge 0]\, \omega^2 x^2 + y^2 \le c^2}$$

$$\omega^2 x^2 + y^2 \le c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \,\&\, \omega \ge 0]\, \omega^2 x^2 + y^2 \le c^2$$





$$\frac{\omega^2x^2+y^2\leq c^2 \rightarrow [x'=y, y'=-\omega^2x-2d\omega y, d'=7\ \&\ \omega\geq 0\land d\geq 0]\,\omega^2x^2+y^2\leq c^2}{\omega^2x^2+y^2\leq c^2 \rightarrow [x'=y, y'=-\omega^2x-2d\omega y, d'=7\ \&\ \omega\geq 0]\,\omega^2x^2+y^2\leq c^2}$$

increasingly damped oscillator

$$\dfrac{\dfrac{}{\omega^2x^2+y^2\le c^2 \to [x'=y, y'=-\omega^2x-2d\omega y, d'=7 \,\&\, \omega\ge 0 \land d\ge 0]\, \omega^2x^2+y^2\le c^2}}{\omega^2x^2+y^2\le c^2 \to [x'=y, y'=-\omega^2x-2d\omega y, d'=7 \,\&\, \omega\ge 0]\, \omega^2x^2+y^2\le c^2}$$

ask

$$\dfrac{}{d\ge 0 \to [x'=y, y'=-\omega^2x-2d\omega y, d'=7 \,\&\, \omega\ge 0]\, d\ge 0}$$

increasingly damped oscillator

$$\dfrac{\omega^2x^2+y^2\leq c^2 \rightarrow [x'=y, y'=-\omega^2x-2d\omega y, d'=7 \,\&\, \omega\geq 0 \land d\geq 0]\, \omega^2x^2+y^2\leq c^2}{\omega^2x^2+y^2\leq c^2 \rightarrow [x'=y, y'=-\omega^2x-2d\omega y, d'=7 \,\&\, \omega\geq 0]\, \omega^2x^2+y^2\leq c^2}$$

$$\dfrac{\omega\geq 0 \rightarrow [d':=7]\, d'\geq 0}{d\geq 0 \rightarrow [x'=y, y'=-\omega^2x-2d\omega y, d'=7 \,\&\, \omega\geq 0]\, d\geq 0}$$

increasingly damped oscillator

$$\dfrac{}{\dfrac{\omega^2x^2+y^2\le c^2 \rightarrow [x'=y, y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\ge 0\land d\ge 0]\,\omega^2x^2+y^2\le c^2}{\omega^2x^2+y^2\le c^2 \rightarrow [x'=y, y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\ge 0]\,\omega^2x^2+y^2\le c^2}}$$

$$\dfrac{\dfrac{\dfrac{}{\omega\ge 0 \rightarrow 7\ge 0}}{\omega\ge 0 \rightarrow [d':=7]\,d'\ge 0}}{d\ge 0 \rightarrow [x'=y, y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\ge 0]\,d\ge 0}$$

increasingly damped oscillator

$$\dfrac{\omega^2x^2+y^2\le c^2 \rightarrow [x'=y, y'=-\omega^2x-2d\omega y, d'=7 \,\&\, \omega\ge 0 \wedge d\ge 0]\, \omega^2x^2+y^2\le c^2}{\omega^2x^2+y^2\le c^2 \rightarrow [x'=y, y'=-\omega^2x-2d\omega y, d'=7 \,\&\, \omega\ge 0]\, \omega^2x^2+y^2\le c^2}$$

DC

$$\dfrac{\dfrac{\dfrac{*}{\omega\ge 0 \rightarrow 7\ge 0}}{\omega\ge 0 \rightarrow [d':=7]\, d'\ge 0}}{d\ge 0 \rightarrow [x'=y, y'=-\omega^2x-2d\omega y, d'=7 \,\&\, \omega\ge 0]\, d\ge 0}$$

increasingly damped oscillator

$$\frac{\dfrac{\omega\geq 0\land d\geq 0 \to [x':=y][y':=-\omega^2 x - 2d\omega y]\, 2\omega^2 x x' + 2y y' \leq 0}{\omega^2x^2+y^2\leq c^2 \to [x'=y, y'=-\omega^2 x - 2d\omega y, d'=7 \,\&\, \omega\geq 0\land d\geq 0]\, \omega^2x^2+y^2\leq c^2}}{\omega^2x^2+y^2\leq c^2 \to [x'=y, y'=-\omega^2 x - 2d\omega y, d'=7 \,\&\, \omega\geq 0]\, \omega^2x^2+y^2\leq c^2}$$

$$\cfrac{\cfrac{\cfrac{*}{\omega\geq 0 \to 7\geq 0}}{\omega\geq 0 \to [d':=7]\, d'\geq 0}}{d\geq 0 \to [x'=y, y'=-\omega^2 x - 2d\omega y, d'=7 \,\&\, \omega\geq 0]\, d\geq 0}$$

