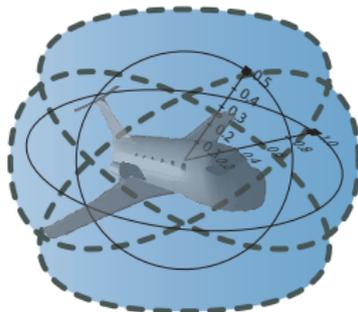# 10: Differential Equations & Differential Invariants
15-424: Foundations of Cyber-Physical Systems

André Platzer

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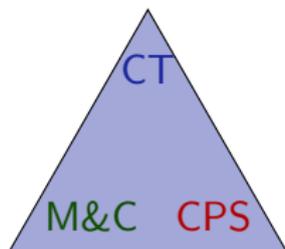Computer Science Department
Carnegie Mellon University, Pittsburgh, PA

Outline

Outline

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

CT

M&C   CPS

understanding continuous dynamics
relate discrete+continuous

semantics of ODEs
operational CPS effects

Differential Facet of Logical Trinity

Axiomatics
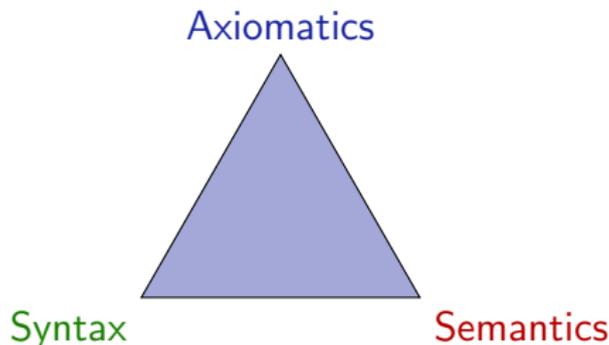
Syntax   Semantics

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

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

$$\llbracket (x' = f(x))^* \rrbracket = \llbracket x' = f(x) \rrbracket$$

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 iteration	effect depends on the past solution
local generator is loop body 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

Loop Invariants Prove Loops

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

Outline

Intuition for Differential Invariants

Differential Invariant

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

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

Intuition for Differential Invariants

Differential Invariant

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

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

Intuition for Differential Invariants

Differential Invariant

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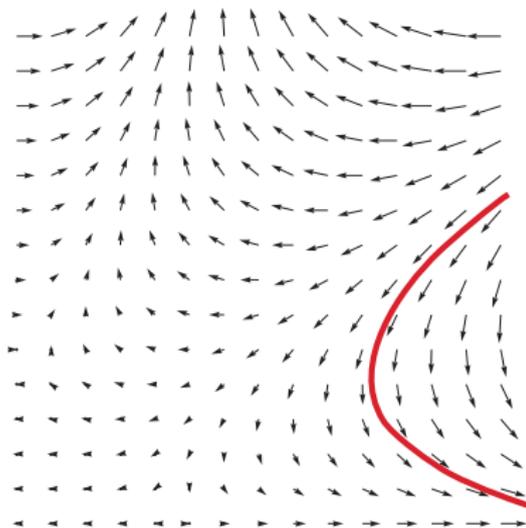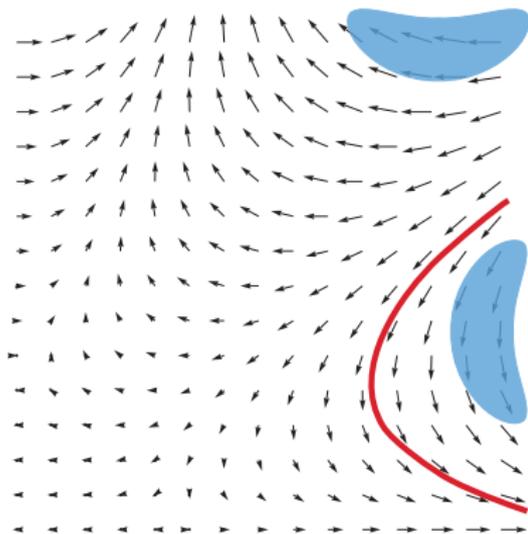

$$[']\ [x' = f(x)]P \leftrightarrow \forall t \geq 0\, [x := y(t)]P \qquad (y' = f(y),\ y(0) = x)$$

Intuition for Differential Invariants

Differential Invariant

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

Want: formula F remains true
in the direction of the dynamics
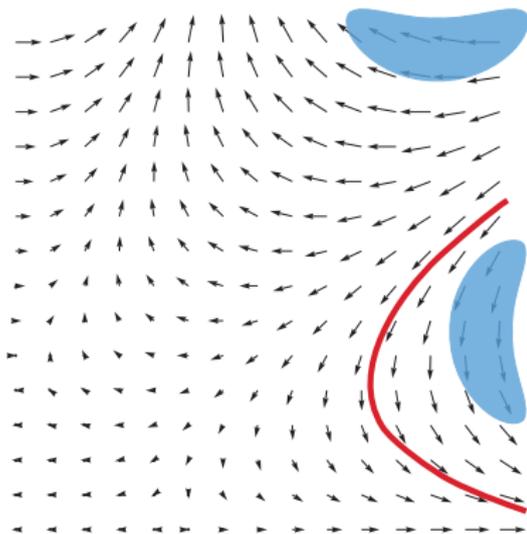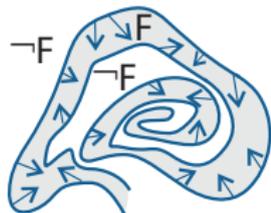
$['] \ [x' = f(x)]P \leftrightarrow \forall t \geq 0 \, [x := y(t)]P \qquad (y' = f(y), \ y(0) = x)$

