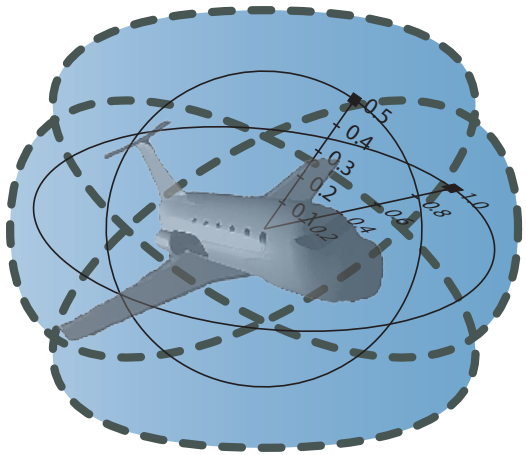
10: Differential Equations & Differential Invariants

15-424: Foundations of Cyber-Physical Systems

André Platzer

aplatzer@cs.cmu.edu
Computer Science Department
Carnegie Mellon University, Pittsburgh, PA



Outline

1. Learning Objectives
2. Differential Equations
   - Descriptive Power of Differential Equations
   - Differential Equations vs. Loops
   - Intuition for Differential Invariants
   - Example: Rotation
   - Derivatives for a Change
   - The Meaning of Prime
   - Semantics of Differential Equations
   - Soundness
   - Example Proofs
3. Soundness Proof
4. Summary

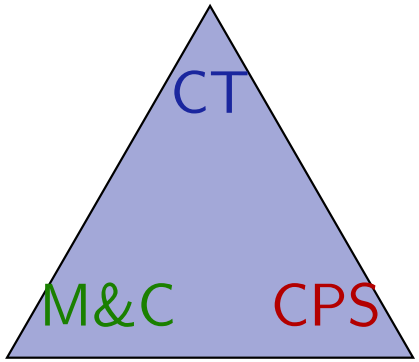
Outline

1. Learning Objectives
2. Differential Equations
   - Descriptive Power of Differential Equations
   - Differential Equations vs. Loops
   - Intuition for Differential Invariants
   - Example: Rotation
   - Derivatives for a Change
   - The Meaning of Prime
   - Semantics of Differential Equations
   - Soundness
   - Example Proofs
3. Soundness Proof
4. Summary

Learning Objectives

Differential Equations & Differential Invariants

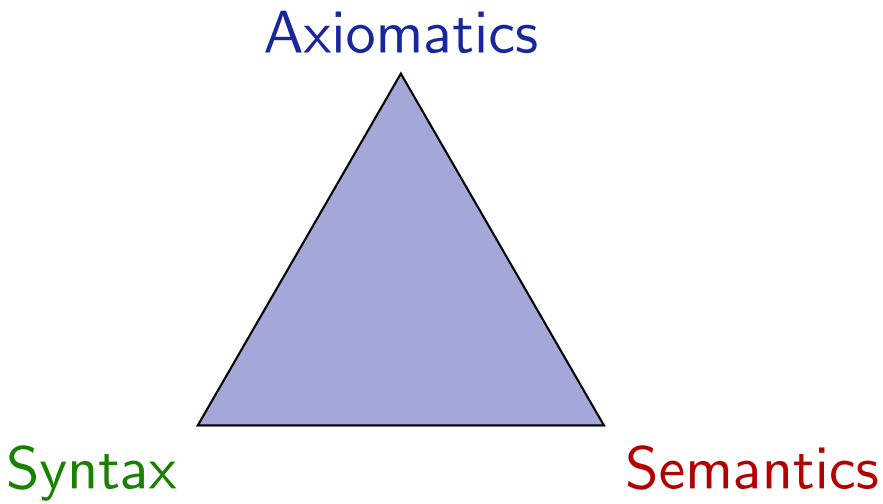
discrete vs. continuous analogies
rigorous reasoning about ODEs
induction for differential equations
differential facet of logical trinity



understanding continuous dynamics
relate discrete+continuous

semantics of ODEs
operational CPS effects

Differential Facet of Logical Trinity



Syntax defines the notation
What problems are we allowed to write down?

Semantics what carries meaning.
What real or mathematical objects does the syntax stand for?

Axiomatics internalizes semantic relations into universal syntactic transformations.
How does the semantics of A relate to semantics of $A \wedge B$, syntactically? If A is true, is $A \wedge B$ true, too? Conversely?

Outline

1. Learning Objectives
2. Differential Equations
   - Descriptive Power of Differential Equations
   - Differential Equations vs. Loops
   - Intuition for Differential Invariants
   - Example: Rotation
   - Derivatives for a Change
   - The Meaning of Prime
   - Semantics of Differential Equations
   - Soundness
   - Example Proofs
3. Soundness Proof
4. Summary

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1 - t x_0}$
$x' = \frac{1}{x}, x(0) = 1$	$x(t) = \sqrt{1 + 2t} \ldots$
$y'(x) = -2xy, y(0) = 1$	$y(x) = e^{-x^2}$
$x'(t) = tx, x(0) = x_0$	$x(t) = x_0 e^{\frac{t^2}{2}}$
$x' = \sqrt{x}, x(0) = x_0$	$x(t) = \frac{t^2}{4} \pm t\sqrt{x_0} + x_0$
$x' = y, y' = -x, x(0) = 0, y(0) = 1$	$x(t) = \sin t, y(t) = \cos t$
$x' = 1 + x^2, x(0) = 0$	$x(t) = \tan t$
$x'(t) = \frac{2}{t^3} x(t)$	$x(t) = e^{-\frac{1}{t^2}}$ non-analytic
$x' = x^2 + x^4$	???
$x'(t) = e^{t^2}$	non-elementary

Global Descriptive Power of Local Differential Equations

Descriptive power of differential equations

1. Simple differential equations can describe quite complicated physical processes.
2. Solution is a global description of the system evolution.
3. ODE is a local characterization.
4. Complexity difference between local description and global behavior
5. Let's exploit that phenomenon for proofs!

Differential Equations vs. Loops

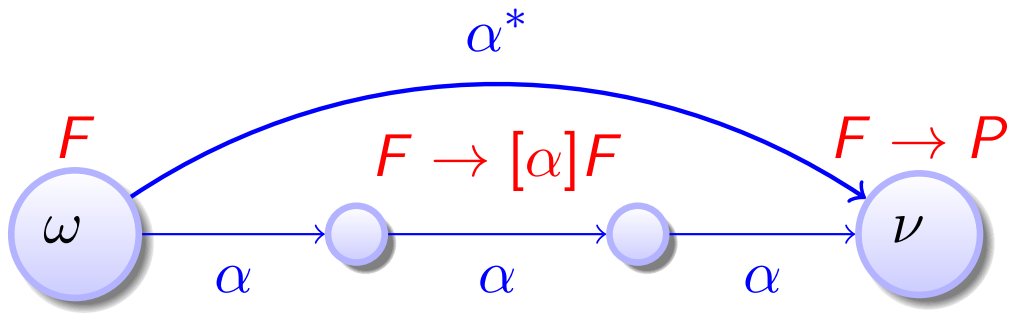
Lemma (Differential equations are their own loop)

$$[\![(x' = f(x))^*]\!] = [\![x' = f(x)]\!]$$

loop α^*	ODE $x' = f(x)$
repeat any number $n \in \mathbb{N}$ of times	evolve for any duration $r \in \mathbb{R}$
can repeat 0 times	can evolve for duration 0
effect depends on previous loop iteratior	effect depends on the past solution
local generator α	local generator $x' = f(x)$
full global execution trace	global solution $\varphi : [0, r] \to \mathcal{S}$
unwinding proof by iteration $[*]$	proof by global solution with $[']$
inductive proof with loop invariant	proof with differential invariant

Proofs for Loops

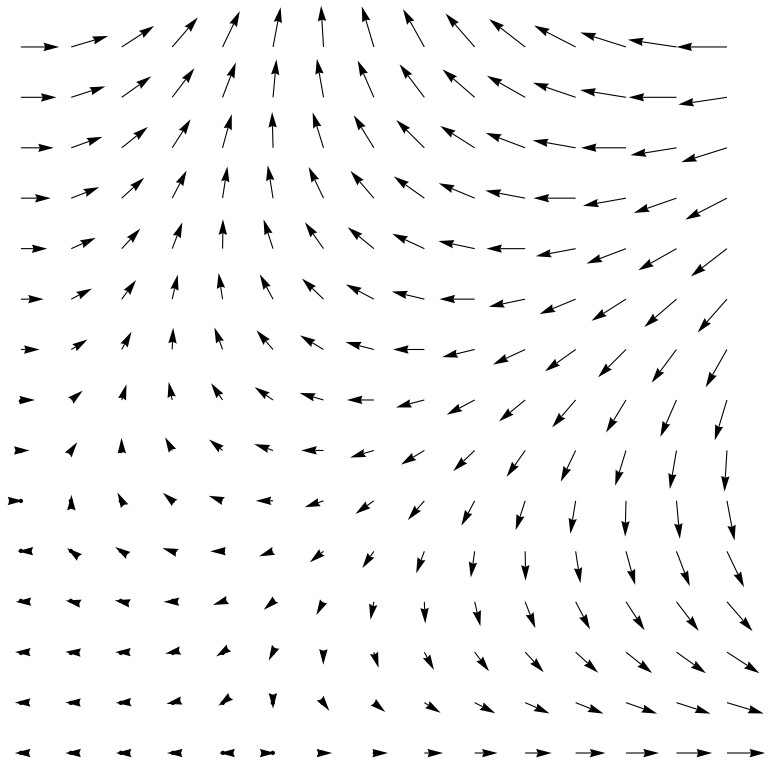
$$\text{loop}\ \frac{\Gamma \vdash F, \Delta \quad F \vdash [\alpha]F \quad F \vdash P}{\Gamma \vdash [\alpha^*]P, \Delta}$$



Intuition for Differential Invariants

Differential Invariant

$$\frac{\Gamma \vdash F, \Delta \quad F \vdash ???F \quad F \vdash P}{\Gamma \vdash [x' = f(x)]P, \Delta}$$

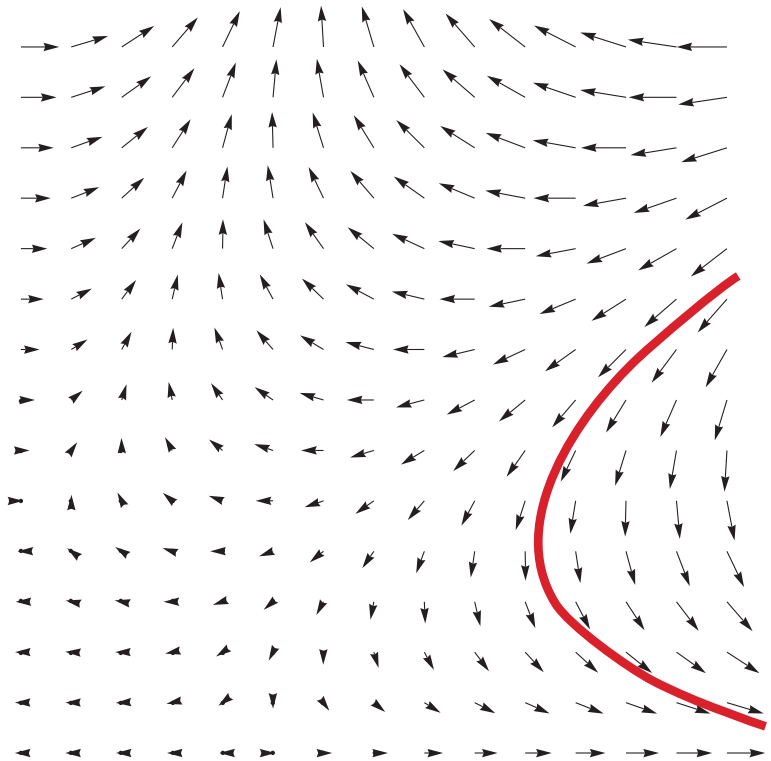


$$[']\ [x' = f(x)]P \leftrightarrow \forall t{\geq}0\, [x := y(t)]P \qquad \text{(y' =f(y), y(0)=x)}$$