increasingly damped oscillator

$$\dfrac{\dfrac{\dfrac{\omega\geq 0\land d\geq 0 \rightarrow 2\omega^2 x y + 2y(-\omega^2 x - 2d\omega y) \leq 0}{\omega\geq 0\land d\geq 0 \rightarrow [x':=y][y':=-\omega^2 x - 2d\omega y]\, 2\omega^2 x x' + 2y y' \leq 0}}{\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d'=7 \,\&\, \omega\geq 0\land d\geq 0]\, \omega^2 x^2 + y^2 \leq c^2}}{\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d'=7 \,\&\, \omega\geq 0]\, \omega^2 x^2 + y^2 \leq c^2}$$

$$\dfrac{\dfrac{\dfrac{*}{\omega\geq 0 \rightarrow 7\geq 0}}{\omega\geq 0 \rightarrow [d':=7]\, d'\geq 0}}{d\geq 0 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d'=7 \,\&\, \omega\geq 0]\, d\geq 0}$$

increasingly damped oscillator

$$\dfrac{\dfrac{\dfrac{*}{\omega\geq 0\land d\geq 0 \rightarrow 2\omega^2 xy + 2y(-\omega^2 x - 2d\omega y) \leq 0}}{\omega\geq 0\land d\geq 0 \rightarrow [x':=y][y':=-\omega^2 x - 2d\omega y]\, 2\omega^2 xx' + 2yy' \leq 0}}{\omega^2x^2+y^2\leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d'=7\,\&\,\omega\geq 0\land d\geq 0]\, \omega^2x^2+y^2\leq c^2}}{\omega^2x^2+y^2\leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d'=7\,\&\,\omega\geq 0]\, \omega^2x^2+y^2\leq c^2}$$

$$\dfrac{\dfrac{\dfrac{*}{\omega\geq 0 \rightarrow 7\geq 0}}{\omega\geq 0 \rightarrow [d':=7]\, d'\geq 0}}{d\geq 0 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d'=7\,\&\,\omega\geq 0]\, d\geq 0}$$

increasingly damped oscillator

$$\frac{\dfrac{\dfrac{*}{\omega\geq0\land d\geq0 \to 2\omega^2xy+2y(-\omega^2x-2d\omega y)\leq 0}}{\omega\geq0\land d\geq0 \to [x':=y][y':=-\omega^2x-2d\omega y]\,2\omega^2xx'+2yy'\leq 0}}{\omega^2x^2+y^2\leq c^2 \to [x'=y,y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\geq0\land d\geq0]\,\omega^2x^2+y^2\leq c^2}}{\omega^2x^2+y^2\leq c^2 \to [x'=y,y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\geq0]\,\omega^2x^2+y^2\leq c^2}$$

init

$$\frac{\dfrac{*}{\omega\geq0 \to 7\geq0}}{\omega\geq0 \to [d':=7]\,d'\geq0}$$
$$d\geq0 \to [x'=y,y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\geq0]\,d\geq0$$

Could repeatedly diffcut in formulas to help the proof

Outline

Differential Equation Axiomatization

Theorem (Algebraic Completeness) (LICS'18,JACM'20)

dL *calculus is a sound & complete axiomatization of algebraic invariants of polynomial differential equations. They are decidable by DI,DC,DG in* dL.

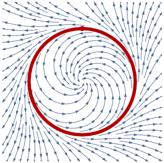
Theorem (Semialgebraic Completeness) (LICS'18,JACM'20)

dL *calculus with RI is a sound & complete axiomatization of semialgebraic invariants of differential equations. They are decidable in* dL.

ODE Axiomatization: Derived Darboux Rules

Darboux equalities are DG

Gaston Darboux 1878



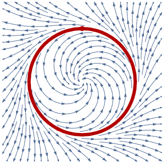
$$\frac{Q \rightarrow e' = ge}{e = 0 \rightarrow [x' = f(x) \,\&\, Q]e = 0} \quad (g \in \mathbb{R}[x])$$

Definable e' for Lie-derivative w.r.t. ODE

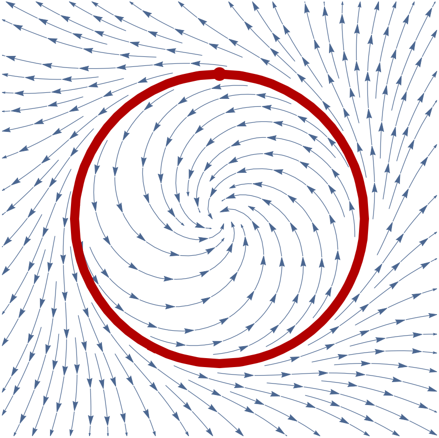
ODE Axiomatization: Derived Darboux Rules

Darboux equalities are DG

Gaston Darboux 1878



$$\frac{Q \rightarrow e' = ge}{e = 0 \rightarrow [x' = f(x) \,\&\, Q]e = 0} \quad (g \in \mathbb{R}[x])$$

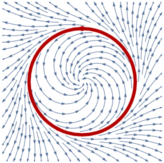


$$\frac{\rightarrow 2uu' + 2vv' = 2(u^2+v^2)(u^2+v^2-1)}{.. \rightarrow \begin{bmatrix} u' = -v-u+u^3+uv^2 \\ v' = u-v+u^2v+v^3 \end{bmatrix} u^2+v^2-1=0}$$

ODE Axiomatization: Derived Darboux Rules

Darboux equalities are DG

$$\frac{Q \to e' = ge}{e = 0 \to [x' = f(x) \,\&\, Q]e = 0} \quad (g \in \mathbb{R}[x])$$



Proof Idea.

