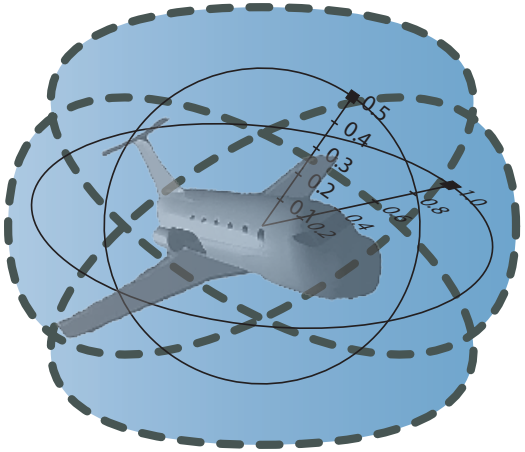
11: Differential Equations & Proofs

15-424: Foundations of Cyber-Physical Systems

André Platzer

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



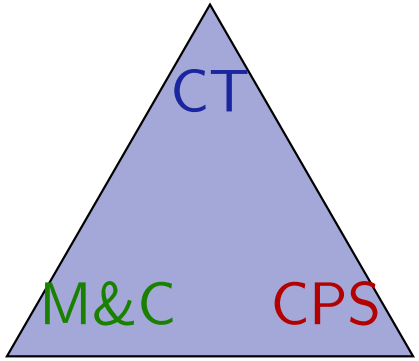
Outline

Outline

Learning Objectives

Differential Equations & Proofs

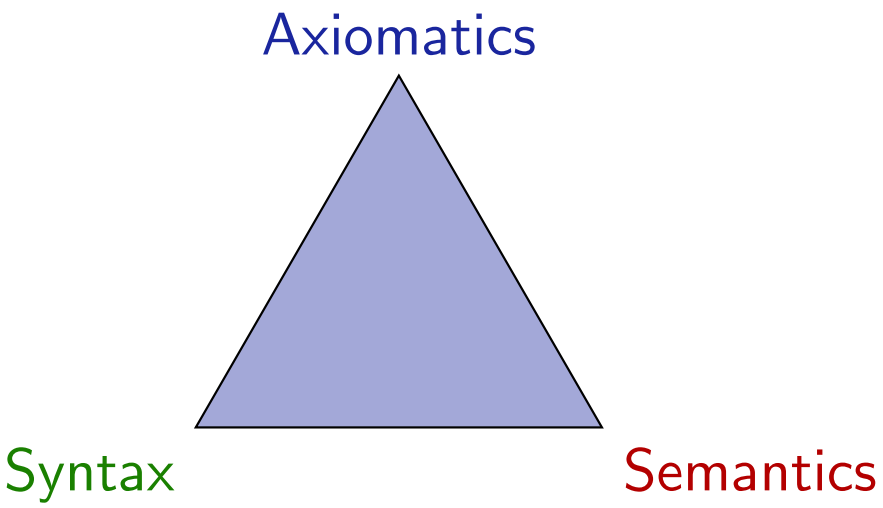
discrete vs. continuous analogy
rigorous reasoning about ODEs
beyond differential invariant terms
differential invariant formulas
cut principles for differential equations
axiomatization of ODEs
differential facet of logical trinity



understanding continuous dynamics
relate discrete+continuous
design-by-invariant

operational CPS effects
state changes along ODE

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

Differentials

Syntax

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

Semantics

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

Axioms

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

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

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

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

ODE

$$[\![x' = f(x) \,\&\, Q]\!] = \{(\varphi(0), \varphi(r)) : \varphi \models x' = f(x) \wedge Q \text{ for some } \varphi : [0, r] \to \mathcal{S}, \text{ some } r \in \mathbb{R}\}$$

$$\varphi(\zeta)(x') = \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(\zeta)$$

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* $0 \leq z \leq r$*:*

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

Lemma (Differential assignment) (Effect on Differentials)

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

Lemma (Derivations) (Equations of Differentials)