Intuition for Differential Invariants

Differential Invariant

$$\frac{\Gamma \vdash F, \Delta \quad F \vdash ???F \quad F \vdash P}{\Gamma \vdash [x' = f(x)]P, \Delta}$$

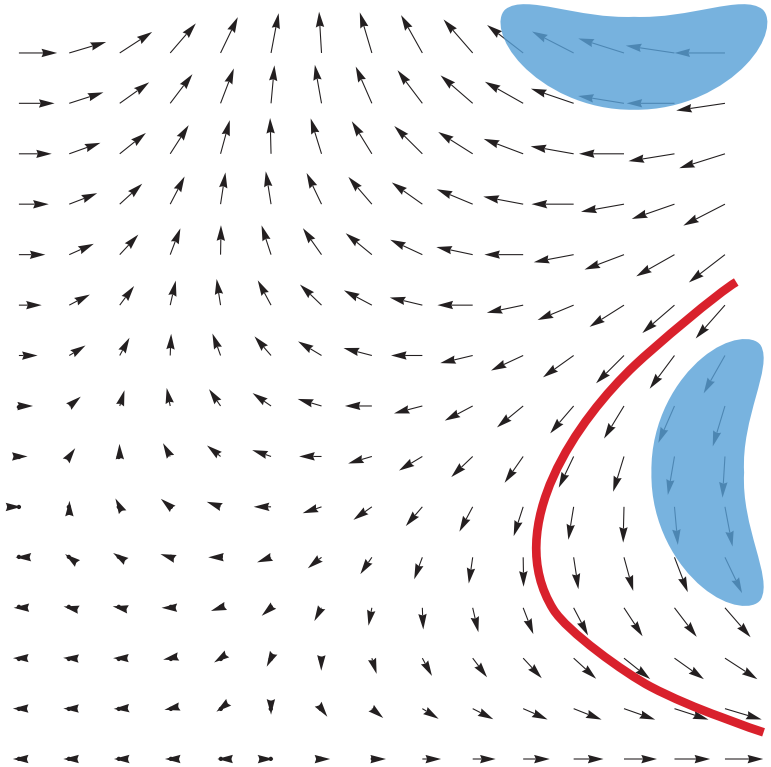


$$[']\ [x' = f(x)]P \leftrightarrow \forall t{\geq}0\, [x := y(t)]P \qquad \text{(y' =f(y), y(0)=x)}$$

Intuition for Differential Invariants

Differential Invariant

$$\frac{\Gamma \vdash F, \Delta \quad F \vdash ???F \quad F \vdash P}{\Gamma \vdash [x' = f(x)]P, \Delta}$$



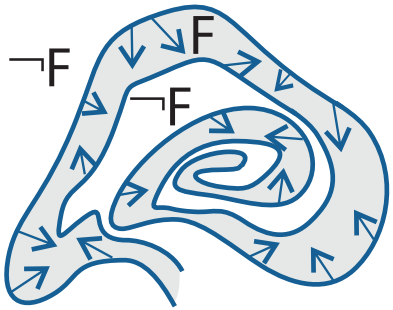
$$[']\ [x' = f(x)]P \leftrightarrow \forall t{\geq}0\, [x := y(t)]P \qquad \text{(y' =f(y), y(0)=x)}$$

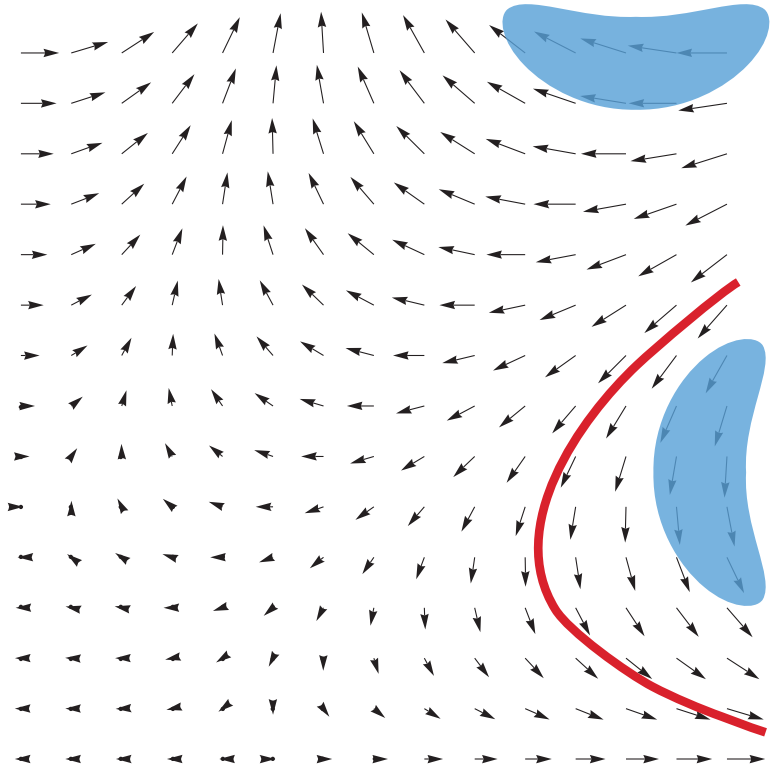
Intuition for Differential Invariants

Differential Invariant

$$\frac{\Gamma \vdash F, \Delta \quad F \vdash ???F \quad F \vdash P}{\Gamma \vdash [x' = f(x)]P, \Delta}$$

Want: F remains true in the direction of the dynamics





$$[']\ [x' = f(x)]P \leftrightarrow \forall t{\geq}0\, [x := y(t)]P \qquad (y' = f(y),\ y(0) = x)$$

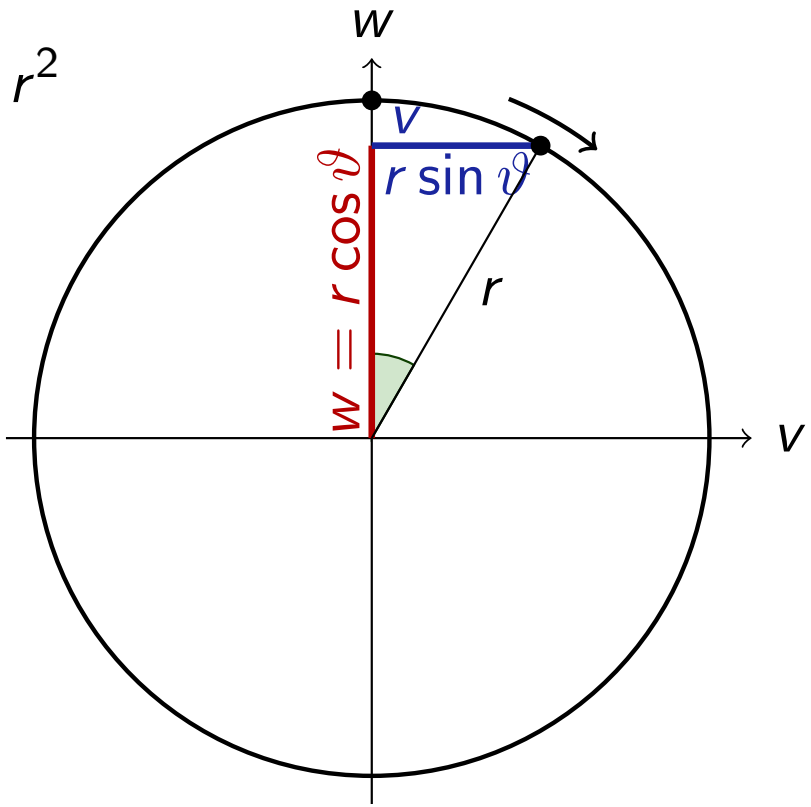
Don't need to know where exactly the system evolves to. Just that it remains somewhere in F.
Show: only evolves into directions in which formula F stays true.

Guiding Example

$$v^2+w^2 = r^2 \rightarrow [v' = w, w' = -v]v^2+w^2 = r^2$$

Guiding Example: Rotational Dynamics

$$v^2+w^2=r^2 \rightarrow [v'=w, w'=-v]v^2+w^2=r^2$$



Guiding Example: Rotational Dynamics

$$v^2+w^2 = r^2 \rightarrow [v' = w, w' = -v]v^2+w^2 = r^2$$

$$\rightarrow\text{R}\ \frac{}{\vdash\ v^2+w^2-r^2=0 \rightarrow [v' = w, w' = -v]v^2+w^2-r^2=0}$$

Derivatives for a Change

Syntax $e ::= x \mid c \mid e + k \mid e - k \mid e \cdot k \mid e/k$

Derivatives for a Change

Syntax $e ::= x \mid c \mid e + k \mid e - k \mid e \cdot k \mid e/k$

Derivatives

$$(e + k)' = (e)' + (k)'$$
$$(e - k)' = (e)' - (k)'$$
$$(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$$
$$(e/k)' = \big((e)' \cdot k - e \cdot (k)'\big)/k^2$$
$$(c())' = 0 \qquad \text{for constants/numbers } c()$$

Derivatives for a Change

Syntax $e ::= x \mid c \mid e + k \mid e - k \mid e \cdot k \mid e/k$

Derivatives

$$(e + k)' = (e)' + (k)'$$
$$(e - k)' = (e)' - (k)'$$
$$(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$$
$$(e/k)' = \big((e)' \cdot k - e \cdot (k)'\big)/k^2 \quad \text{same singularities}$$
$$(c())' = 0 \quad \text{for constants/numbers } c()$$

Derivatives for a Change

Syntax $e ::= x \mid c \mid e + k \mid e - k \mid e \cdot k \mid e/k$

Derivatives

$$(e + k)' = (e)' + (k)'$$
$$(e - k)' = (e)' - (k)'$$
$$(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$$
$$(e/k)' = \big((e)' \cdot k - e \cdot (k)'\big)/k^2 \quad \text{same singularities}$$
$$(c())' = 0 \quad \text{for constants/numbers } c()$$

. . . What do these primes mean? . . .

Derivatives for a Change

Syntax $e ::= x \mid c \mid e+k \mid e-k \mid e \cdot k \mid e/k \mid (e)'$

internalize primes into d$\mathcal{L}$ syntax

Derivatives

$$(e+k)' = (e)' + (k)'$$
$$(e-k)' = (e)' - (k)'$$
$$(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$$
$$(e/k)' = \big((e)' \cdot k - e \cdot (k)'\big)/k^2 \quad \text{same singularities}$$
$$(c())' = 0 \quad \text{for constants/numbers } c()$$

. . . What do these primes mean? . . .