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

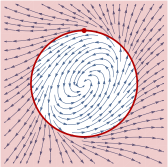
Derive $[x' = f(x) \,\&\, Q](e)' = ge \to (e = 0 \to [x' = f(x) \,\&\, Q]e = 0)$

ODE Axiomatization: Derived Darboux Rules

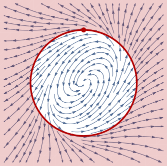
Darboux inequalities are DG

Thomas Grönwall 1919

$$\frac{Q \rightarrow e' \geq ge}{e \succcurlyeq 0 \rightarrow [x' = f(x) \,\&\, Q] e \succcurlyeq 0} \quad (g \in \mathbb{R}[x])$$



ODE Axiomatization: Derived Darboux Rules



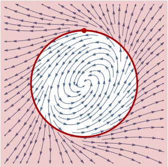
Darboux inequalities are DG

$$\frac{Q \rightarrow e' \geq ge}{e \succcurlyeq 0 \rightarrow [x' = f(x) \,\&\, Q] e \succcurlyeq 0} \quad (g \in \mathbb{R}[x])$$

Proof Idea.

1. DG counterweight $y' = -gy$ to reduce $e \succcurlyeq 0$ to $ey \succcurlyeq 0 \wedge y > 0$.
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 $y > 0$) $ey \succcurlyeq 0$ are differential invariants by construction as $(ey)' = e'y - gye \geq 0$ from premise since $y > 0$. □

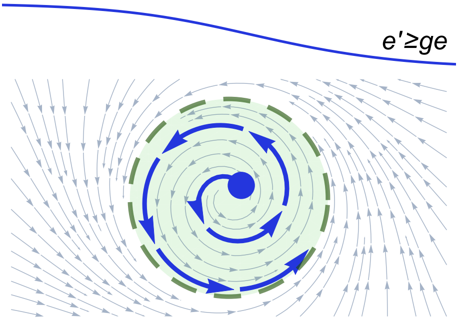
Derive $[x' = f(x) \,\&\, Q](e)' \geq ge \rightarrow (e \succcurlyeq 0 \rightarrow [x' = f(x) \,\&\, Q] e \succcurlyeq 0)$

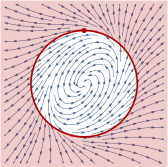


Darboux inequalities are DG

$$\frac{Q \rightarrow e' \geq ge}{e \succcurlyeq 0 \rightarrow [x' = f(x) \,\&\, Q] e \succcurlyeq 0} \quad (g \in \mathbb{R}[x])$$

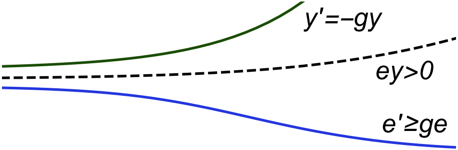
$$\frac{(1-u^2-v^2)' \geq -\frac{1}{2}(u^2+v^2)(1-u^2-v^2)}{\ldots \rightarrow \left[\begin{array}{l} u' = -v + \frac{u}{4}(1-u^2-v^2) \\ v' = \quad u + \frac{v}{4}(1-u^2-v^2) \end{array} \right] 1-u^2-v^2 > 0}$$

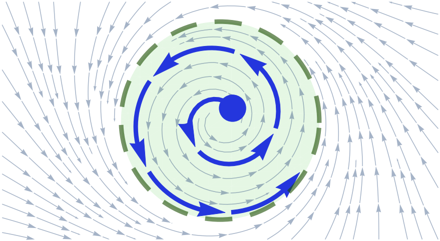




Darboux inequalities are DG

$$\frac{Q \to e' \geq ge}{e \succcurlyeq 0 \to [x' = f(x) \,\&\, Q] e \succcurlyeq 0} \quad (g \in \mathbb{R}[x])$$





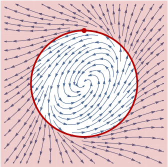
$$\frac{(1-u^2-v^2)' \geq -\frac{1}{2}(u^2+v^2)(1-u^2-v^2)}{\ldots \to \left[\begin{array}{l} u' = -v + \frac{u}{4}(1-u^2-v^2) \\ v' = u + \frac{v}{4}(1-u^2-v^2) \\ y' = \frac{1}{2}(u^2+v^2)y \end{array}\right] 1-u^2-v^2 > 0}$$

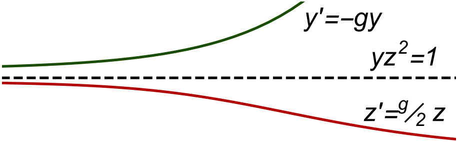
$$(1-u^2-v^2)y > 0$$

ODE Axiomatization: Derived Darboux Rules

Darboux inequalities are DG

$$\frac{Q \rightarrow e' \geq ge}{e \succcurlyeq 0 \rightarrow [x' = f(x) \,\&\, Q] e \succcurlyeq 0} \quad (g \in \mathbb{R}[x])$$