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

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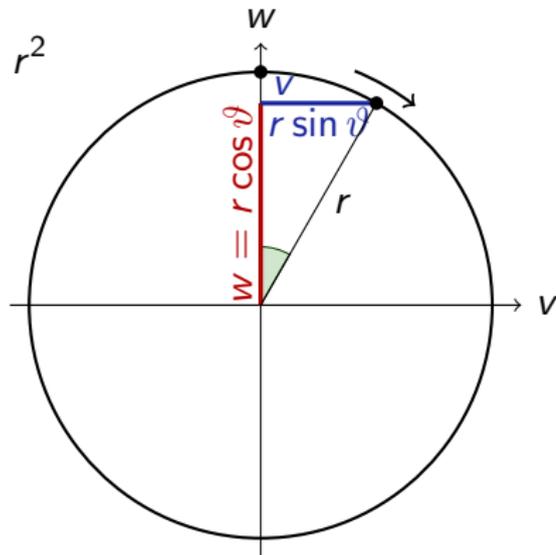
$v^2 + w^2 = r^2 \rightarrow [v' = w, w' = -v] v^2 + w^2 = r^2$

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

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

Derivatives for a Change

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

Derivatives for a Change

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

Derivatives

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

$(e - k)' = (e)' - (k)'$

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

$(e/k)' = ((e)' \cdot k - e \cdot (k)')/k^2$

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

Derivatives for a Change

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

Derivatives

$(e + k)' = (e)' + (k)'$
$(e - k)' = (e)' - (k)'$
$(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$
$(e/k)' = ((e)' \cdot k - e \cdot (k)')/k^2 \quad$ same singularities
$(c())' = 0 \qquad\qquad\qquad$ 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

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

$(e - k)' = (e)' - (k)'$

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

$(e/k)' = ((e)' \cdot k - e \cdot (k)')/k^2$ same singularities

$(c())' = 0$ for constants/numbers $c()$

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

Derivatives for a Change

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

internalize primes into dL syntax

Derivatives

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

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

The Meaning of Primes

The Meaning of Primes

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

The Meaning of Primes

Semantics $\quad \omega[\![(e)']\!] = \dfrac{\mathrm{d}\omega[\![e]\!]}{\mathrm{d}t}$

The Meaning of Primes
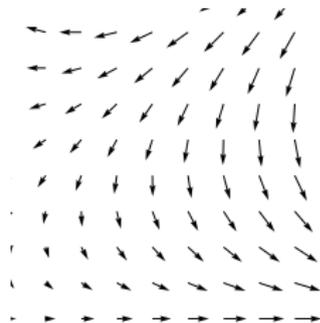
Semantics $\quad \omega[\![(e)']\!] = \dfrac{\mathrm{d}\omega[\![e]\!]}{\mathrm{d}t} \quad$ no!

depends on the differential equation?

The Meaning of Primes
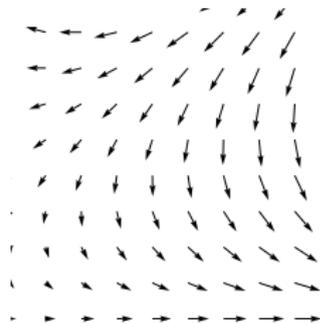
Semantics $\quad \omega[\![(e)']\!] = \dfrac{d\omega[\![e]\!]}{dt} \quad$ no!

depends on the differential equation? Not compositional!
well-defined in isolated state ω at all?

The Meaning of Primes
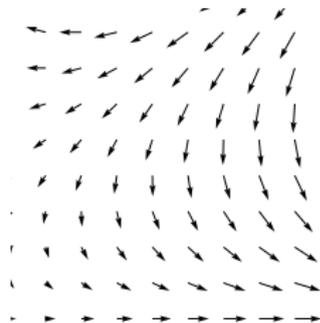
Semantics $\quad \omega[\![(e)']\!] = \dfrac{\mathrm{d}\omega[\![e]\!]}{\mathrm{d}t} \quad$ no!

depends on the differential equation?   Not compositional!
well-defined in isolated state ω at all? No time-derivative without time!

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

depends on the differential equation?   Not compositional!
well-defined in isolated state ω at all?   No time-derivative without time!
meaning is a function of x and x'.