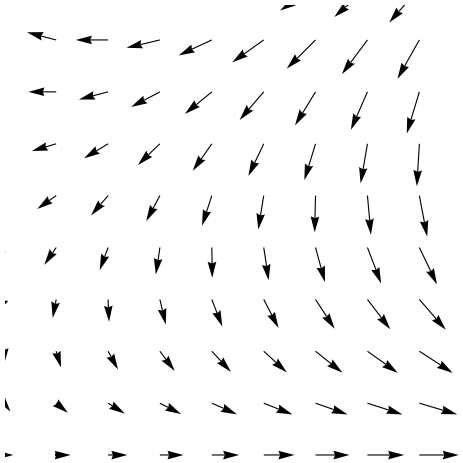
The Meaning of Prime

The Meaning of Prime

Semantics $[\![(e)']\!]\omega =$

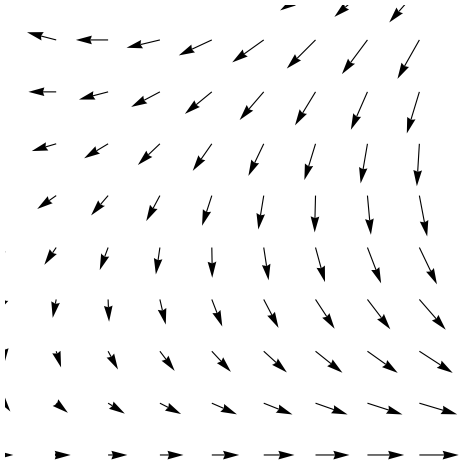
The Meaning of Prime

Semantics $[\![(e)']\!]\omega =$



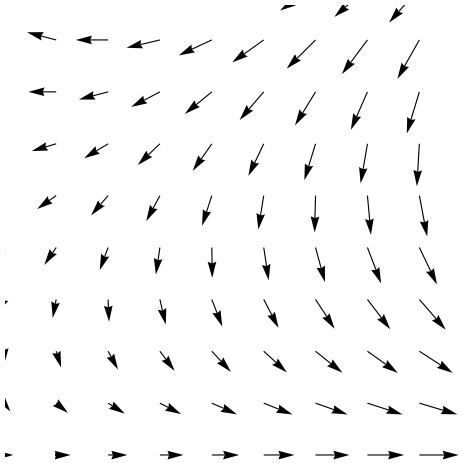
depends on the differential equation?

Semantics $[\![(e)']\!]\omega =$



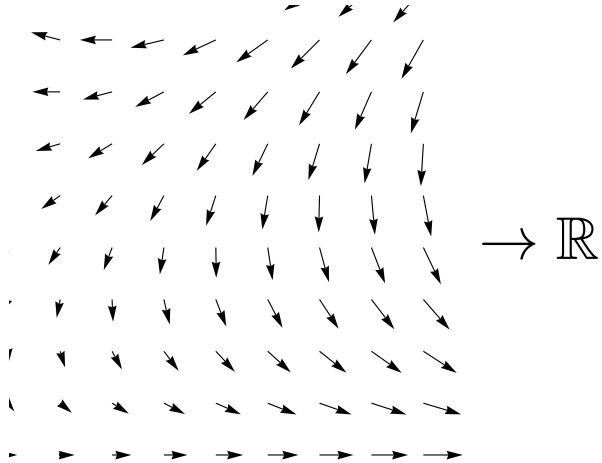
depends on the differential equation?
well-defined in isolated state ω at all?

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



depends on the differential equation?
well-defined in isolated state ω at all?

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



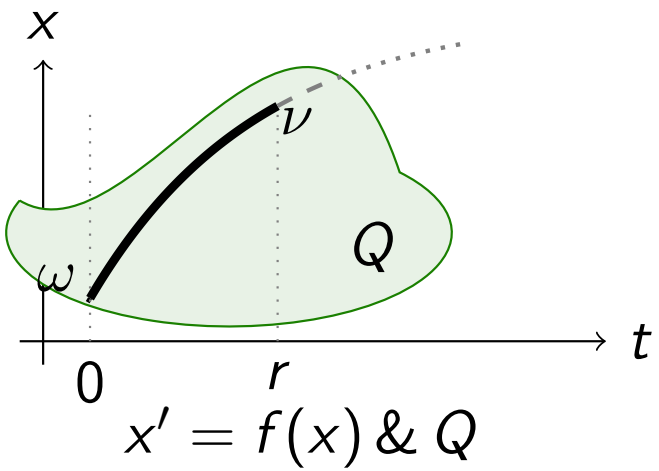
depends on the differential equation?
well-defined in isolated state ω at all?

Differential Dynamic Logic d$\mathcal{L}$: Semantics

Definition (Hybrid program semantics) $([\![\cdot]\!] : \text{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$

$$[\![x' = f(x) \,\&\, Q]\!] = \{(\varphi(0)|_{\{x'\}^{\complement}}, \varphi(r)) : \varphi(z) \models x' = f(x) \wedge Q \text{ for all } 0 \leq z \leq r$$
$$\text{for a solution } \varphi : [0, r] \to \mathcal{S} \text{ of any duration } r \in \mathbb{R}\}$$

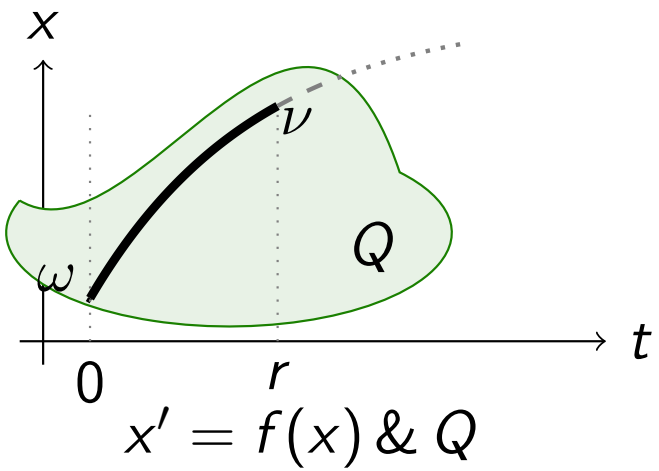
$$\text{where } \varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)$$



Differential Dynamic Logic d$\mathcal{L}$: Semantics

Definition (Hybrid program semantics) $([\![\cdot]\!] : \text{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$

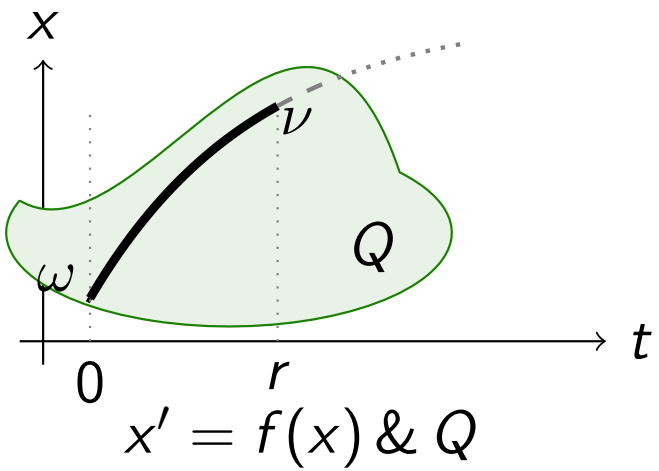
$$[\![x' = f(x)\,\&\,Q]\!] = \{(\omega,\nu) : \varphi(z) \models x' = f(x) \wedge Q \text{ for all } 0 \leq z \leq r$$
$$\text{for a solution } \varphi : [0,r] \to \mathcal{S} \text{ of any duration } r \in \mathbb{R}$$
$$\text{with } \varphi(0) = \omega \text{ and } \varphi(r) = \nu\}$$
$$\text{where } \varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)$$



Differential Dynamic Logic d$\mathcal{L}$: Semantics

Definition (Hybrid program semantics) $([\![\cdot]\!] : \text{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$

$$[\![x' = f(x) \,\&\, Q]\!] = \{(\omega, \nu) : \varphi(z) \models x' = f(x) \wedge Q \text{ for all } 0 \leq z \leq r$$
$$\text{for a solution } \varphi : [0, r] \to \mathcal{S} \text{ of any duration } r \in \mathbb{R}$$
$$\text{with } \varphi(0) = \omega \text{ except on } x' \text{ and } \varphi(r) = \nu\}$$
$$\text{where } \varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)$$

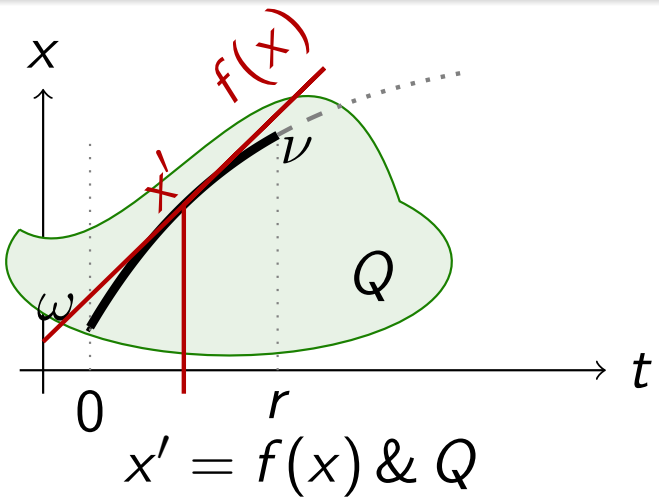


Initial value of x' in ω is irrelevant since defined by ODE.
Final value of x' is carried over to the final state ν.

Differential Dynamic Logic dℒ: Semantics

Definition (Hybrid program semantics) $([\![\cdot]\!] : \text{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$

$$[\![x' = f(x)\,\&\,Q]\!] = \{(\omega,\nu) : \varphi(z) \models x' = f(x) \wedge Q \text{ for all } 0 \leq z \leq r$$
$$\text{for a solution } \varphi : [0,r] \to \mathcal{S} \text{ of any duration } r \in \mathbb{R}$$
$$\text{with } \varphi(0) = \omega \text{ except on } x' \text{ and } \varphi(r) = \nu\}$$
$$\text{where } \varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)$$



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

Initial value of x' in ω is irrelevant since defined by ODE.
Final value of x' is carried over to the final state ν.

Differential Substitution Lemmas

Lemma (Differential lemma) (Differential value vs. Time-derivative)

If $\varphi \models x' = f(x) \land Q$ *for duration* $r > 0$, *then for all* $0 \leq z \leq r$:

Syntactic $[\![(e)']\!]\varphi(z) = \dfrac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$ Analytic

Lemma (Differential assignment) (Effect on Differentials)

If $\varphi \models x' = f(x) \land Q$ *then* $\varphi \models P \leftrightarrow [x' := f(x)]P$

Lemma (Derivations) (Equations of Differentials)

$$(e + k)' = (e)' + (k)'$$
$$(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$$
$$(c())' = 0 \qquad \text{for constants/numbers } c()$$
$$(x)' = x' \qquad \text{for variables } x \in \mathcal{V}$$

Differential Substitution Lemmas

Lemma (Differential lemma) (Differential value vs. Time-derivative)

If $\varphi \models x' = f(x) \land Q$ *for duration* $r > 0$, *then for all* $0 \leq z \leq r$:

$$[\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

Lemma (Differential assignment) (Effect on Differentials)

If $\varphi \models x' = f(x) \land Q$ *then* $\varphi \models P \leftrightarrow [x' := f(x)]P$

Axiomatics

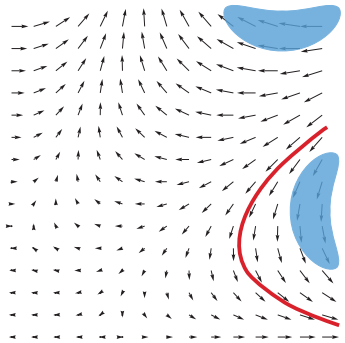
DE $[x' = f(x)\,\&\,Q]P \leftrightarrow [x' = f(x)\,\&\,Q][x' := f(x)]P$