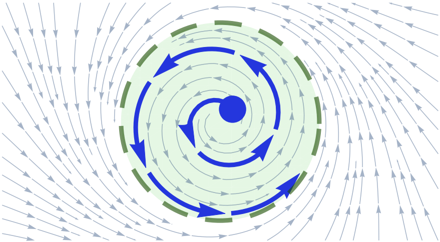




$$\frac{(1-u^2-v^2)' \geq -\frac{1}{2}(u^2+v^2)(1-u^2-v^2)}{\ldots \rightarrow \left[\begin{array}{l} u' = -v + \frac{u}{4}(1-u^2-v^2) \\ v' = \quad u + \frac{v}{4}(1-u^2-v^2) \\ y' = \frac{1}{2}(u^2+v^2)y \\ z' = -\frac{1}{4}(u^2+v^2)z \end{array}\right] 1-u^2-v^2 > 0}$$

$$(1-u^2-v^2)y > 0$$

$$yz^2 = 1$$



Darboux Inequalities are Differential Ghosts: Details

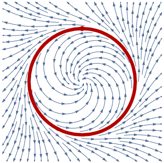
$$*$$
$$\text{R}\ \overline{\quad Q \rightarrow (-gy)z^2 + y(2z(\tfrac{g}{2}z)) = 0 \quad}$$
$$\text{dI}\ \overline{\quad yz^2 = 1 \rightarrow [x' = f(x), y' = -gy, z' = \tfrac{g}{2}z \,\&\, Q]\, yz^2 = 1 \quad}$$
$$\text{M,}\exists\text{R}\ \overline{\quad y > 0 \rightarrow \exists z\, [x' = f(x), y' = -gy, z' = \tfrac{g}{2}z \,\&\, Q]\, y > 0 \quad}$$
$$\text{dG}\ \overline{\quad y > 0 \rightarrow [x' = f(x), y' = -gy \,\&\, Q]\, y > 0 \quad}$$

$$Q \rightarrow e' \geq ge \qquad \dfrac{*}{e' \geq ge, y > 0 \rightarrow e'y - gye \geq 0}\ \text{R}$$
$$\text{cut}\ \overline{\quad Q, y > 0 \rightarrow e'y - gye \geq 0 \quad}$$
$$\text{dI}\ \overline{\quad e \succcurlyeq 0, y > 0 \rightarrow [x' = f(x), y' = -gy \,\&\, Q \wedge y > 0]\, ey \succcurlyeq 0 \quad \triangleright}$$
$$\text{dC}\ \overline{\quad e \succcurlyeq 0, y > 0 \rightarrow [x' = f(x), y' = -gy \,\&\, Q](y > 0 \wedge ey \succcurlyeq 0) \quad}$$
$$\text{M,}\exists\text{R}\ \overline{\quad e \succcurlyeq 0 \rightarrow \exists y\, [x' = f(x), y' = -gy \,\&\, Q]\, e \succcurlyeq 0 \quad}$$
$$\text{dG}\ \overline{\quad e \succcurlyeq 0 \rightarrow [x' = f(x) \,\&\, Q]\, e \succcurlyeq 0 \quad}$$

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

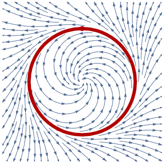
Vectorial Darboux are DG

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



Definable $\mathbf{e}'$ for component-wise Lie-derivative w.r.t. ODE

ODE Axiomatization: Derived Darboux Rules



Vectorial Darboux are DG

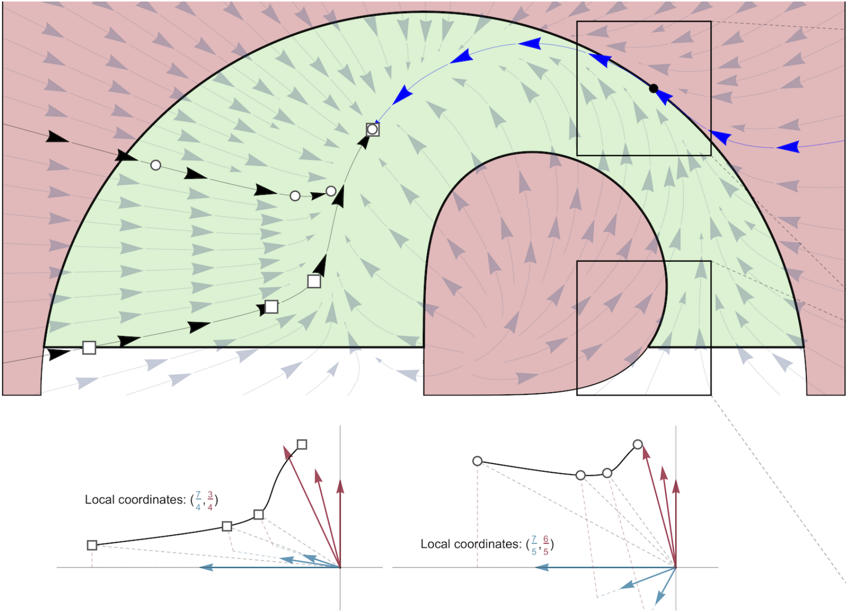
$$\frac{Q \rightarrow \mathbf{e}' = G\mathbf{e}}{\mathbf{e} = 0 \rightarrow [x' = f(x) \,\&\, Q]\mathbf{e} = 0} \quad (G \in \mathbb{R}[x]^{n \times n})$$

Proof Idea.