Semantics $\omega[\![(e)']\!] = \sum_x \omega(x') \dfrac{\partial [\![e]\!]}{\partial x}(\omega)$
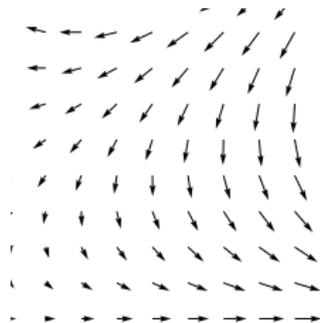
 $\to \mathbb{R}$

depends on the differential equation?   Not compositional!
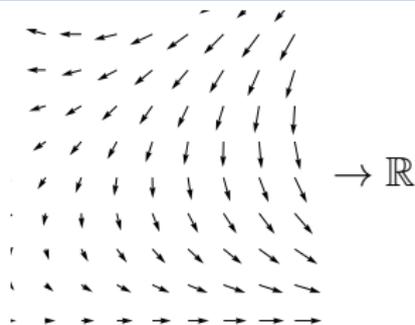well-defined in isolated state ω at all?   No time-derivative without time!
meaning is a function of x and x'.   Differential form!

Differential Dynamic Logic dL: Semantics

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

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

$\text{where } \varphi(z)(x') \stackrel{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)$
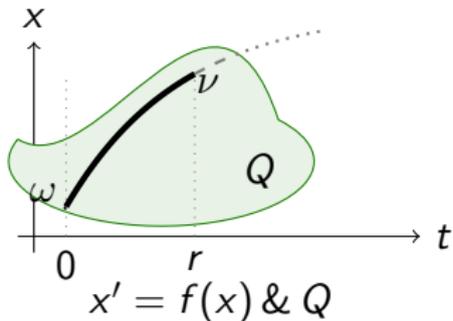
$$x' = f(x) \,\&\, Q$$

Differential Dynamic Logic dL: Semantics

> **Definition (Hybrid program semantics)** $(\llbracket \cdot \rrbracket : \mathrm{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$
>
> $\llbracket x' = f(x) \,\&\, Q \rrbracket = \{(\omega, \nu) : \varphi(z) \models x' = f(x) \wedge Q \text{ for all } 0 \leq z \leq r$
> $\qquad\qquad\qquad$ for a solution $\varphi : [0, r] \to \mathcal{S}$ of any duration $r \in \mathbb{R}$
> $\qquad\qquad\qquad$ with $\varphi(0) = \omega$ and $\varphi(r) = \nu\}$
> $\qquad\qquad\qquad$ where $\varphi(z)(x') \stackrel{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)$

Differential Dynamic Logic dL: Semantics

> **Definition (Hybrid program semantics)** $(\llbracket \cdot \rrbracket : \text{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$
>
> $\llbracket x' = f(x) \, \& \, Q \rrbracket = \{(\omega, \nu) : \varphi(z) \models x' = f(x) \wedge Q \text{ for all } 0 \leq z \leq r$
> $\quad\quad\quad \text{for a solution } \varphi : [0, r] \to \mathcal{S} \text{ of any duration } r \in \mathbb{R}$
> $\quad\quad\quad \text{with } \varphi(0) = \omega \text{ except on } x' \text{ and } \varphi(r) = \nu\}$
> $\quad\quad\quad \text{where } \varphi(z)(x') \stackrel{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)$

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

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 Dynamic Logic dL: Semantics

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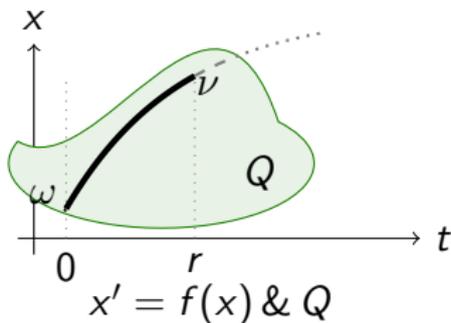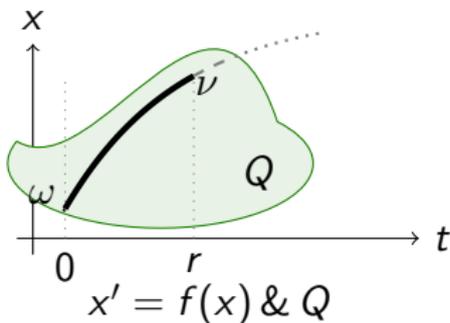$\qquad$ for a solution $\varphi : [0, r] \to \mathcal{S}$ of any duration $r \in \mathbb{R}$
$\qquad$ with $\varphi(0) = \omega$ except on x' and $\varphi(r) = \nu\}$
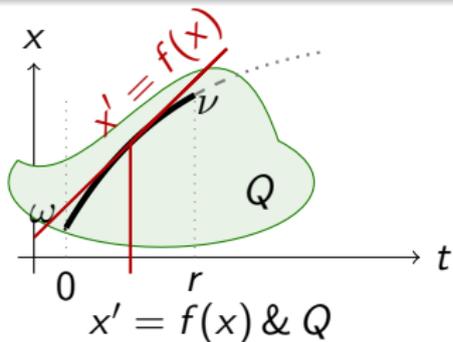$\qquad$ where $\varphi(z)(x') \stackrel{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)$

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

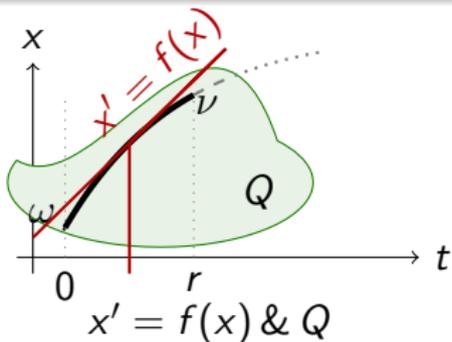Initial value of x' in ω is irrelevant since defined by ODE.
Final value of x' is carried over to the final state ν.