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

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

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

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

Differential Substitution Lemmas $\rightsquigarrow$ Proofs

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

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

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

Lemma (Differential assignment) (Effect on Differentials)

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

Lemma (Derivations) (Equations of Differentials)

$+'$	$(e + k)' = (e)' + (k)'$
$\cdot'$	$(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$
c'	$(c())' = 0$
x'	$(x)' = x'$

Soundness: Proof of Derivations Lemma

Lemma (Derivations) (Equations of Differentials)

$+'$	$(e+k)' = (e)' + (k)'$
$\cdot'$	$(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$
c'	$(c())' = 0$
x'	$(x)' = x'$

Soundness: Proof of Derivations Lemma

Lemma (Derivations) (Equations of Differentials)

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

Proof.

$[\![(e+k)']\!]\omega =$

$\square$

Soundness: Proof of Derivations Lemma

Lemma (Derivations) (Equations of Differentials)

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

Proof.

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

□

Soundness: Proof of Derivations Lemma

Lemma (Derivations) (Equations of Differentials)

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

Proof.

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

□

Soundness: Proof of Derivations Lemma

Lemma (Derivations) (Equations of Differentials)

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

Proof.

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

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

□

Soundness: Proof of Derivations Lemma

Lemma (Derivations) (Equations of Differentials)

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

Proof.

$$\begin{aligned}
[\![(e+k)']\!]\omega &= \sum_x \omega(x')\frac{\partial[\![e+k]\!]}{\partial x}(\omega) = \sum_x \omega(x')\frac{\partial([\![e]\!]+[\![k]\!])}{\partial x}(\omega) \\
&= \sum_x \omega(x')\Big(\frac{\partial[\![e]\!]}{\partial x}(\omega) + \frac{\partial[\![k]\!]}{\partial x}(\omega)\Big) \\
&= \sum_x \omega(x')\frac{\partial[\![e]\!]}{\partial x}(\omega) + \sum_x \omega(x')\frac{\partial[\![k]\!]}{\partial x}(\omega)
\end{aligned}$$

□

Soundness: Proof of Derivations Lemma

Lemma (Derivations) (Equations of Differentials)

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

Proof.

$$
\begin{aligned}
[\![(e+k)']\!]\omega &= \sum_x \omega(x')\frac{\partial[\![e+k]\!]}{\partial x}(\omega) = \sum_x \omega(x')\frac{\partial([\![e]\!]+[\![k]\!])}{\partial x}(\omega) \\
&= \sum_x \omega(x')\Big(\frac{\partial[\![e]\!]}{\partial x}(\omega) + \frac{\partial[\![k]\!]}{\partial x}(\omega)\Big) \\
&= \sum_x \omega(x')\frac{\partial[\![e]\!]}{\partial x}(\omega) + \sum_x \omega(x')\frac{\partial[\![k]\!]}{\partial x}(\omega) \\
&= [\![(e)']\!]\omega + [\![(k)']\!]\omega
\end{aligned}
$$

□

Soundness: Proof of Derivations Lemma

Lemma (Derivations) (Equations of Differentials)

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

Proof.

$$
\begin{aligned}
[\![(e+k)']\!]\omega &= \sum_x \omega(x')\frac{\partial[\![e+k]\!]}{\partial x}(\omega) = \sum_x \omega(x')\frac{\partial([\![e]\!]+[\![k]\!])}{\partial x}(\omega) \\
&= \sum_x \omega(x')\Big(\frac{\partial[\![e]\!]}{\partial x}(\omega) + \frac{\partial[\![k]\!]}{\partial x}(\omega)\Big) \\
&= \sum_x \omega(x')\frac{\partial[\![e]\!]}{\partial x}(\omega) + \sum_x \omega(x')\frac{\partial[\![k]\!]}{\partial x}(\omega) \\
&= [\![(e)']\!]\omega + [\![(k)']\!]\omega = [\![(e)' + (k)']\!]\omega
\end{aligned}
$$

□

Soundness: Proof of Derivations Lemma

Lemma (Derivations) (Equations of Differentials)