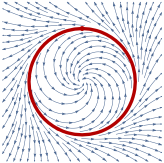
1. DG counterweight $\mathbf{y}' = -G^T\mathbf{y}$ to change $\mathbf{e} = 0$ to $\mathbf{e} \cdot \mathbf{y} = 0$.
2. But: $\mathbf{e} \cdot \mathbf{y} = 0 \not\Rightarrow \mathbf{e} = 0$ even if $\mathbf{y} \neq 0$.
3. Redo: time-varying independent DG matrix $Y' = -YG$ with $Y\mathbf{e} = 0$.
4. $Y\mathbf{e} = 0 \Rightarrow \mathbf{e} = 0$ if $\det Y \neq 0$.
5. DC $\det Y \neq 0$ proves by dbx with Liouville: $\det(Y)' = -\mathrm{tr}(G)\det(Y)$
6. Continuous change of basis Y^{-1} balancing out motion of $\mathbf{e}$: constant!
7. Continuous change to new evolving variables is sound by DG. □

Derive $[x' = f(x) \,\&\, Q](\mathbf{e})' = G\mathbf{e} \rightarrow (\mathbf{e} = 0 \rightarrow [x' = f(x) \,\&\, Q]\mathbf{e} = 0)$

Time is defined so that motion looks simple ≈Poincaré



ODE Axiomatization: Derived Darboux Rules



Vectorial Darboux are DG

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

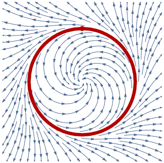
Proof Idea.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{(\mathbf{e})' = G\mathbf{e} \rightarrow -2\mathbf{e}\cdot(\mathbf{e})' \geq g(-\|\mathbf{e}\|^2)}\text{R}}{(\mathbf{e})' = G\mathbf{e} \rightarrow (-\|\mathbf{e}\|^2)' \geq g(-\|\mathbf{e}\|^2)}(\,)'}{[x' = f(x) \,\&\, Q](\mathbf{e})' = G\mathbf{e} \rightarrow [x' = f(x) \,\&\, Q](-\|\mathbf{e}\|^2)' \geq g(-\|\mathbf{e}\|^2)}\text{M}}{[x' = f(x) \,\&\, Q](\mathbf{e})' = G\mathbf{e}, -\|\mathbf{e}\|^2 \geq 0 \rightarrow [x' = f(x) \,\&\, Q] -\|\mathbf{e}\|^2 \geq 0}\text{DBX}}{[x' = f(x) \,\&\, Q](\mathbf{e})' = G\mathbf{e}, \mathbf{e} = 0 \rightarrow [x' = f(x) \,\&\, Q]\mathbf{e} = 0}\text{M}$$

where $g \stackrel{\text{def}}{=} 1 + \sum_{i=1}^{n} \sum_{j=1}^{n} G_{ij}^2$ 1 + squared Frobenius □

Derive $[x' = f(x) \,\&\, Q](\mathbf{e})' = G\mathbf{e} \rightarrow (\mathbf{e} = 0 \rightarrow [x' = f(x) \,\&\, Q]\mathbf{e} = 0)$

ODE Axiomatization: Derived Invariant Rules

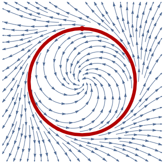


Vectorial Darboux are DG

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

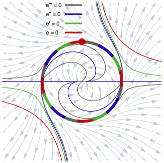
Vectorial Darboux are DG

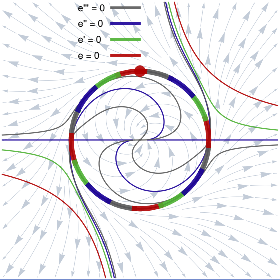
$$\frac{Q \rightarrow \mathbf{e}' = G\mathbf{e}}{\mathbf{e} = 0 \rightarrow [x' = f(x) \,\&\, Q]\mathbf{e} = 0}$$

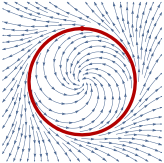


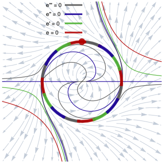
Differential Radical Invariants are DG

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









Vectorial Darboux are DG

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

Differential Radical Invariants are DG

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

Proof Idea.

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

□

ODE Axiomatization: Derived Invariant Rules

Vectorial Darboux are DG

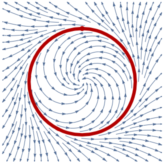
$$\frac{Q \rightarrow \mathbf{e}' = G\mathbf{e}}{\mathbf{e} = 0 \rightarrow [x' = f(x) \,\&\, Q]\mathbf{e} = 0}$$

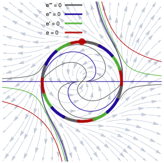
$e'^* = 0$

Differential Radical Invariants are DG

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

N exists





ODE Axiomatization: Derived Invariant Rules

Vectorial Darboux are DG

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

$e'^{*} = 0$

Differential Radical Invariants are DG

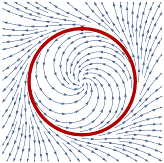
$$\frac{\Gamma, Q \rightarrow \bigwedge_{i=0}^{N-1} e^{(i)} = 0 \quad Q \rightarrow e^{(N)} = \sum_{i=0}^{N-1} g_i e^{(i)}}{\Gamma \rightarrow [x' = f(x) \,\&\, Q] e = 0}$$