DI $$\frac{\vdash [x' = f(x)\,\&\,Q](e)' = 0}{e = 0 \vdash [x' = f(x)\,\&\,Q]e = 0}$$

Differential Invariants for Differential Equations

Differential Invariant

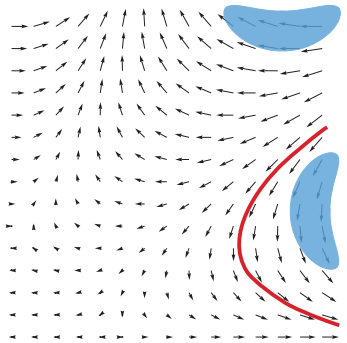
$$\mathrm{DI}_{=0}\ \frac{\vdash [x' := f(x)](e)' = 0}{e = 0 \vdash [x' = f(x)]e = 0}$$



Differential Invariants for Differential Equations

Differential Invariant

$$\text{DI}_{=0}\ \frac{\vdash [x' := f(x)](e)' = 0}{e = 0 \vdash [x' = f(x)]e = 0}$$



$$\text{DI}\ \frac{\vdash [x' = f(x)](e)' = 0}{e = 0 \vdash [x' = f(x)]e = 0} \qquad \text{DE}\ [x' = f(x)]P \leftrightarrow [x' = f(x)][x' := f(x)]P$$

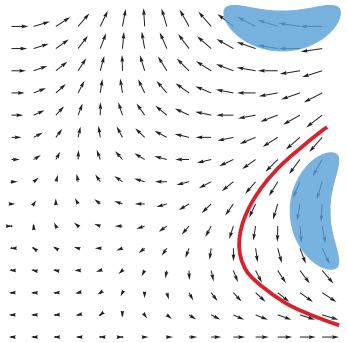
$\text{DI}_{=0}$ is a derived rule:

$$\text{DI}\ \frac{}{e = 0 \vdash [x' = f(x)]e = 0}$$

Differential Invariants for Differential Equations

Differential Invariant

$$\text{DI}_{=0}\ \frac{\vdash [x' := f(x)](e)' = 0}{e = 0 \vdash [x' = f(x)]e = 0}$$



$$\text{DI}\ \frac{\vdash [x' = f(x)](e)' = 0}{e = 0 \vdash [x' = f(x)]e = 0} \qquad \text{DE}\ [x' = f(x)]P \leftrightarrow [x' = f(x)][x' := f(x)]P$$

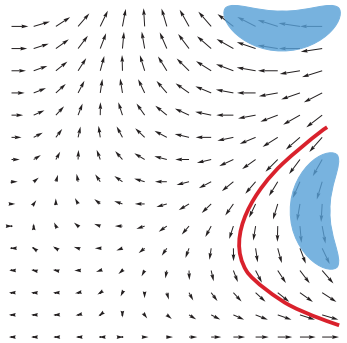
$\text{DI}_{=0}$ is a derived rule:

$$\text{DI}\ \frac{\text{DE}\ \dfrac{}{\vdash [x' = f(x)](e)' = 0}}{e = 0 \vdash [x' = f(x)]e = 0}$$

Differential Invariants for Differential Equations

Differential Invariant

$$\text{DI}_{=0}\ \frac{\vdash [x' := f(x)](e)' = 0}{e = 0 \vdash [x' = f(x)]e = 0}$$



$$\text{DI}\ \frac{\vdash [x' = f(x)](e)' = 0}{e = 0 \vdash [x' = f(x)]e = 0} \qquad \text{DE}\ [x' = f(x)]P \leftrightarrow [x' = f(x)][x' := f(x)]P$$

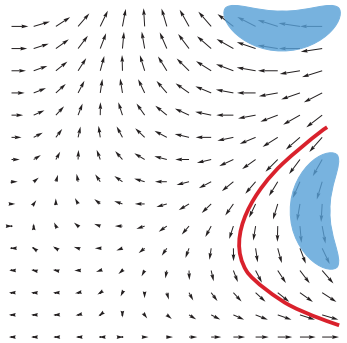
$\text{DI}_{=0}$ is a derived rule:

$$\cfrac{\cfrac{\cfrac{}{\vdash [x' = f(x)][x' := f(x)](e)' = 0}\,\text{G}}{\vdash [x' = f(x)](e)' = 0}\,\text{DE}}{e = 0 \vdash [x' = f(x)]e = 0}\,\text{DI}$$

Differential Invariants for Differential Equations

Differential Invariant

$$\text{DI}_{=0}\ \frac{\vdash [x' := f(x)](e)' = 0}{e = 0 \vdash [x' = f(x)]e = 0}$$



$$\text{DI}\ \frac{\vdash [x' = f(x)](e)' = 0}{e = 0 \vdash [x' = f(x)]e = 0} \qquad \text{DE}\ [x' = f(x)]P \leftrightarrow [x' = f(x)][x' := f(x)]P$$

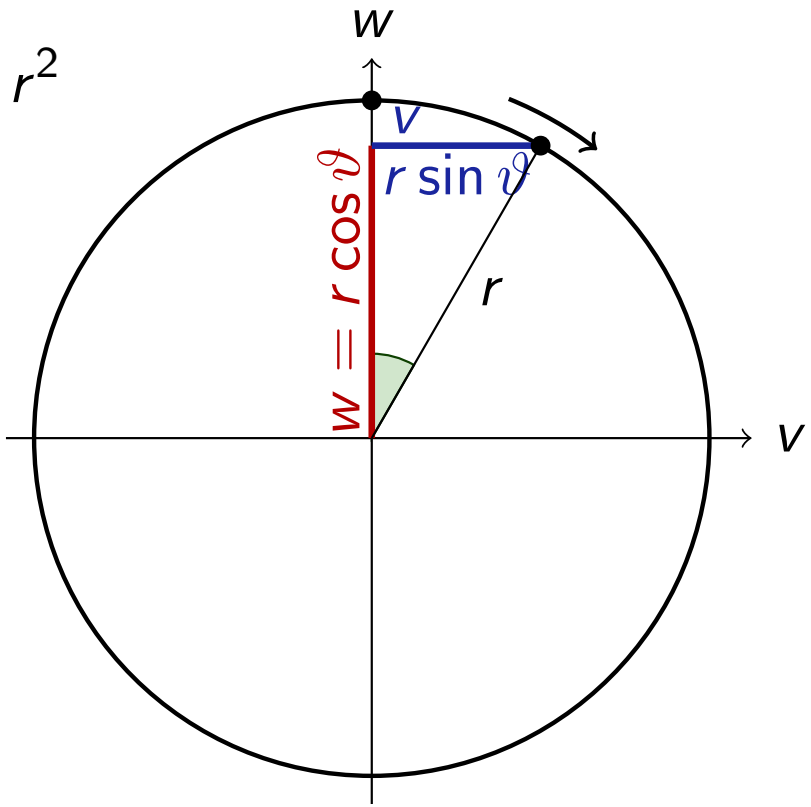
$\text{DI}_{=0}$ is a derived rule:

$$\text{DI}\ \frac{\text{DE}\ \dfrac{\text{G}\ \dfrac{\vdash [x' := f(x)](e)' = 0}{\vdash [x' = f(x)][x' := f(x)](e)' = 0}}{\vdash [x' = f(x)](e)' = 0}}{e = 0 \vdash [x' = f(x)]e = 0}$$

$$\text{G}\ \frac{P}{[\alpha]P}$$

Guiding Example: Rotational Dynamics

$$v^2+w^2=r^2 \rightarrow [v'=w, w'=-v]v^2+w^2=r^2$$



Guiding Example: Rotational Dynamics

$$v^2+w^2 = r^2 \rightarrow [v' = w, w' = -v]v^2+w^2 = r^2$$

$$\rightarrow\mathrm{R}\ \frac{}{\vdash\ v^2+w^2-r^2=0 \rightarrow [v' = w, w' = -v]v^2+w^2-r^2=0}$$

Guiding Example: Rotational Dynamics

$$v^2+w^2 = r^2 \rightarrow [v' = w, w' = -v]v^2+w^2 = r^2$$

$$\text{DI}_{=0}\frac{}{v^2+w^2-r^2=0 \vdash [v' = w, w' = -v]v^2 + w^2 - r^2 = 0}$$
$$\rightarrow\text{R}\frac{}{\vdash v^2+w^2-r^2=0 \rightarrow [v' = w, w' = -v]v^2+w^2-r^2=0}$$

Guiding Example: Rotational Dynamics

$$v^2+w^2 = r^2 \rightarrow [v' = w, w' = -v]v^2+w^2 = r^2$$

$$\dfrac{\dfrac{\dfrac{}{\vdash [v':=w][w':=-v]2vv' + 2ww' - r' = 0}[':=]}{v^2+w^2-r^2=0 \vdash [v' = w, w' = -v]v^2 + w^2 - r^2 = 0}\mathrm{DI}_{=0}}{\vdash v^2+w^2-r^2=0 \rightarrow [v' = w, w' = -v]v^2+w^2-r^2=0}\rightarrow\mathrm{R}$$

Guiding Example: Rotational Dynamics

$$v^2+w^2 = r^2 \rightarrow [v' = w, w' = -v]v^2+w^2 = r^2$$

$$\mathbb{R}\ \frac{}{\vdash 2v(w)+2w(-v)=0}$$

$$[':=]\ \frac{\vdash 2v(w)+2w(-v)=0}{\vdash [v':=w][w':=-v]2vv'+2ww'-r'=0}$$

$$\mathrm{DI}_{=0}\ \frac{\vdash [v':=w][w':=-v]2vv'+2ww'-r'=0}{v^2+w^2-r^2=0 \vdash [v' = w, w' = -v]v^2+w^2-r^2=0}$$

$$\rightarrow\mathrm{R}\ \frac{v^2+w^2-r^2=0 \vdash [v' = w, w' = -v]v^2+w^2-r^2=0}{\vdash v^2+w^2-r^2=0 \rightarrow [v' = w, w' = -v]v^2+w^2-r^2=0}$$

Guiding Example: Rotational Dynamics

$$v^2+w^2 = r^2 \rightarrow [v' = w, w' = -v]v^2+w^2 = r^2$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\mathbb{R}}\,*}{[':=]}}{\mathrm{DI}_{=0}}}{\rightarrow \mathrm{R}}$$

$$\begin{array}{l}
\vdash 2v(w) + 2w(-v) = 0 \\
\vdash [v':=w][w':=-v]2vv' + 2ww' - r' = 0 \\
v^2+w^2-r^2=0 \vdash [v' = w, w' = -v]v^2 + w^2 - r^2 = 0 \\
\vdash v^2+w^2-r^2=0 \rightarrow [v' = w, w' = -v]v^2+w^2-r^2=0
\end{array}$$