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

Proof.

$$
\begin{aligned}
[\![(e+k)']\!]\omega &= \sum_x \omega(x')\frac{\partial[\![e+k]\!]}{\partial x}(\omega) = \sum_x \omega(x')\frac{\partial([\![e]\!]+[\![k]\!])}{\partial x}(\omega) \\
&= \sum_x \omega(x')\Big(\frac{\partial[\![e]\!]}{\partial x}(\omega) + \frac{\partial[\![k]\!]}{\partial x}(\omega)\Big) \\
&= \sum_x \omega(x')\frac{\partial[\![e]\!]}{\partial x}(\omega) + \sum_x \omega(x')\frac{\partial[\![k]\!]}{\partial x}(\omega) \\
&= [\![(e)']\!]\omega + [\![(k)']\!]\omega = [\![(e)' + (k)']\!]\omega
\end{aligned}
$$

□

Differential Substitution Lemmas $\rightsquigarrow$ Proofs

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

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

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

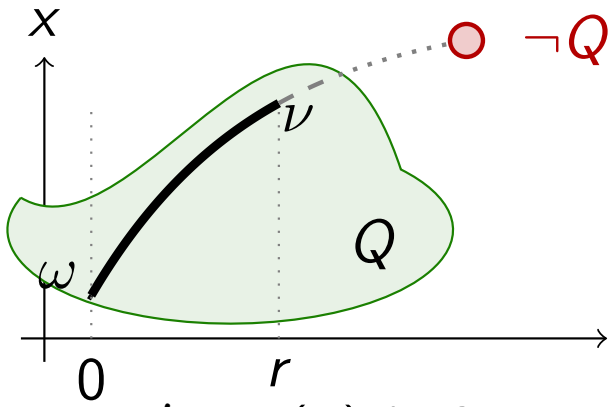
Lemma (Differential assignment) (Effect on Differentials)

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

Lemma (Derivations) (Equations of Differentials)

$+'$	$(e + k)' = (e)' + (k)'$
$\cdot'$	$(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$
c'	$(c())' = 0$
x'	$(x)' = x'$

Differential Weakening



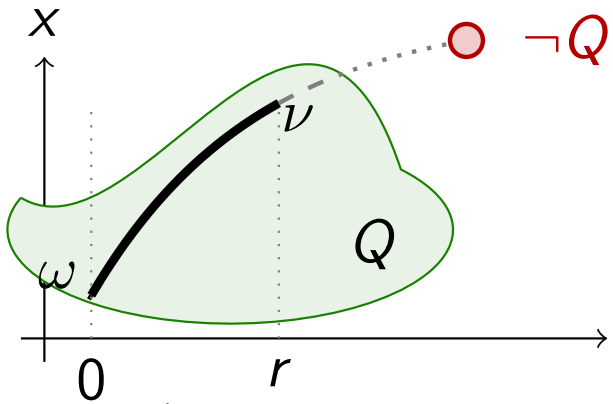
$x' = f(x) \,\&\, Q$

ODE

$$[\![x' = f(x) \,\&\, Q]\!] = \{(\varphi(0), \varphi(r)) : \varphi \models x' = f(x) \wedge Q \text{ for some } \varphi : [0, r] \to \mathcal{S}, \text{ some } r \in \mathbb{R}\}$$

$$\varphi(\zeta)(x') = \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(\zeta)$$