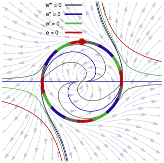
N exists

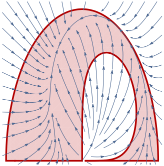
Semialgebraic Invariants are derived

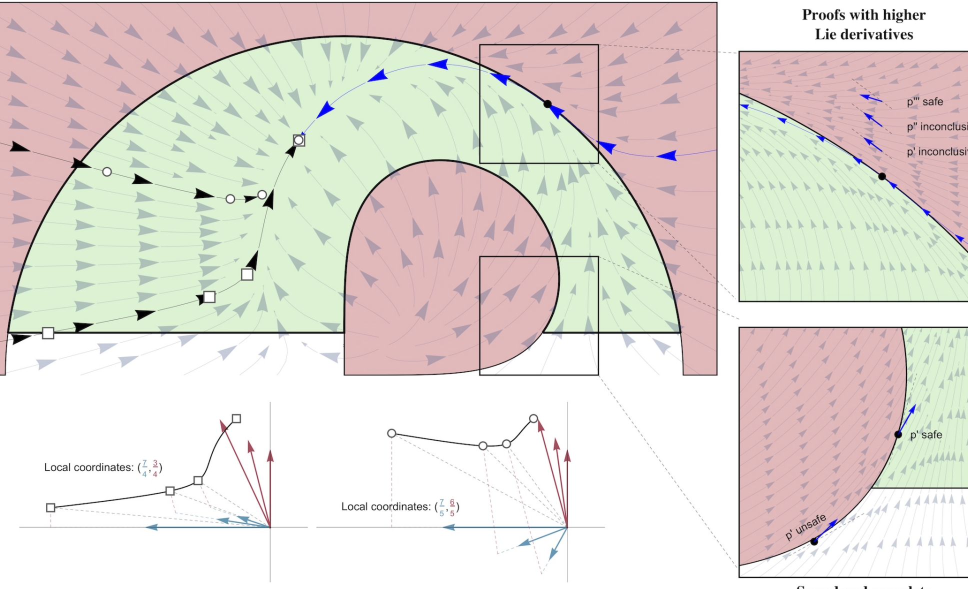
$$\frac{Q \rightarrow e'^{*} \succcurlyeq 0 \quad Q \rightarrow e^{(N)} = \sum_{i=0}^{N-1} g_i e^{(i)}}{\Gamma \rightarrow [x' = f(x) \,\&\, Q] e \succcurlyeq 0}$$

$$e'^{*} \geq 0 \;\equiv\; e \geq 0 \land (e = 0 \rightarrow (e')'^{*} \geq 0)$$
$$e'^{*} > 0 \;\equiv\; e > 0 \lor (e = 0 \land (e')'^{*} > 0)$$









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

Sound and complete ODE invariance proofs

Extended Axiomatization

Unique Solutions

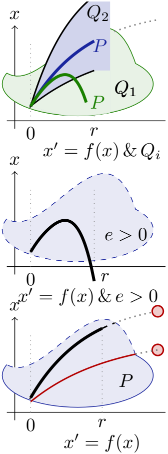
$$\langle x' = f(x) \,\&\, Q_1 \wedge Q_2 \rangle P \leftrightarrow \langle x' = f(x) \,\&\, Q_1 \rangle P \wedge \langle x' = f(x) \,\&\, Q_2 \rangle P$$

Continuous Existence

$$\langle x' = f(x) \,\&\, e > 0 \rangle x \neq y \leftrightarrow e > 0$$

Real Induction

$$[x' = f(x)]P \leftrightarrow \forall y\, [x' = f(x) \,\&\, P \vee x{=}y] \big(x{=}y \rightarrow P \wedge \langle x' = f(x) \,\&\, P \rangle x \neq y\big)$$



Unique Solutions

$$\langle x' = f(x) \,\&\, Q_1 \wedge Q_2 \rangle P \leftrightarrow \langle x' = f(x) \,\&\, Q_1 \rangle P \wedge \langle x' = f(x) \,\&\, Q_2 \rangle P$$

Continuous Existence

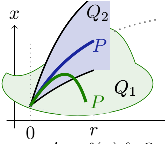
$$\langle x' = f(x) \,\&\, e > 0 \rangle x \neq y \leftrightarrow e > 0$$

Real Induction

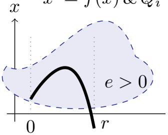
$$[x' = f(x)]P \leftrightarrow \forall y \, [x' = f(x) \,\&\, P \vee x{=}y] \big(x{=}y \rightarrow P \wedge \langle x' = f(x) \,\&\, P \rangle x \neq y\big)$$

Differential Adjoint

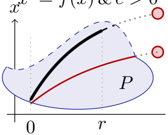
$$\langle x'{=}f(x) \,\&\, Q(x) \rangle x{=}y \leftrightarrow \langle y'{=}{-}f(y) \,\&\, Q(y) \rangle y{=}x$$