Guiding Example: Rotational Dynamics

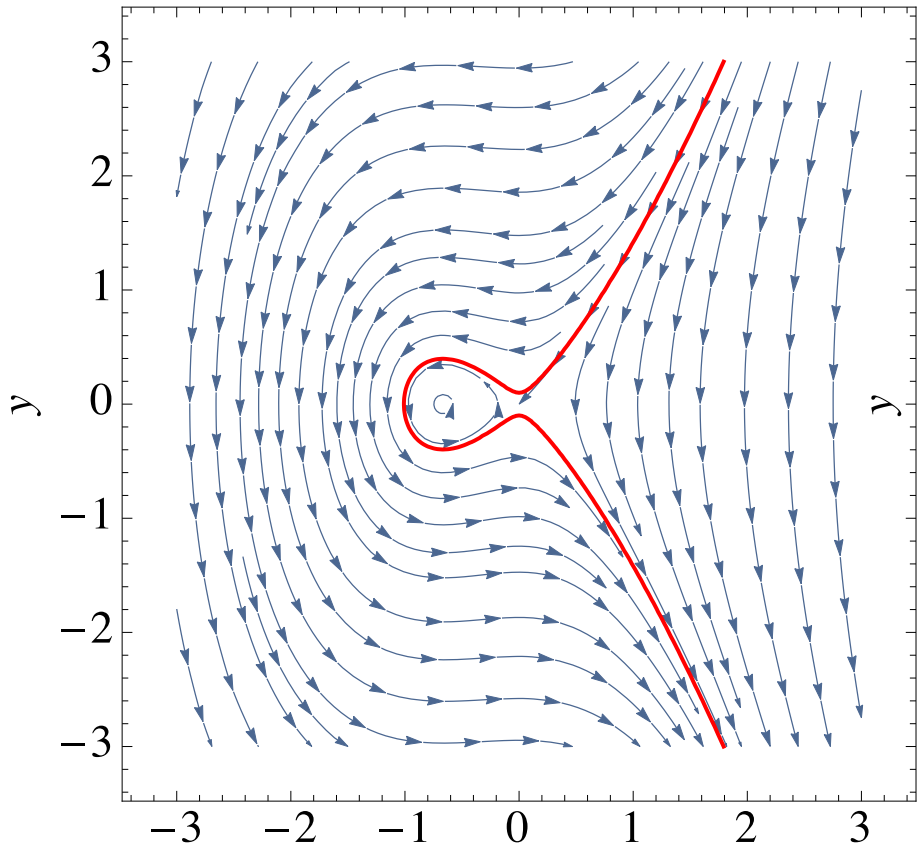
$$v^2+w^2 = r^2 \rightarrow [v' = w, w' = -v]v^2+w^2 = r^2$$

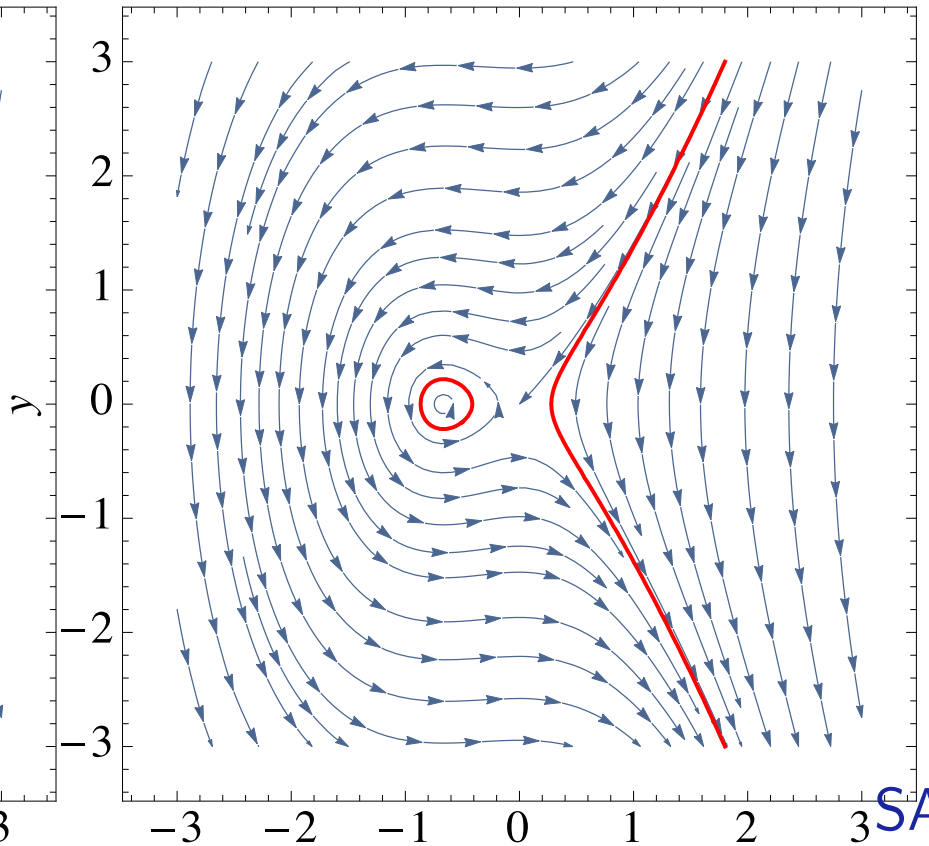
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash 2v(w)+2w(-v)=0}\,\mathbb{R}}{\vdash [v':=w][w':=-v]2vv'+2ww'-r'=0}\,[':=]}{v^2+w^2-r^2=0 \vdash [v' = w, w' = -v]v^2+w^2-r^2=0}\,\mathrm{DI}_{=0}}{\vdash v^2+w^2-r^2=0 \rightarrow [v' = w, w' = -v]v^2+w^2-r^2=0}\,\rightarrow\mathrm{R}}\ *$$

Simple proof without solving ODE

Example Proof: Self-crossing

$$\mathrm{DI}_{=0}\ \frac{}{x^2+x^3-y^2-c=0 \vdash [x'=-2y, y'=-2x-3x^2]x^2+x^3-y^2-c=0}$$

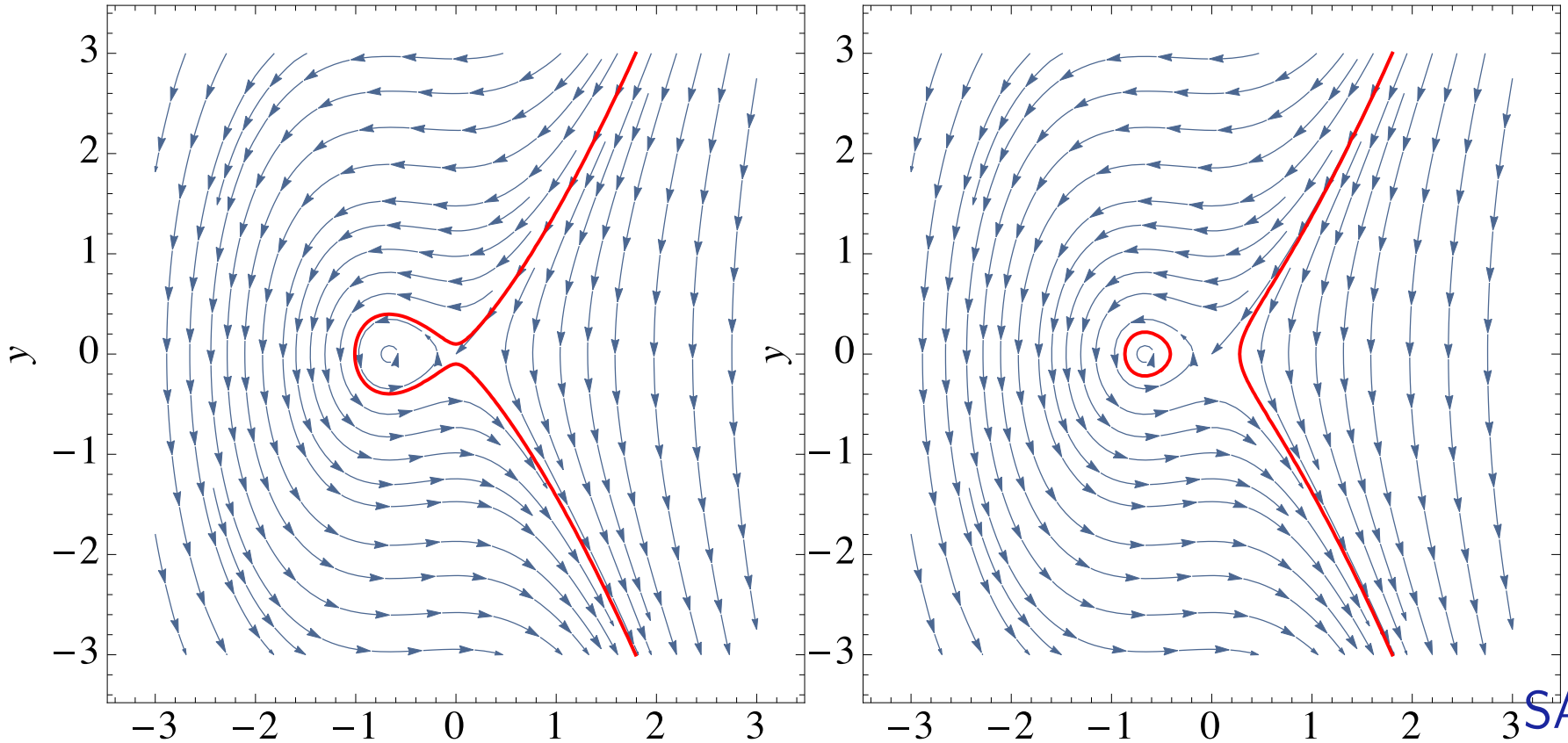




SAS'14

Example Proof: Self-crossing

$$\mathrm{DI}_{=0}\ \frac{[':=]\ \dfrac{}{\vdash [x':=-2y][y':=-2x-3x^2](2xx'+3x^2x'-2yy')=0}}{x^2+x^3-y^2-c=0 \vdash [x'=-2y, y'=-2x-3x^2]x^2+x^3-y^2-c=0}$$