Differential Weakening



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

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

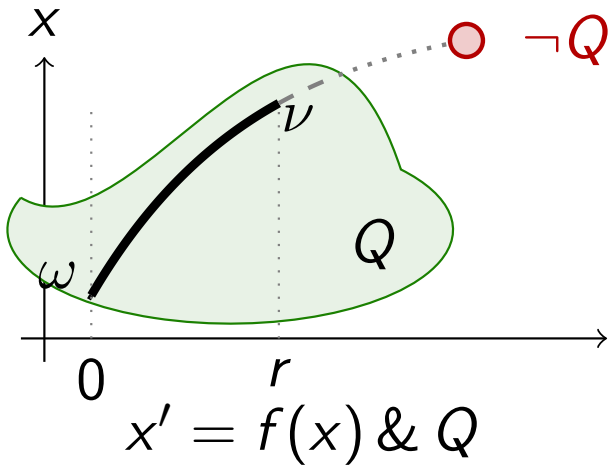
ODE

$$[\![x' = f(x) \,\&\, Q]\!] = \{(\varphi(0), \varphi(r)) : \varphi \models x' = f(x) \wedge Q \text{ for some } \varphi : [0, r] \to \mathcal{S}, \text{ some } r \in \mathbb{R}\}$$

$$\varphi(\zeta)(x') = \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(\zeta)$$

Differential equations cannot leave their domains.

Differential Weakening



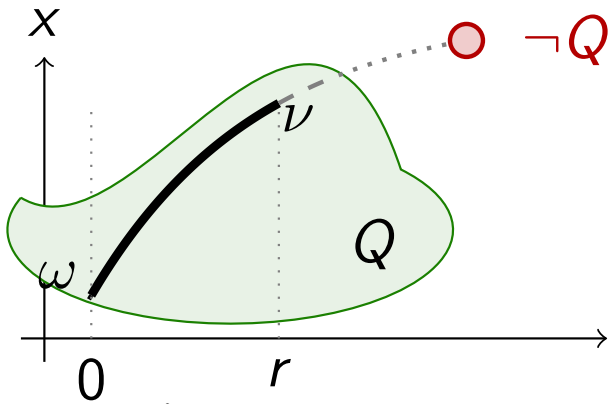
DW $[x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x) \,\&\, Q](Q \rightarrow P)$

Example (Bouncing ball)

$$\text{DW}\,\frac{}{\vdash [x' = v, v' = -g \,\&\, x \geq 0]0 \leq x}$$

No need to solve any ODEs to prove that bouncing ball is above ground.

Differential Weakening



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

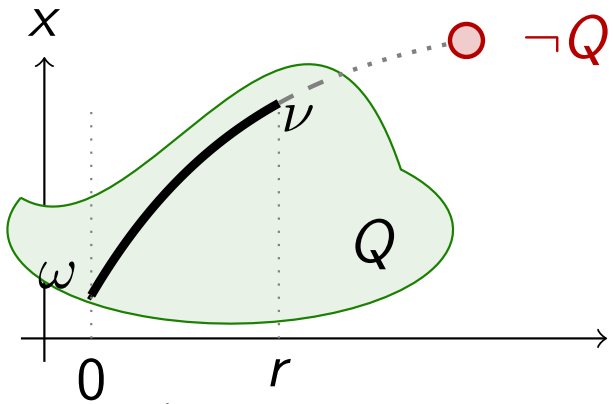
$x' = f(x) \,\&\, Q$

Example (Bouncing ball)

$$\text{DW}\ \dfrac{\text{G}\ \dfrac{}{\vdash [x' = v, v' = -g \,\&\, x \geq 0](x \geq 0 \to 0 \leq x)}}{\vdash [x' = v, v' = -g \,\&\, x \geq 0]0 \leq x}$$

No need to solve any ODEs to prove that bouncing ball is above ground.

Differential Weakening



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

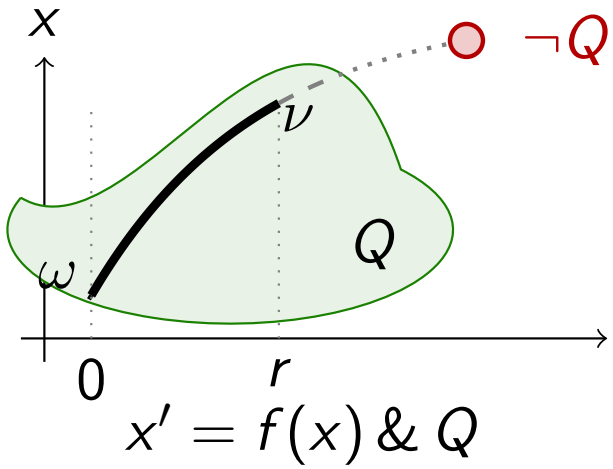
DW $[x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x) \,\&\, Q](Q \to P)$