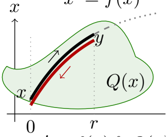
$x' = f(x) \,\&\, Q_i$



$x' = f(x) \,\&\, e > 0$

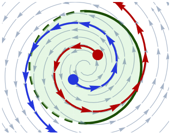


$x' = f(x)$



$x' = f(x) \,\&\, Q(x$

ODE Axiomatization: Derived Invariance Rule $x_0' = 1$



Real Induction Rule

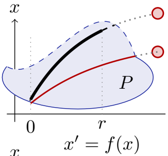
$$\frac{P \rightarrow \langle x' = f(x) \,\&\, P \rangle \bigcirc \qquad \neg P \rightarrow \langle x' = -f(x) \,\&\, \neg P \rangle \bigcirc}{P \rightarrow [x' = f(x)] P}$$

$$\langle x' = f(x) \,\&\, P \rangle \bigcirc \equiv \langle y := x \rangle \langle x' = f(x) \,\&\, P \lor x = y \rangle x \neq y$$

Local progress to P

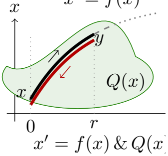
Real Induction

$$[x' = f(x)] P \leftrightarrow \forall y \, [x' = f(x) \,\&\, P \lor x = y] \big(x = y \rightarrow P \land \langle x' = f(x) \,\&\, P \rangle x \neq y \big)$$



Differential Adjoint

$$\langle x' = f(x) \,\&\, Q(x) \rangle x = y \leftrightarrow \langle y' = -f(y) \,\&\, Q(y) \rangle y = x$$



Local Progress Step

$$e > 0 \lor e = 0 \land \langle x' = f(x) \,\&\, e' \geq 0 \rangle \bigcirc \rightarrow \langle x' = f(x) \,\&\, e \geq 0 \rangle \bigcirc$$

Local Progress $\geq$

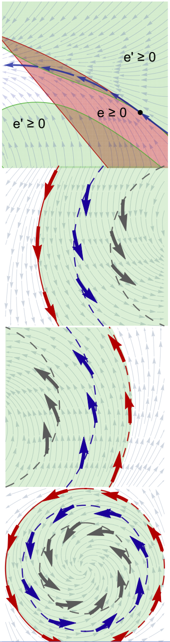
$$e'^{*} \geq 0 \rightarrow \langle x' = f(x) \,\&\, e \geq 0 \rangle \bigcirc$$

Local Progress $>$

$$e'^{*} > 0 \rightarrow \langle x' = f(x) \,\&\, e > 0 \rangle \bigcirc$$

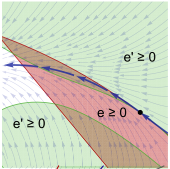
Local Progress Semialgebraic

$$\langle x' = f(x) \,\&\, P \rangle \bigcirc \leftrightarrow P'^{*}$$



Local Progress Step

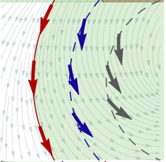
$$e > 0 \lor e = 0 \land \langle x' = f(x) \,\&\, e' \geq 0 \rangle \bigcirc \rightarrow \langle x' = f(x) \,\&\, e \geq 0 \rangle \bigcirc$$



Local Progress ≥

$$e'^{*} \geq 0 \rightarrow \langle x' = f(x) \,\&\, e \geq 0 \rangle \bigcirc$$

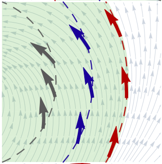
$$e'^{*} \geq 0 \equiv e \geq 0 \land (e = 0 \rightarrow (e')'^{*} \geq 0)$$



Local Progress >

$$e'^{*} > 0 \rightarrow \langle x' = f(x) \,\&\, e > 0 \rangle \bigcirc$$

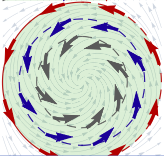
$$e'^{*} > 0 \equiv e > 0 \lor (e = 0 \land (e')'^{*} > 0)$$



Local Progress Semialgebraic

$$\langle x' = f(x) \,\&\, P \rangle \bigcirc \leftrightarrow P'^{*}$$

$$(P \land Q)'^{*} \equiv P'^{*} \land Q'^{*}$$
$$(P \lor Q)'^{*} \equiv P'^{*} \lor Q'^{*}$$



Differential Equation Axiomatization

Theorem (Algebraic Completeness) (LICS'18,JACM'20)

dL *calculus is a sound & complete axiomatization of algebraic invariants of polynomial differential equations. They are decidable with a derived axiom:*

$$\text{(DRI)} \quad [x' = f(x)\,\&\,Q]e = 0 \leftrightarrow \big(Q \rightarrow e'^{*} = 0\big) \qquad (Q \text{ open})$$

Theorem (Semialgebraic Completeness) (LICS'18,JACM'20)

dL *calculus with RI is a sound & complete axiomatization of semialgebraic invariants of differential equations. They are decidable with derived axiom:*

$$\text{(SAI)} \quad \forall x\,(P \rightarrow [x' = f(x)]P) \leftrightarrow \forall x\,\big(P \rightarrow P'^{*}\big) \land \forall x\,\big(\neg P \rightarrow (\neg P)'^{*-}\big)$$

Definable e'^{*} is short for *all/significant* Lie derivative w.r.t. ODE
Definable e'^{*-} is w.r.t. backwards ODE $x' = -f(x)$. Also for P.