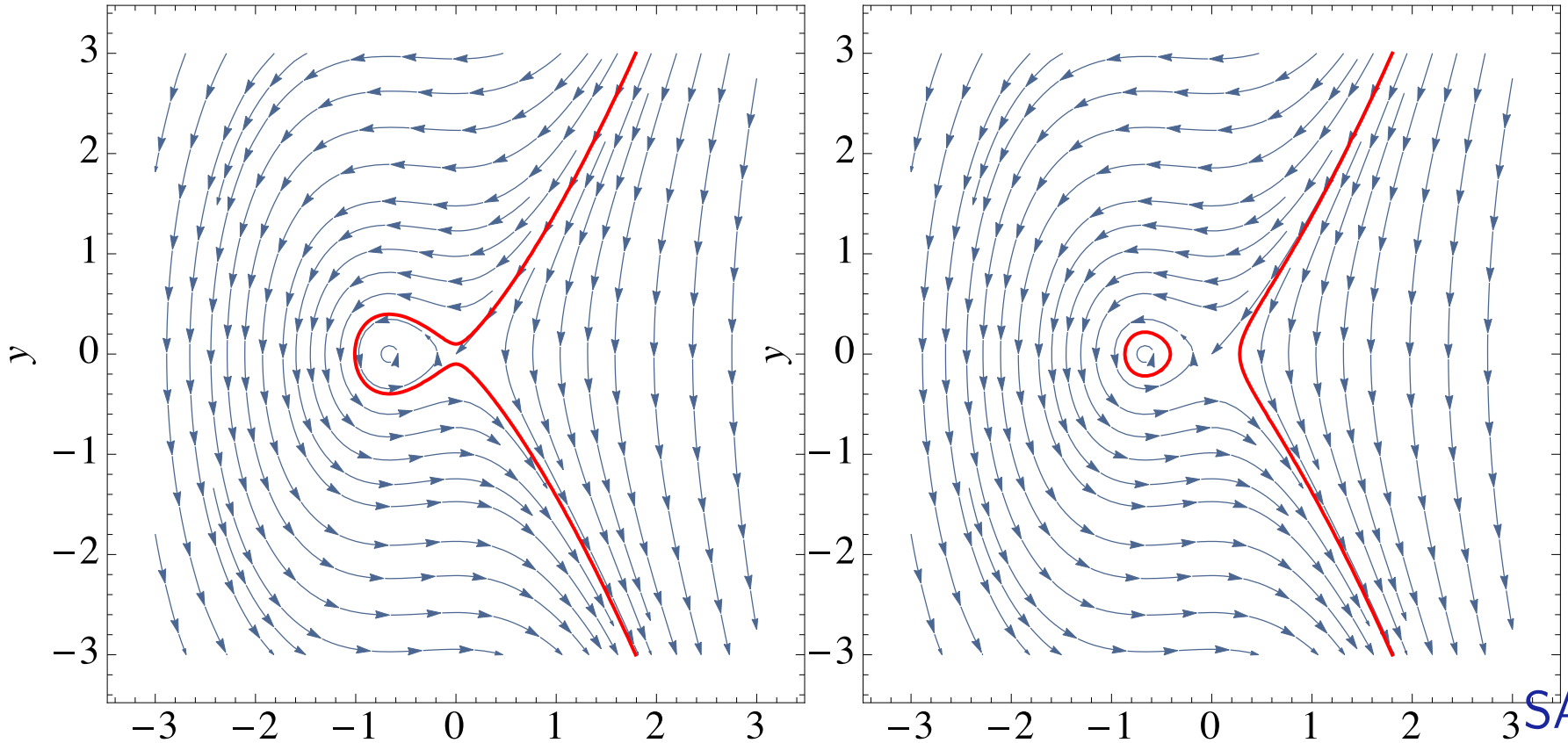
SAS'14

Example Proof: Self-crossing

$$\mathbb{R}\ \frac{}{\vdash 2x(-2y)+3x^2(-2y)-2y(-2x-3x^2)=0}$$

$$[':=]\ \frac{}{\vdash [x':=-2y][y':=-2x-3x^2](2xx'+3x^2x'-2yy')=0}$$

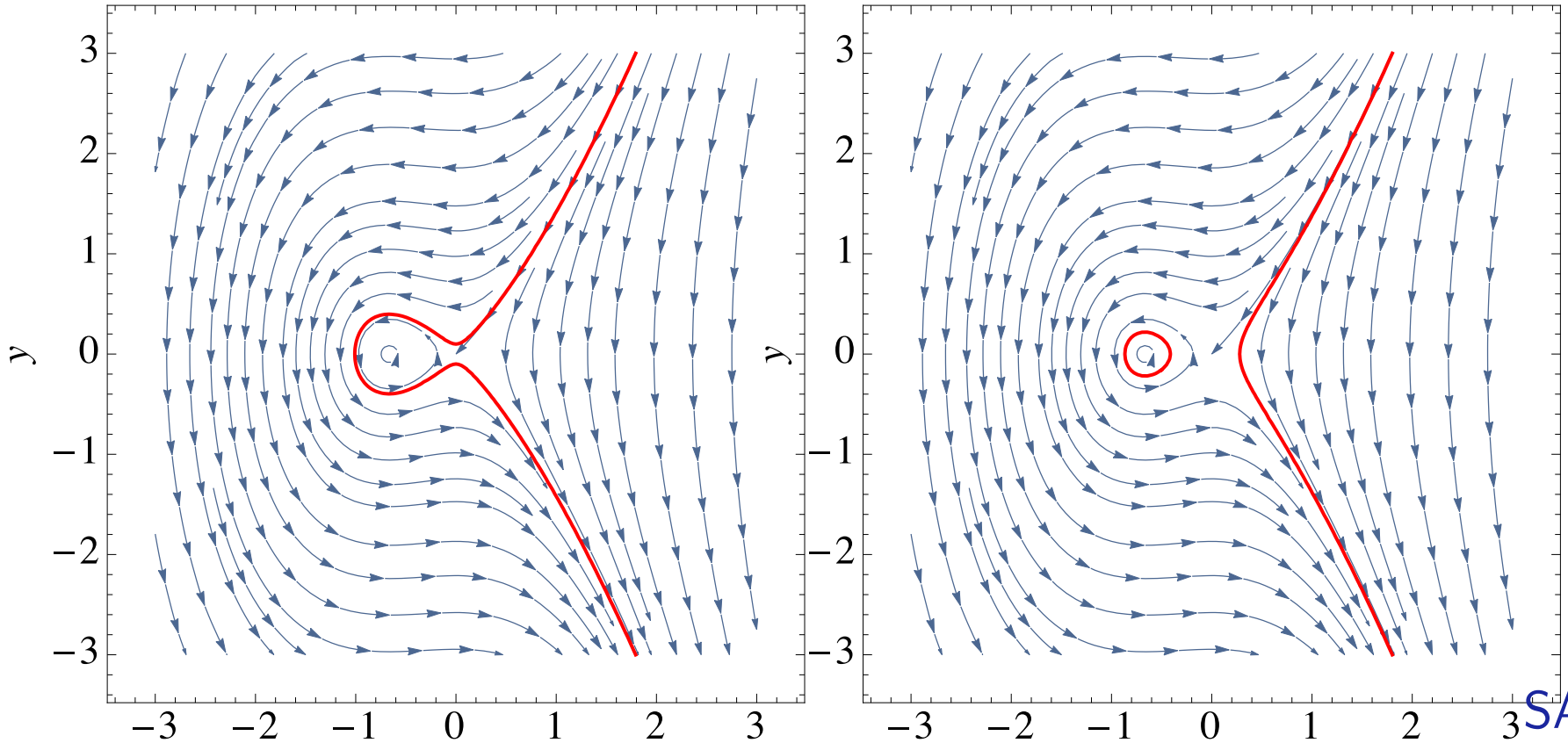
$$\mathrm{DI}_{=0}\ \frac{}{x^2+x^3-y^2-c=0 \vdash [x'=-2y, y'=-2x-3x^2]x^2+x^3-y^2-c=0}$$



SAS'14

Example Proof: Self-crossing

$$
\dfrac{\dfrac{\dfrac{}{\mathbb{R}}\ *}{[':=]}}{\mathrm{DI}_{=0}}
\qquad
\begin{array}{l}
\vdash 2x(-2y)+3x^2(-2y)-2y(-2x-3x^2)=0 \\
\vdash [x':=-2y][y':=-2x-3x^2](2xx'+3x^2x'-2yy')=0 \\
x^2+x^3-y^2-c=0 \vdash [x'=-2y, y'=-2x-3x^2]x^2+x^3-y^2-c=0
\end{array}
$$



SAS'14

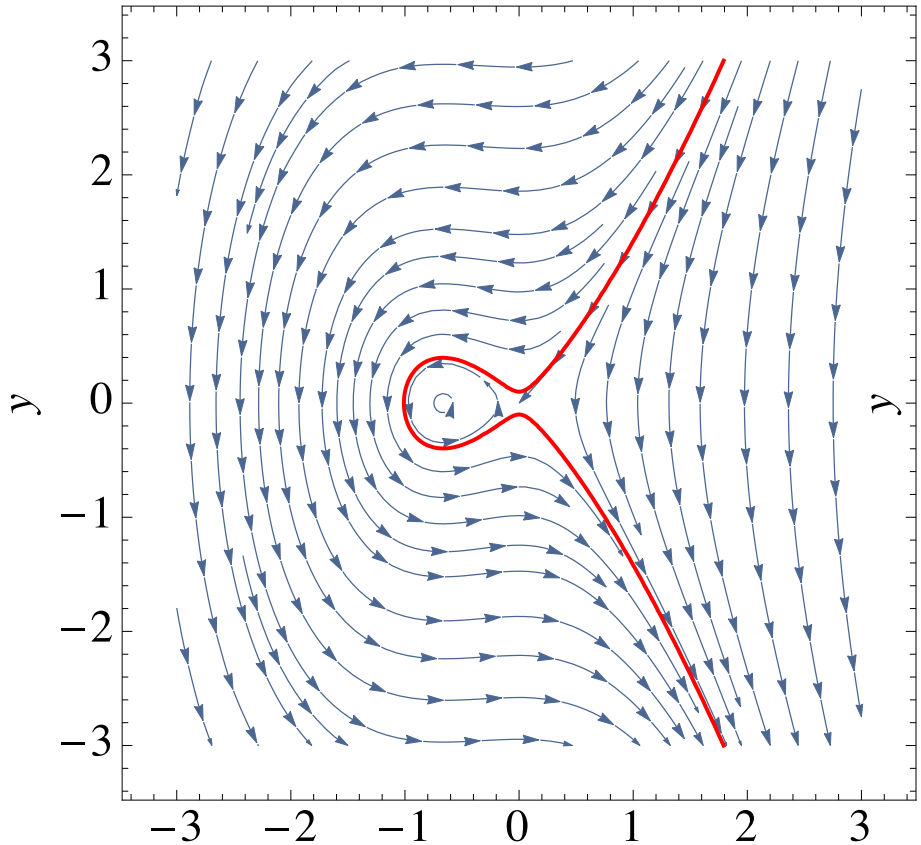
Example Proof: Self-crossing

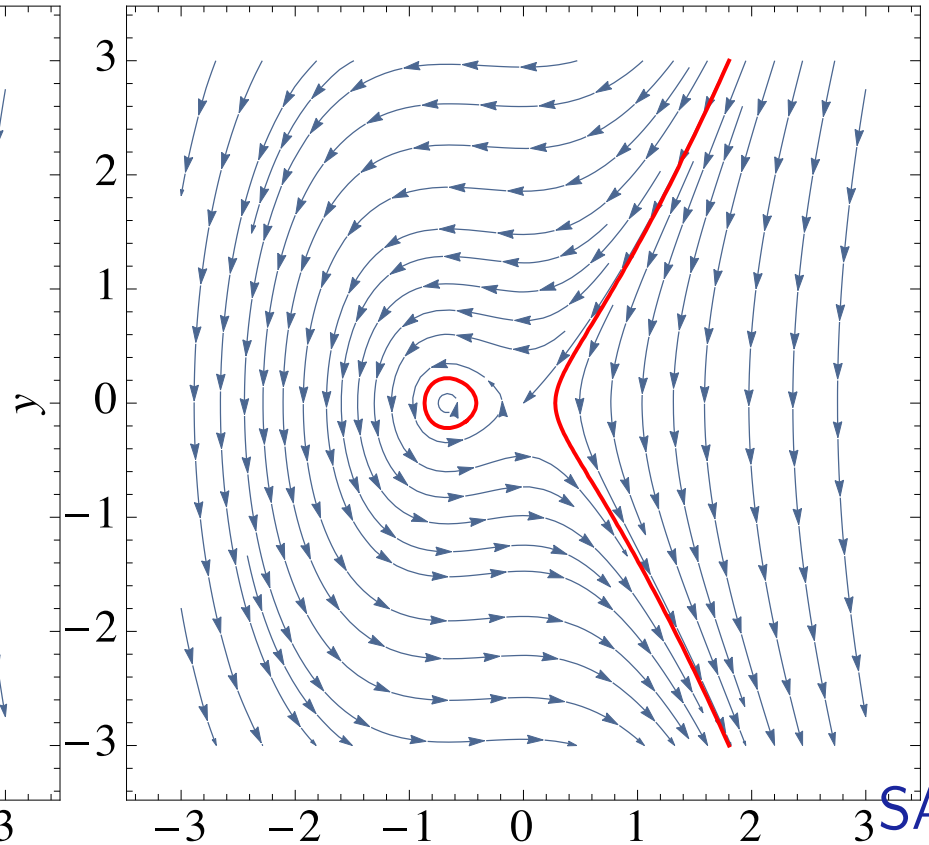
$$\dfrac{\dfrac{\dfrac{}{\mathbb{R}}\ *}{[':=]}}{\mathrm{DI}_{=0}}$$