Differential Dynamic Logic dL: Semantics

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 $0 \leq z \leq r$, $FV(e) \subseteq \{x\}$:

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

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

Differential Substitution Lemmas

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

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

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

Lemma (Differential assignment) (Effect on Differentials)

If $\varphi \models x' = f(x) \wedge Q$ 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 $\big([x' = f(x)]e = 0 \leftrightarrow e = 0\big) \leftarrow [x' = f(x)](e)' = 0$

Differential Substitution Lemmas

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

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

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

Lemma (Differential assignment)   (Effect on Differentials)

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

Axiomatics

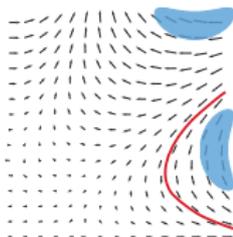DE $[x' = f(x) \& Q]P \leftrightarrow [x' = f(x) \& Q][x' := f(x)]P$

DI $([x' = f(x)]e = 0 \leftrightarrow e = 0) \leftarrow [x' = f(x)](e)' = 0$

rate of change of e along ODE is 0

Differential Invariants for Differential Equations

Differential Invariant

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

Differential Invariants for Differential Equations

Differential Invariant

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

DI $\left([x' = f(x)]e = 0 \leftrightarrow e = 0\right) \leftarrow [x' = f(x)](e)' = 0$

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

Differential Invariants for Differential Equations

Differential Invariant

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

DI $\left([x' = f(x)]e = 0 \leftrightarrow e = 0\right) \leftarrow [x' = f(x)](e)' = 0$

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

Proof (dI is a derived rule).

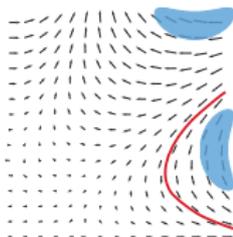$$\text{DI} \; \overline{e = 0 \vdash [x' = f(x)]e = 0}$$

$\square$

Differential Invariants for Differential Equations

Differential Invariant

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

DI $\left([x' = f(x)]e = 0 \leftrightarrow e = 0\right) \leftarrow [x' = f(x)](e)' = 0$

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

Proof (dI is a derived rule).

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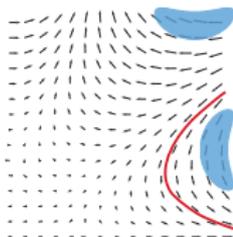
□

Differential Invariants for Differential Equations

Differential Invariant

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

DI $\left([x' = f(x)]e = 0 \leftrightarrow e = 0\right) \leftarrow [x' = f(x)](e)' = 0$

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

Proof (dI is a derived rule).

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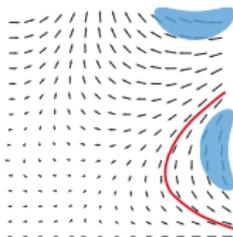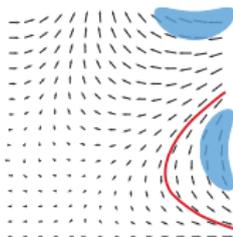
□

Differential Invariants for Differential Equations

Differential Invariant

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

DI $\left([x' = f(x)]e = 0 \leftrightarrow e = 0\right) \leftarrow [x' = f(x)](e)' = 0$

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

Proof (dI is a derived rule).

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

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

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

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

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

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

Guiding Example: Rotational Dynamics

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

$$
\begin{array}{ll}
[':=] & \dfrac{\vdash [v':=w][w':=-v]2vv' + 2ww' - 2rr' = 0}{v^2+w^2-r^2=0 \vdash [v' = w, w' = -v]v^2 + w^2 - r^2 = 0} \\[2em]
\text{dI} & \dfrac{v^2+w^2-r^2=0 \vdash [v' = w, w' = -v]v^2 + w^2 - r^2 = 0}{\vdash v^2+w^2-r^2=0 \rightarrow [v' = w, w' = -v]v^2+w^2-r^2=0} \\
\rightarrow\text{R} &
\end{array}
$$

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

$$
\begin{array}{ll}
\mathbb{R} & \dfrac{}{\vdash 2v(w) + 2w(-v) = 0} \\[1.2em]
[':=] & \dfrac{}{\vdash [v':=w][w':=-v]2vv' + 2ww' - 2rr' = 0} \\[1.2em]
\text{dI} & \dfrac{}{v^2 + w^2 - r^2 = 0 \vdash [v' = w, w' = -v]v^2 + w^2 - r^2 = 0} \\[1.2em]
\rightarrow\text{R} & \dfrac{}{\vdash v^2 + w^2 - r^2 = 0 \rightarrow [v' = w, w' = -v]v^2 + w^2 - r^2 = 0}
\end{array}
$$