Differential Equation Axiomatization

Theorem (Analytic Completeness) (LICS'18,JACM'20)

dL *calculus is a sound & complete axiomatization of analytic invariants of analytic differential equations.*

$$\text{(DRI)} \quad [x' = f(x) \,\&\, Q]e = 0 \leftrightarrow \left(Q \rightarrow e'^{*} = 0\right) \qquad (Q \text{ open})$$

Theorem (Semianalytic Completeness) (LICS'18,JACM'20)

dL *calculus with RI is a sound & complete axiomatization of semianalytic invariants of differential equations.*

$$\text{(SAI)} \quad \forall x\,(P \rightarrow [x' = f(x)]P) \leftrightarrow \forall x\left(P \rightarrow P'^{*}\right) \land \forall x\left(\neg P \rightarrow (\neg P)'^{*-}\right)$$

- (S) Smooth function interpretations $h : \mathbb{R}^k \rightarrow \mathbb{R}$
- (P) Partial derivatives of $h(y_1, \ldots, y_k)$ have syntactic term representation $\frac{\partial h}{\partial y_i}$
- (R) Computable differential radicals: compute N, g_i for $e^{(N)} = \sum_{i=0}^{N-1} g_i e^{(i)}$

Completeness for Noetherian Functions

Definition (Noetherian Function)

$h : H \subseteq \mathbb{R}^k \to \mathbb{R}$ is *Noetherian function* iff $h(y) = p(y, h_1(y), \dots, h_r(y))$ for a polynomial p and *Noetherian chain* $h_1, \dots, h_r : H \subseteq \mathbb{R}^k \to \mathbb{R}$, i.e., real analytic

$$\frac{\partial h_j}{\partial y_i}(y) = q_{ij}(y, h_1(y), \dots, h_r(y)) \text{ for some polynomial } q_{ij} \in \mathbb{R}[y, z]$$

Example: $\frac{\partial \sin}{\partial y}(y) = \cos(y)$ and $\frac{\partial \cos}{\partial y}(y) = -\sin(y)$ and $\frac{\partial \exp}{\partial y}(y) = \exp(y)$

Theorem Noetherian functions satisfy SPR conditions.

$\Rightarrow$ Completeness for logic + differential equations with Noetherian functions.

(S) Smooth function interpretations $h : \mathbb{R}^k \to \mathbb{R}$

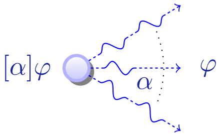
(P) Partial derivatives of $h(y_1, \dots, y_k)$ have syntactic term representation $\frac{\partial h}{\partial y_i}$

(R) Computable differential radicals: compute N, g_i for $e^{(N)} = \sum_{i=0}^{N-1} g_i e^{(i)}$

Outline

differential dynamic logic

dL = DL + HP



Properties

1. Poincaré: qualitative ODE
2. Complete axiomatization
3. Algebraic ODE invariants
4. Semialgebraic ODE invariants
5. Algebraic hybrid systems
6. Local ODE progress
7. Decide by dL proof/disproof
8. Uniform substitution axioms
9. Analytic extensions: Noetherian

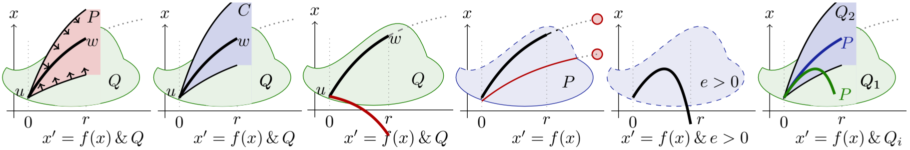
1. MVT
2. Prefix
3. Picard-Lind
4. $\mathbb{R}$-complete
5. Existence
6. Uniqueness

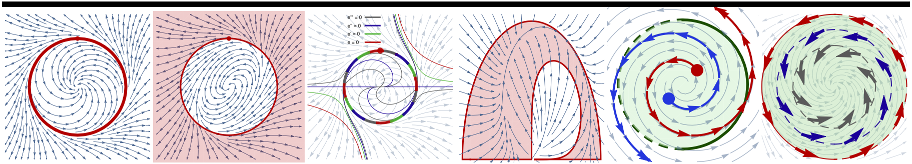
1. Differential invariants
2. Differential cuts
3. Differential ghosts
4. Real induction
5. Continuous existence
6. Unique solutions

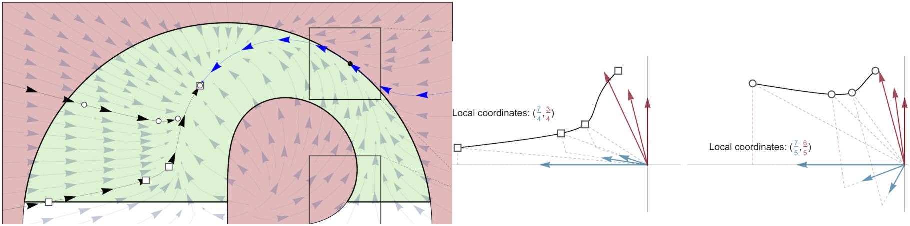
Impressive power of differential ghosts

LICS'18,JACM'20

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**