$$\vdash 2x(-2y)+3x^2(-2y)-2y(-2x-3x^2)=0$$

$$\vdash [x':=-2y][y':=-2x-3x^2](2xx'+3x^2x'-2yy')=0$$

$$x^2+x^3-y^2-c=0 \vdash [x'=-2y, y'=-2x-3x^2]x^2+x^3-y^2-c=0$$

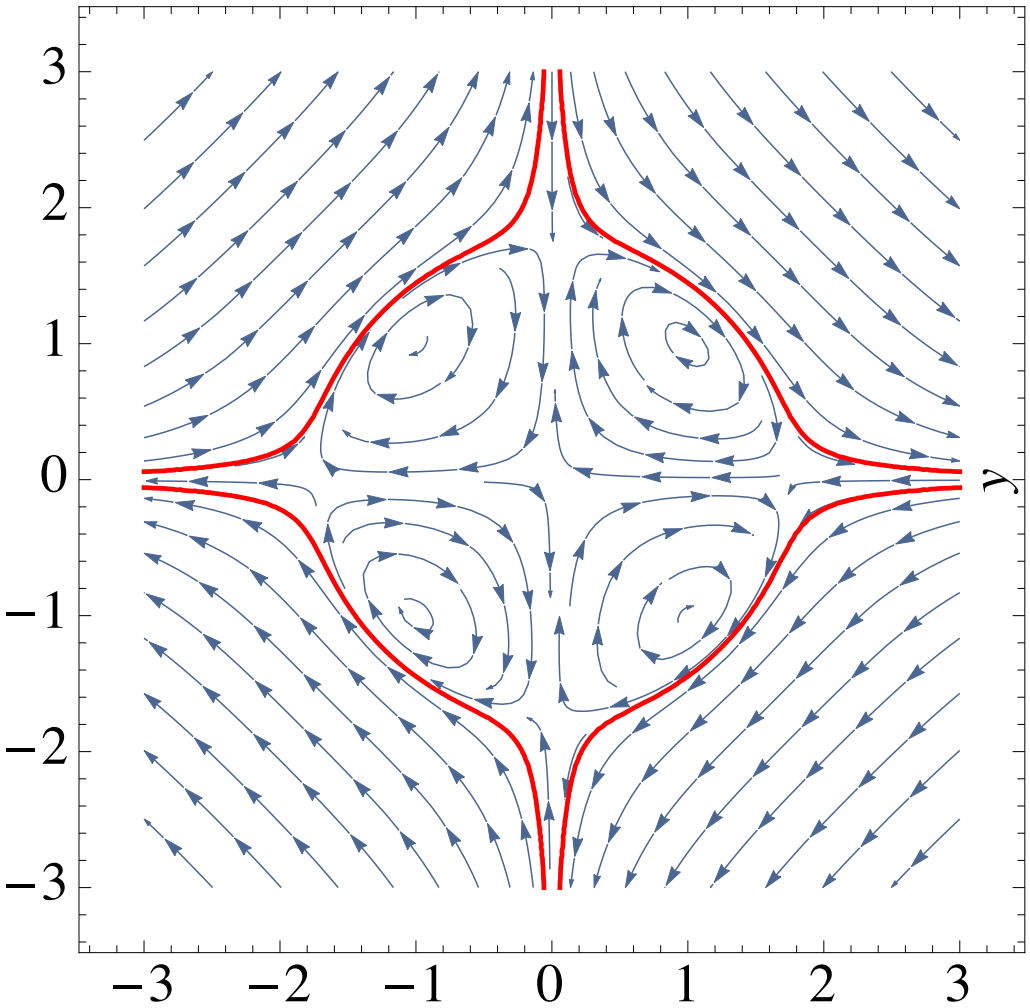


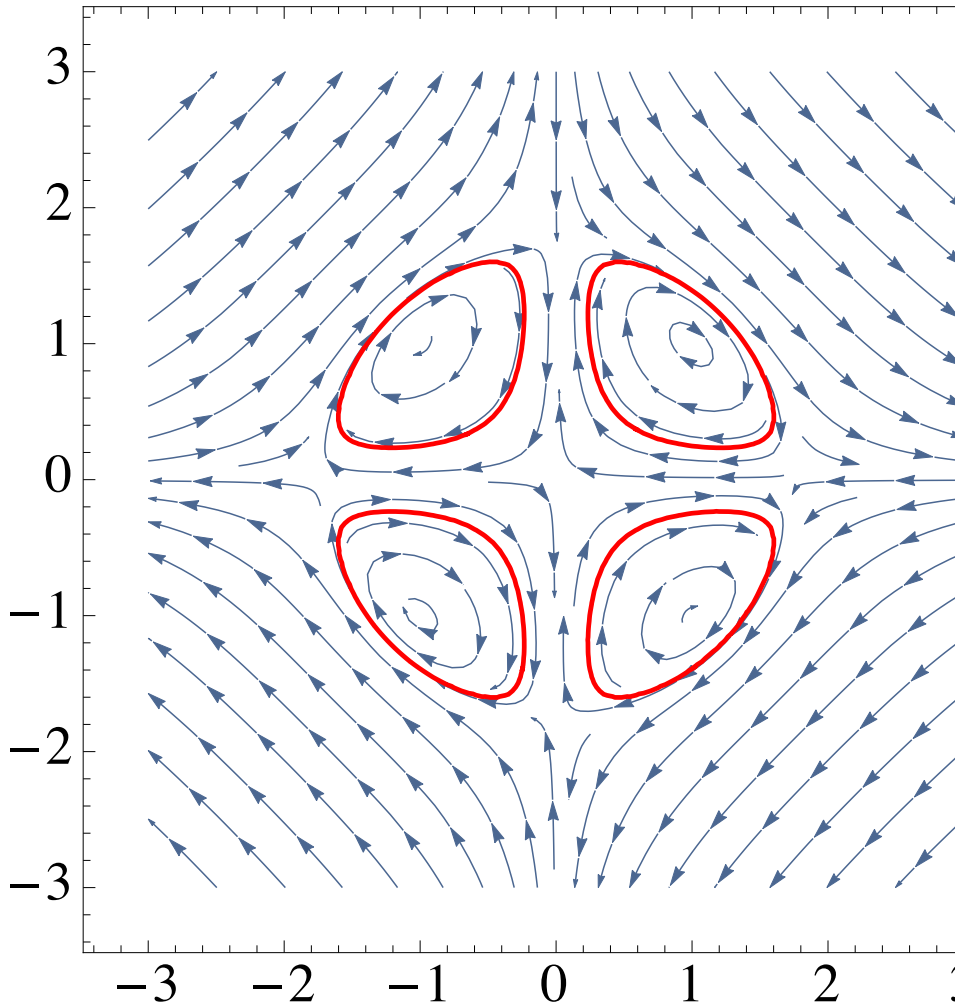


SAS'14

Example Proof: Motzkin

$$\ldots[x' = 2x^4y+4x^2y^3-6x^2y, y' = -4x^3y^2-2xy^4+6xy^2]x^4y^2+x^2y^4-3x^2y^2=c$$





SAS'14

Generalizing Differential Invariants

$$\rightarrow\mathrm{R}\ \frac{}{\vdash x^2+y^2=0 \rightarrow [x'=4y^3, y'=-4x^3]\, x^2+y^2=0}$$

Generalizing Differential Invariants

$$\text{cut,MR}\;\frac{\dfrac{}{x^2+y^2=0 \vdash [x'=4y^3,y'=-4x^3]\,x^2+y^2=0}}{\to\text{R}\;\vdash x^2+y^2=0 \to [x'=4y^3,y'=-4x^3]\,x^2+y^2=0}$$

Generalizing Differential Invariants

$$\dfrac{\dfrac{\dfrac{}{x^4+y^4=0 \vdash [x'=4y^3,y'=-4x^3]\,x^4+y^4=0}\,\mathrm{DI}_{=0}}{x^2+y^2=0 \vdash [x'=4y^3,y'=-4x^3]\,x^2+y^2=0}\,\mathrm{cut,MR}}{\vdash x^2+y^2=0 \to [x'=4y^3,y'=-4x^3]\,x^2+y^2=0}\,{\to}\mathrm{R}$$

Generalizing Differential Invariants

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{\vdash [x':=4y^3][y':=-4x^3](4x^3x' + 4y^3y') = 0}\,[':=]
}{x^4 + y^4 = 0 \vdash [x' = 4y^3, y' = -4x^3]\, x^4 + y^4 = 0}\,\mathrm{DI}_{=0}
}{x^2 + y^2 = 0 \vdash [x' = 4y^3, y' = -4x^3]\, x^2 + y^2 = 0}\,\mathrm{cut,MR}
}{\vdash x^2 + y^2 = 0 \to [x' = 4y^3, y' = -4x^3]\, x^2 + y^2 = 0}\,{\to}\mathrm{R}
$$

Generalizing Differential Invariants

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash 4x^3(4y^3)+4y^3(-4x^3)=0}\,\mathbb{R}}{\vdash [x'{:=}4y^3][y'{:=}-4x^3](4x^3x'+4y^3y')=0}\,[':=]}{x^4+y^4=0 \vdash [x'=4y^3,y'=-4x^3]\,x^4+y^4=0}\,\mathrm{DI}_{=0}}{x^2+y^2=0 \vdash [x'=4y^3,y'=-4x^3]\,x^2+y^2=0}\,\text{cut,MR}}{\vdash x^2+y^2=0 \to [x'=4y^3,y'=-4x^3]\,x^2+y^2=0}\,{\to}\mathrm{R}
$$

Generalizing Differential Invariants

$$
\begin{array}{lll}
 & & * \\
\mathbb{R} & & \vdash 4x^3(4y^3)+4y^3(-4x^3)=0 \\
[':=] & & \vdash [x':=4y^3][y':=-4x^3](4x^3x'+4y^3y')=0 \\
\mathrm{DI}_{=0} & x^4+y^4=0 & \vdash [x'=4y^3,y'=-4x^3]\,x^4+y^4=0 \\
\text{cut,MR} & x^2+y^2=0 & \vdash [x'=4y^3,y'=-4x^3]\,x^2+y^2=0 \\
\to\mathrm{R} & & \vdash x^2+y^2=0 \to [x'=4y^3,y'=-4x^3]\,x^2+y^2=0
\end{array}
$$

Generalizing Differential Invariants

$$
\begin{array}{ll}
 & * \\
\hline
\mathbb{R} & \vdash 4x^3(4y^3)+4y^3(-4x^3)=0 \\
\hline
[':=] & \vdash [x':=4y^3][y':=-4x^3](4x^3x'+4y^3y')=0 \\
\hline
\mathrm{DI}_{=0} & x^4+y^4=0 \vdash [x'=4y^3,y'=-4x^3]\,x^4+y^4=0 \\
\hline
\text{cut,MR} & x^2+y^2=0 \vdash [x'=4y^3,y'=-4x^3]\,x^2+y^2=0 \\
\hline
\to\mathrm{R} & \vdash x^2+y^2=0 \to [x'=4y^3,y'=-4x^3]\,x^2+y^2=0
\end{array}
$$

Generalizing Differential Invariants

$$
\begin{array}{rl}
 & * \\
\hline
\mathbb{R} & \vdash 4x^3(4y^3)+4y^3(-4x^3)=0 \\
\hline
[':=] & \vdash [x':=4y^3][y':=-4x^3](4x^3x'+4y^3y')=0 \\
\hline
\mathrm{DI}_{=0} & x^4+y^4=0 \vdash [x'=4y^3,y'=-4x^3]\,x^4+y^4=0 \\
\hline
\text{cut,MR} & x^2+y^2=0 \vdash [x'=4y^3,y'=-4x^3]\,x^2+y^2=0 \\
\hline
\to\mathrm{R} & \vdash x^2+y^2=0 \to [x'=4y^3,y'=-4x^3]\,x^2+y^2=0
\end{array}
$$

Theorem (Lie)

$$DI_c \quad \frac{Q \vdash [x':=f(x)](e)'=0}{\forall c\,\big(e=c \to [x'=f(x)\,\&\,Q]e=c\big)}$$

premise and conclusion are equivalent if Q is a domain, i.e. characterizing a connected open set.