Guiding Example: Rotational Dynamics

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

$$
\begin{array}{ll}
\mathbb{R} & \dfrac{*}{\vdash 2v(w) + 2w(-v) = 0} \\[2ex]
{['\!:=]} & \dfrac{}{\vdash [v'\!:=\!w][w'\!:=\!-v]2vv' + 2ww' - 2rr' = 0} \\[2ex]
\text{dI} & \dfrac{}{v^2 + w^2 - r^2 = 0 \vdash [v' = w, w' = -v]v^2 + w^2 - r^2 = 0} \\[2ex]
{\rightarrow}\text{R} & \dfrac{}{\vdash v^2 + w^2 - r^2 = 0 \rightarrow [v' = w, w' = -v]v^2 + w^2 - r^2 = 0}
\end{array}
$$

Guiding Example: Rotational Dynamics

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

$$
\begin{array}{c}
\mathbb{R} \dfrac{\qquad\qquad\qquad *}{\vdash 2v(w) + 2w(-v) = 0} \\[2mm]
['\!:=] \dfrac{}{\vdash [v'\!:=\!w][w'\!:=\!-v]2vv' + 2ww' - 2rr' = 0} \\[2mm]
\text{dI} \dfrac{v^2 + w^2 - r^2 = 0 \vdash [v' = w, w' = -v]v^2 + w^2 - r^2 = 0}{} \\[2mm]
\rightarrow \text{R} \dfrac{}{\vdash v^2 + w^2 - r^2 = 0 \rightarrow [v' = w, w' = -v]v^2 + w^2 - r^2 = 0}
\end{array}
$$

Simple proof without solving ODE

Example Proof: Self-crossing

$$\text{dI} \quad \frac{}{x^2 + x^3 - y^2 - c = 0 \vdash [x' = -2y, y' = -2x - 3x^2]x^2 + x^3 - y^2 - c = 0}$$
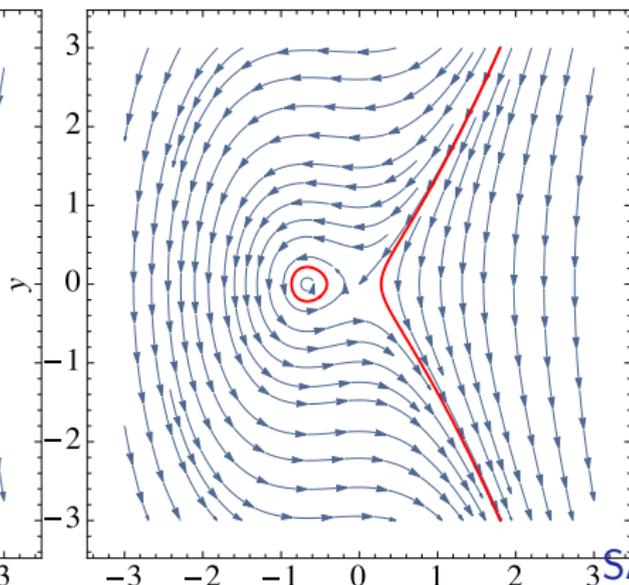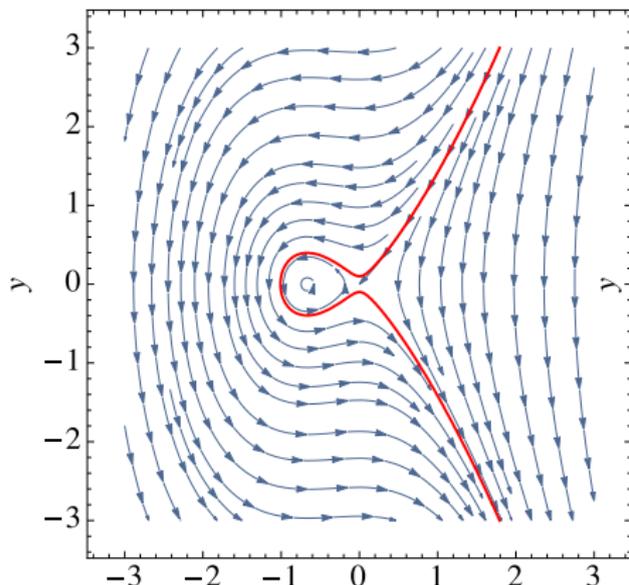
SAS'14