Example (Bouncing ball)

$$\mathrm{DW}\,\dfrac{\mathrm{G}\,\dfrac{\mathbb{R}\,\dfrac{}{\vdash x \geq 0 \to 0 \leq x}}{\vdash [x' = v, v' = -g \,\&\, x \geq 0](x \geq 0 \to 0 \leq x)}}{\vdash [x' = v, v' = -g \,\&\, x \geq 0]0 \leq x}$$

No need to solve any ODEs to prove that bouncing ball is above ground.

Differential Weakening



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

Example (Bouncing ball)

$$\mathrm{DW}\,\dfrac{\mathrm{G}\,\dfrac{\mathbb{R}\,\dfrac{*}{\vdash x \geq 0 \to 0 \leq x}}{\vdash [x' = v, v' = -g \,\&\, x \geq 0](x \geq 0 \to 0 \leq x)}}{\vdash [x' = v, v' = -g \,\&\, x \geq 0]0 \leq x}$$

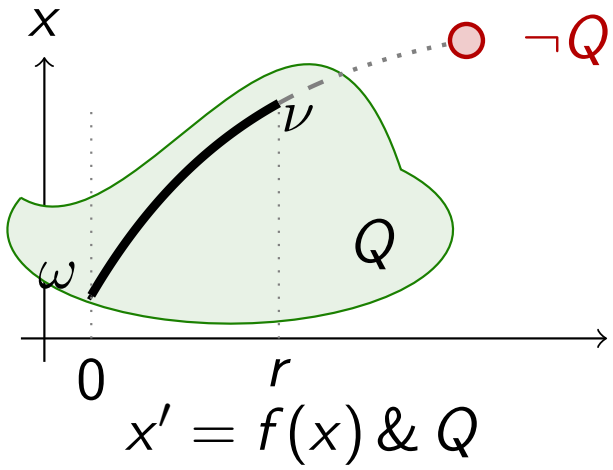
No need to solve any ODEs to prove that bouncing ball is above ground.

Differential Weakening

Differential Weakening

$$\text{DW}\ \frac{}{\Gamma \vdash [x' = f(x) \,\&\, q(x)]p(x), \Delta}$$

$$\text{DW}\ \ [x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x) \,\&\, Q](Q \rightarrow P)$$



Example (Bouncing ball)

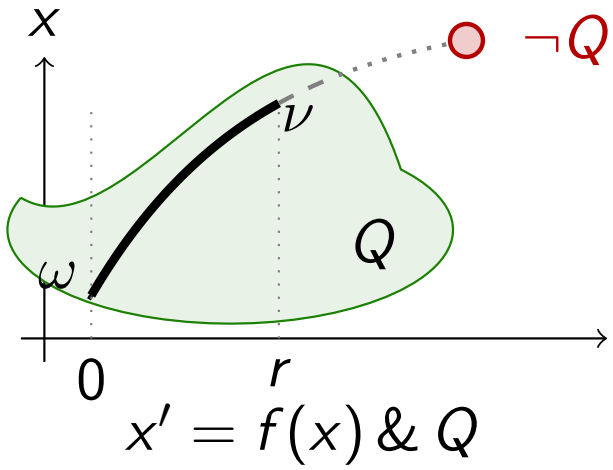
$$\text{DW}\ \frac{\text{G}\ \dfrac{\mathbb{R}\ \dfrac{*}{\vdash x \geq 0 \rightarrow 0 \leq x}}{\vdash [x' = v, v' = -g \,\&\, x \geq 0](x \geq 0 \rightarrow 0 \leq x)}}{\vdash [x' = v, v' = -g \,\&\, x \geq 0]0 \leq x}$$

No need to solve any ODEs to prove that bouncing ball is above ground.