Generalizing Differential Invariants

$$
\begin{array}{ll}
 & * \\
\hline
\mathbb{R} & \vdash 4x^3(4y^3)+4y^3(-4x^3)=0 \\
\hline
[':=] & \vdash [x':=4y^3][y':=-4x^3](4x^3x'+4y^3y')=0 \\
\hline
\mathrm{DI}_{=0} & x^4+y^4=0 \vdash [x'=4y^3,y'=-4x^3]\,x^4+y^4=0 \\
\hline
\text{cut,MR} & x^2+y^2=0 \vdash [x'=4y^3,y'=-4x^3]\,x^2+y^2=0 \\
\hline
\to\mathrm{R} & \vdash x^2+y^2=0 \to [x'=4y^3,y'=-4x^3]\,x^2+y^2=0
\end{array}
$$

Theorem (Lie)

$$
DI_c \quad \frac{Q \vdash [x':=f(x)](e)'=0}{\forall c\,\big(e=c \to [x'=f(x)\,\&\,Q]e=c\big)}
$$

premise and conclusion are equivalent if Q is a domain, i.e. characterizing a connected open set.

Clou: $(e-c)'=(e)'$ independent of additive constants

Strengthening Induction Hypotheses

Stronger Induction Hypotheses

1. As usual in math and in proofs with loops:
2. Inductive proofs may need stronger induction hypotheses to succeed.
3. Differentially inductive proofs may need a stronger differential inductive structure to succeed.
4. Even if $\{(x,y) \in \mathbb{R}^2 \ : \ x^2 + y^2 = 0\} = \{\{(x,y) \in \mathbb{R}^2 \ : \ x^4 + y^4 = 0\}$ have the same solutions, they have different differential structure.

Outline

1. Learning Objectives
2. Differential Equations
   - Descriptive Power of Differential Equations
   - Differential Equations vs. Loops
   - Intuition for Differential Invariants
   - Example: Rotation
   - Derivatives for a Change
   - The Meaning of Prime
   - Semantics of Differential Equations
   - Soundness
   - Example Proofs
3. Soundness Proof
4. Summary

Differential Substitution Lemmas

Lemma (Differential lemma) **(Differential value vs. Time-derivative)**

If $\varphi \models x' = f(x) \land Q$ *for duration* $r > 0$, *then for all* $0 \leq z \leq r$:

Syntactic $[\![(e)']\!]\varphi(z) = \dfrac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$ Analytic

Lemma (Differential assignment) **(Effect on Differentials)**

If $\varphi \models x' = f(x) \land Q$ *then* $\varphi \models P \leftrightarrow [x' := f(x)]P$

Lemma (Derivations) **(Equations of Differentials)**

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

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

$$(c())' = 0 \qquad \text{for constants/numbers } c()$$

$$(x)' = x' \qquad \text{for variables } x \in \mathcal{V}$$

Soundness Proof

Lemma (Differential lemma) **(Differential value vs. Time-derivative)**

If $\varphi \models x' = f(x) \wedge Q$ *for duration* $r > 0$, *then for all* $0 \leq z \leq r$:

$$[\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

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

Definition (Hybrid program semantics) $([\![\cdot]\!] : \mathrm{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$

$$[\![x' = f(x)\,\&\,Q]\!] = \{(\varphi(0), \varphi(r)) : \varphi(z) \models x' = f(x) \wedge Q \text{ for all } 0 \leq z \leq r$$
$$\text{for a } \varphi : [0, r] \to \mathcal{S} \text{ where } \varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)\}$$

Soundness Proof

Lemma (Differential lemma) (Differential value vs. Time-derivative)

If $\varphi \models x' = f(x) \wedge Q$ *for duration* $r > 0$, *then for all* $0 \leq z \leq r$:

$$[\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

$$\frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

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

Definition (Hybrid program semantics) ($[\![\cdot]\!] : \mathrm{HP} \to \wp(\mathcal{S} \times \mathcal{S})$)

$$[\![x' = f(x)\,\&\,Q]\!] = \{(\varphi(0), \varphi(r)) : \varphi(z) \models x' = f(x) \wedge Q \text{ for all } 0 \leq z \leq r$$
$$\text{for a } \varphi : [0, r] \to \mathcal{S} \text{ where } \varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)\}$$

Soundness Proof

Lemma (Differential lemma) (Differential value vs. Time-derivative)

If $\varphi \models x' = f(x) \wedge Q$ *for duration* $r > 0$, *then for all* $0 \leq z \leq r$:

$$[\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

$$\frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z) \overset{\text{chain}}{=} \sum_x \frac{\partial[\![e]\!]}{\partial x}(\varphi(z))\frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)$$

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

Definition (Hybrid program semantics) ($[\![\cdot]\!] : \mathrm{HP} \to \wp(\mathcal{S} \times \mathcal{S})$)

$$[\![x' = f(x)\,\&\,Q]\!] = \{(\varphi(0), \varphi(r)) : \varphi(z) \models x' = f(x) \wedge Q \text{ for all } 0 \leq z \leq r$$
$$\text{for a } \varphi : [0, r] \to \mathcal{S} \text{ where } \varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)\}$$

Soundness Proof

Lemma (Differential lemma) (Differential value vs. Time-derivative)

If $\varphi \models x' = f(x) \wedge Q$ *for duration* $r > 0$, *then for all* $0 \leq z \leq r$:

$$[\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

$$\frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z) \overset{\text{chain}}{=} \sum_x \frac{\partial[\![e]\!]}{\partial x}(\varphi(z))\frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)$$

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

Definition (Hybrid program semantics) ($[\![\cdot]\!] : \mathrm{HP} \to \wp(\mathcal{S} \times \mathcal{S})$)

$$[\![x' = f(x)\,\&\,Q]\!] = \{(\varphi(0), \varphi(r)) : \varphi(z) \models x' = f(x) \wedge Q \text{ for all } 0 \leq z \leq r$$
$$\text{for a } \varphi : [0, r] \to \mathcal{S} \text{ where } \varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)\}$$

Soundness Proof

Lemma (Differential lemma) (Differential value vs. Time-derivative)

If $\varphi \models x' = f(x) \wedge Q$ *for duration* $r > 0$, *then for all* $0 \leq z \leq r$:

$$[\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

$$\frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z) \overset{\text{chain}}{=} \sum_x \frac{\partial[\![e]\!]}{\partial x}(\varphi(z))\frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z) = \sum_x \frac{\partial[\![e]\!]}{\partial x}(\varphi(z))\varphi(z)(x')$$

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

Definition (Hybrid program semantics) ($[\![\cdot]\!] : \mathrm{HP} \to \wp(\mathcal{S} \times \mathcal{S})$)

$$[\![x' = f(x)\,\&\,Q]\!] = \{(\varphi(0), \varphi(r)) : \varphi(z) \models x' = f(x) \wedge Q \text{ for all } 0 \leq z \leq r$$
$$\text{for a } \varphi : [0, r] \to \mathcal{S} \text{ where } \varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)\}$$

Soundness Proof

Lemma (Differential lemma) **(Differential value vs. Time-derivative)**

If $\varphi \models x' = f(x) \wedge Q$ *for duration* $r > 0$, *then for all* $0 \leq z \leq r$:

$$[\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

$$\frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z) \overset{\text{chain}}{=} \sum_x \frac{\partial[\![e]\!]}{\partial x}(\varphi(z))\frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z) = \sum_x \frac{\partial[\![e]\!]}{\partial x}(\varphi(z))\varphi(z)(x')$$

Semantics $[\![(e)']\!]\varphi(z) = \sum_x \varphi(z)(x')\frac{\partial[\![e]\!]}{\partial x}(\varphi(z))$

Definition (Hybrid program semantics) **($[\![\cdot]\!] : \mathrm{HP} \to \wp(\mathcal{S} \times \mathcal{S})$)**

$$[\![x' = f(x)\,\&\,Q]\!] = \{(\varphi(0), \varphi(r)) : \varphi(z) \models x' = f(x) \wedge Q \text{ for all } 0 \leq z \leq r$$
$$\text{for a } \varphi : [0, r] \to \mathcal{S} \text{ where } \varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)\}$$

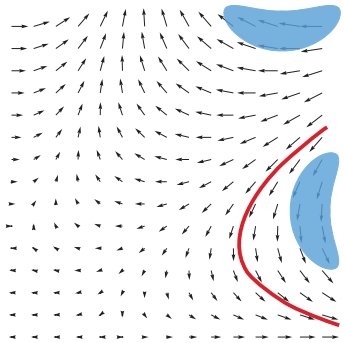
Outline

1. Learning Objectives
2. Differential Equations
   - Descriptive Power of Differential Equations
   - Differential Equations vs. Loops
   - Intuition for Differential Invariants
   - Example: Rotation
   - Derivatives for a Change
   - The Meaning of Prime
   - Semantics of Differential Equations
   - Soundness
   - Example Proofs
3. Soundness Proof
4. Summary

Differential Invariants for Differential Equations

Differential Invariant

$$\mathrm{DI}_{=0}\ \frac{\vdash [x' := f(x)](e)' = 0}{e = 0 \vdash [x' = f(x)]e = 0}$$



Differential Substitution Lemmas

Lemma (Differential lemma) **(Differential value vs. Time-derivative)**

If $\varphi \models x' = f(x) \land Q$ *for duration* $r > 0$, *then for all* $0 \leq z \leq r$:

Syntactic $[\![(e)']\!]\varphi(z) = \dfrac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$ Analytic

Lemma (Differential assignment) **(Effect on Differentials)**

If $\varphi \models x' = f(x) \land Q$ *then* $\varphi \models P \leftrightarrow [x' := f(x)]P$

Lemma (Derivations) **(Equations of Differentials)**

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

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

$$(c())' = 0 \qquad \text{for constants/numbers } c()$$

$$(x)' = x' \qquad \text{for variables } x \in \mathcal{V}$$


André Platzer.
Foundations of cyber-physical systems.
Lecture Notes 15-424/624, Carnegie Mellon University, 2016.
URL: http://www.cs.cmu.edu/~aplatzer/course/fcps16.html.


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. Springer, 2015.
doi:10.1007/978-3-319-21401-6_32.


André Platzer.
Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.
Springer, Heidelberg, 2010.
doi:10.1007/978-3-642-14509-4.


André Platzer.
Logics of dynamical systems.
In *LICS*, pages 13–24. IEEE, 2012.

doi:10.1109/LICS.2012.13.


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.
The structure of differential invariants and differential cut elimination.
Log. Meth. Comput. Sci., 8(4):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. Springer, 2012.
doi:10.1007/978-3-642-32347-8_3.


Khalil Ghorbal, Andrew Sogokon, and André Platzer.
Invariance of conjunctions of polynomial equalities for algebraic differential equations.

In Markus Müller-Olm and Helmut Seidl, editors, *SAS*, volume 8723 of *LNCS*, pages 151–167. Springer, 2014.
doi:10.1007/978-3-319-10936-7_10.