Example Proof: Self-crossing

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

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

SAS'14
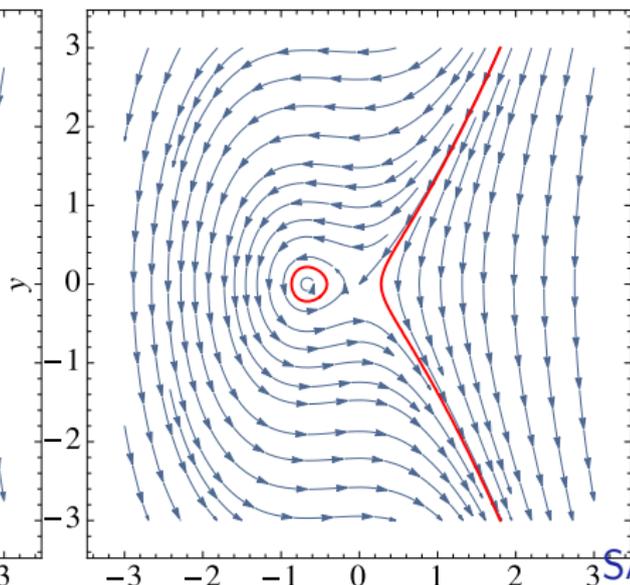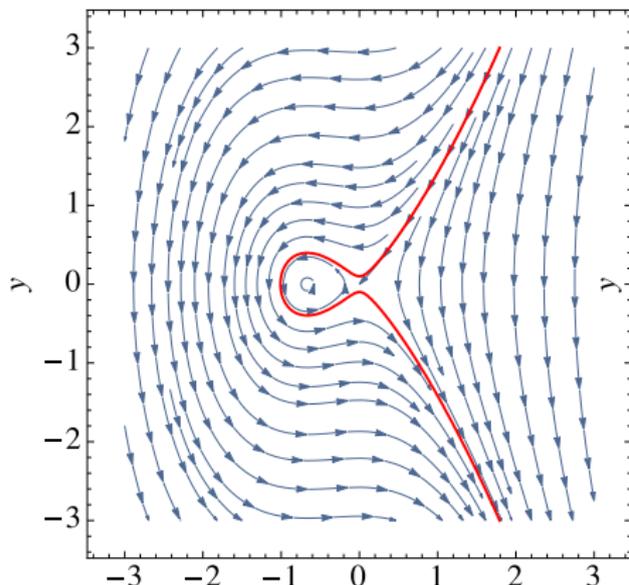
Example Proof: Self-crossing

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

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

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

SAS'14

Example Proof: Self-crossing

$$
\begin{array}{ll}
\mathbb{R} & \dfrac{*}{\vdash 2x(-2y) + 3x^2(-2y) - 2y(-2x - 3x^2) = 0} \\[2ex]
[':=] & \dfrac{}{\vdash [x':=-2y][y':=-2x - 3x^2](2xx'+3x^2x'-2yy') = 0} \\[2ex]
\text{dI} & \dfrac{}{x^2+x^3-y^2-c=0 \vdash [x' = -2y, y' = -2x - 3x^2]x^2+x^3-y^2-c=0}
\end{array}
$$

SAS'14

Example Proof: Self-crossing

$$
\begin{array}{ll}
\mathbb{R} & \dfrac{*}{\vdash 2x(-2y) + 3x^2(-2y) - 2y(-2x - 3x^2) = 0} \\[2ex]
['{:}=] & \dfrac{}{\vdash [x':=-2y][y':=-2x - 3x^2](2xx'+3x^2x'-2yy') = 0} \\[2ex]
\text{dI} & \dfrac{}{x^2+x^3-y^2-c=0 \vdash [x' = -2y, y' = -2x - 3x^2]x^2+x^3-y^2-c=0}
\end{array}
$$

SAS'14
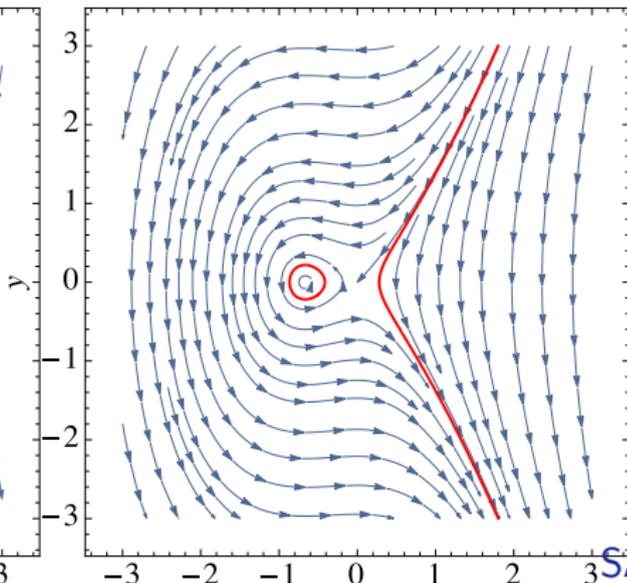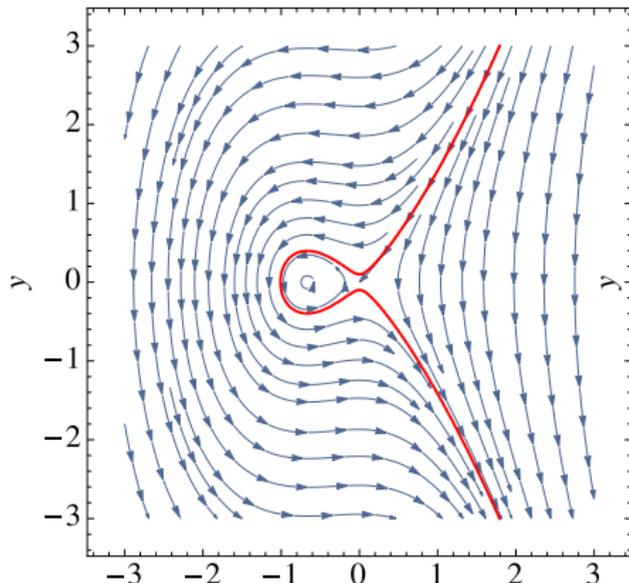
Example Proof: Motzkin

$\dots[x' = 2x^4y+4x^2y^3-6x^2y, y' = -4x^3y^2-2xy^4+6xy^2]x^4y^2+x^2y^4-3x^2y^2=c$
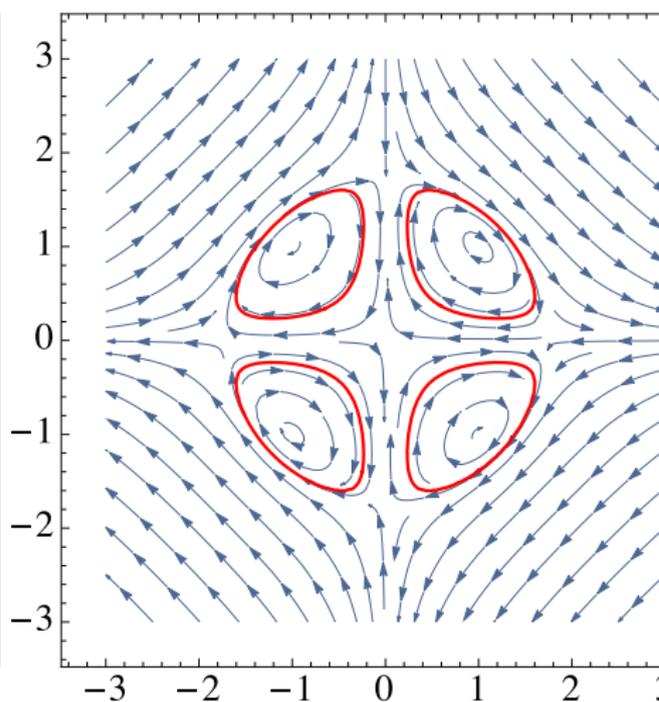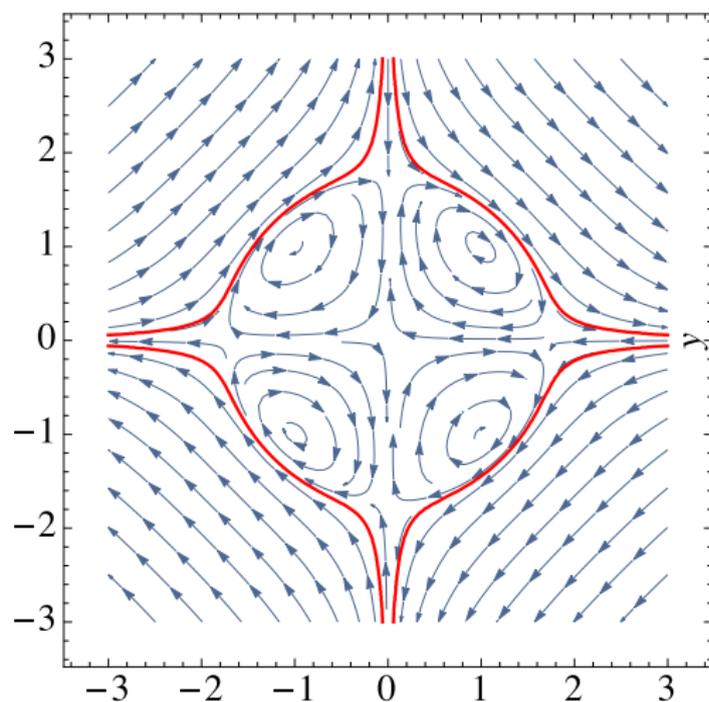
$\rightarrow$R $\dfrac{}{\vdash x^2 + y^2 = 0 \to [x' = 4y^3, y' = -4x^3]\, x^2 + y^2 = 0}$

$$\frac{\text{cut,MR} \ \overline{}}{\quad x^2 + y^2 = 0 \vdash [x' = 4y^3, y' = -4x^3]\, x^2 + y^2 = 0}$$
$$\text{→R} \ \frac{}{\vdash x^2 + y^2 = 0 \rightarrow [x' = 4y^3, y' = -4x^3]\, x^2 + y^2 = 0}$$

$$\dfrac{}{\text{dI} \quad \dfrac{}{x^4 + y^4 = 0 \vdash [x' = 4y^3, y' = -4x^3]\, x^4 + y^4 = 0}}$$

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

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

$$['\!:=] \quad \frac{\vdash [x':=4y^3][y':=-4x^3](4x^3x' + 4y^3y') = 0}{}$$

$$\text{dI} \quad \frac{x^4 + y^4 = 0 \vdash [x' = 4y^3, y' = -4x^3]\, x^4 + y^4 = 0}{}$$

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

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

$$\mathbb{R} \frac{\vdash 4x^3(4y^3) + 4y^3(-4x^3) = 0}{}$$

$$['{:}=] \frac{\vdash [x':=4y^3][y':=-4x^3](4x^3x' + 4y^3y') = 0}{}$$

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

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

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

$$
\begin{array}{ll}
\mathbb{R} & \dfrac{\ast}{\vdash 4x^3({\color{red}4y^3}) + 4y^3({\color{red}-4x^3}) = 0} \\[2ex]
['{:=}] & \dfrac{}{\vdash [x'{:=}{\color{red}4y^3}][y'{:=}{\color{red}-4x^3}](4x^3x' + 4y^3y') = 0} \\[2ex]
\mathrm{dI} & \dfrac{}{x^4 + y^4 = 0 \vdash [x' = 4y^3, y' = -4x^3]\, x^4 + y^4 = 0} \\[2ex]
\mathrm{cut,MR} & \dfrac{}{x^2 + y^2 = 0 \vdash [x' = 4y^3, y' = -4x^3]\, x^2 + y^2 = 0} \\[2ex]
{\rightarrow}\mathrm{R} & \dfrac{}{\vdash x^2 + y^2 = 0 \rightarrow [x' = 4y^3, y' = -4x^3]\, x^2 + y^2 = 0}
\end{array}
$$

$$\frac{\begin{array}{c} * \\ \hline \vdash 4x^3(4y^3) + 4y^3(-4x^3) = 0 \\ \hline \vdash [x':=4y^3][y':=-4x^3](4x^3x' + 4y^3y') = 0 \\ \hline x^4 + y^4 = 0 \vdash [x' = 4y^3, y' = -4x^3]\, x^4 + y^4 = 0 \\ \hline x^2 + y^2 = 0 \vdash [x' = 4y^3, y' = -4x^3]\, x^2 + y^2 = 0 \\ \hline \vdash x^2 + y^2 = 0 \rightarrow [x' = 4y^3, y' = -4x^3]\, x^2 + y^2 = 0 \end{array}}{}$$

with left labels:
$\mathbb{R}$, $[':=]$, dI , cut,MR , $\rightarrow$R

$$
\begin{array}{rl}
\mathbb{R} & \dfrac{*}{\vdash 4x^3(4y^3) + 4y^3(-4x^3) = 0} \\[2ex]
[':=] & \dfrac{}{\vdash [x':=4y^3][y':=-4x^3](4x^3x' + 4y^3y') = 0} \\[2ex]
\text{dI} & \dfrac{}{x^4 + y^4 = 0 \vdash [x' = 4y^3, y' = -4x^3]\, x^4 + y^4 = 0} \\[2ex]
\text{cut,MR} & \dfrac{}{x^2 + y^2 = 0 \vdash [x' = 4y^3, y' = -4x^3]\, x^2 + y^2 = 0} \\[2ex]
\rightarrow\text{R} & \dfrac{}{\vdash x^2 + y^2 = 0 \rightarrow [x' = 4y^3, y' = -4x^3]\, x^2 + y^2 = 0}
\end{array}
$$

Theorem (Sophus Lie)

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

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

$$
\begin{array}{ll}
\mathbb{R} & \dfrac{*}{\vdash 4x^3(4y^3) + 4y^3(-4x^3) = 0} \\[2ex]
[':=] & \dfrac{}{\vdash [x':=4y^3][y':=-4x^3](4x^3x' + 4y^3y') = 0} \\[2ex]
\text{dI} & \dfrac{}{x^4 + y^4 = 0 \vdash [x' = 4y^3, y' = -4x^3]\, x^4 + y^4 = 0} \\[2ex]
\text{cut,MR} & \dfrac{}{x^2 + y^2 = 0 \vdash [x' = 4y^3, y' = -4x^3]\, x^2 + y^2 = 0} \\[2ex]
\rightarrow\text{R} & \dfrac{}{\vdash x^2 + y^2 = 0 \rightarrow [x' = 4y^3, y' = -4x^3]\, x^2 + y^2 = 0}
\end{array}
$$

Theorem (Sophus Lie)

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

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

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 $0 \le z \le r$, $FV(e) \subseteq \{x\}$:

Syntactic $'$

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

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 $\varphi \models x' = f(x) \land Q$ for duration $r > 0$, then for all $0 \leq z \leq r$, $FV(e) \subseteq \{x\}$:

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

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

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

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

Soundness Proof

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

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

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

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

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

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

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

Soundness Proof

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

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

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

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

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

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

$[\![x' = f(x) \,\&\, Q]\!] = \{(\varphi(0), \varphi(r)) : \varphi(z) \models x' = f(x) \land Q \text{ for all } 0 \leq z \leq r$

$\text{for a } \varphi : [0, r] \to \mathcal{S} \text{ where } \varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)\}$

Soundness Proof

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

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

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

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

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

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

$[\![x' = f(x) \& Q]\!] = \{(\varphi(0), \varphi(r)) : \varphi(z) \models x' = f(x) \land Q$ for all $0 \leq z \leq r$
for a $\varphi : [0, r] \to \mathcal{S}$ 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 $0 \le z \le r$, $FV(e) \subseteq \{x\}$:

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

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

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

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

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

Soundness Proof

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

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

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

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

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

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

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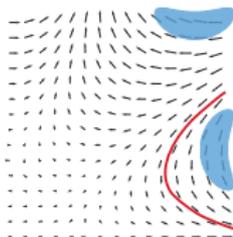
Outline

Differential Invariants for Differential Equations

Differential Invariant

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

DI $\left([x' = f(x)]e = 0 \leftrightarrow e = 0\right) \leftarrow [x' = f(x)](e)' = 0$

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

Differential Substitution Lemmas

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

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

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

Lemma (Differential assignment)   (Effect on Differentials)

If $\varphi \models x' = f(x) \wedge Q$ 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 15-424/624/824, Carnegie Mellon University, 2017.
URL: http://lfcps.org/course/fcps17.html.

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

J. Autom. Reas., 2016.
doi:10.1007/s10817-016-9385-1.

📄 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.