Differential Weakening

Differential Weakening

$$\text{DW}\quad \frac{\Gamma \vdash \forall x\,(q(x) \to p(x)), \Delta}{\Gamma \vdash [x' = f(x)\,\&\,q(x)]p(x), \Delta}$$



DW $\quad [x' = f(x)\,\&\,Q]P \leftrightarrow [x' = f(x)\,\&\,Q](Q \to P)$

Example (Bouncing ball)

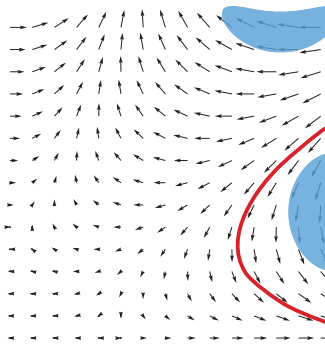
$$\text{DW}\;\dfrac{\text{G}\;\dfrac{\mathbb{R}\;\dfrac{*}{\vdash x \geq 0 \to 0 \leq x}}{\vdash [x' = v, v' = -g\,\&\,x \geq 0](x \geq 0 \to 0 \leq x)}}{\vdash [x' = v, v' = -g\,\&\,x \geq 0]0 \leq x}$$

No need to solve any ODEs to prove that bouncing ball is above ground.

Differential Invariant Terms for Differential Equations

Differential Invariant

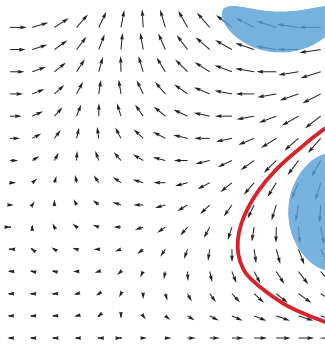
$$\text{dI}\quad \frac{Q \vdash [x' := f(x)](e)' = 0}{e = 0 \vdash [x' = f(x) \,\&\, Q]e = 0}$$



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

$$\text{DW}\quad [x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x) \,\&\, Q](Q \rightarrow P)$$

Differential Invariant Terms for Differential Equations



Differential Invariant

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

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

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

$$\text{DW}\quad [x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x) \,\&\, Q](Q \rightarrow P)$$

dI is a derived rule:

$$\text{DI}\;\dfrac{\text{DE}\;\dfrac{\text{DW}\;\dfrac{\text{G},\rightarrow\text{R}\;\dfrac{Q \vdash [x' := f(x)](e)' = 0}{\vdash [x' = f(x) \,\&\, Q](Q \rightarrow [x' := f(x)](e)' = 0)}}{\vdash [x' = f(x) \,\&\, Q][x' := f(x)](e)' = 0}}{\vdash [x' = f(x) \,\&\, Q](e)' = 0}}{e = 0 \vdash [x' = f(x) \,\&\, Q]e = 0}$$

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

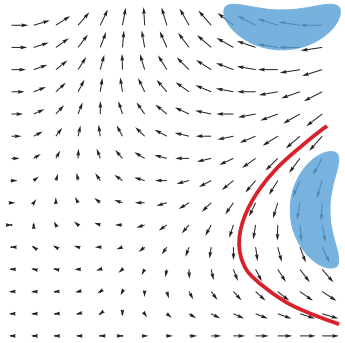
Differential Invariant Equations

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

$$\varphi \models x' = f(x) \wedge Q \ \textit{for}\ r > 0 \ \Rightarrow\ \forall 0 \leq z \leq r \ \ [\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

Differential Invariant

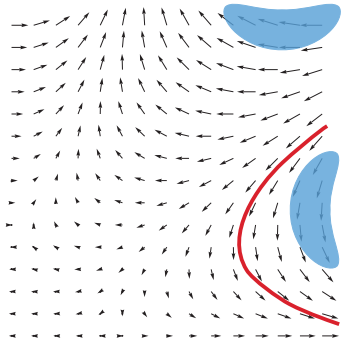
$$\text{dI}\ \frac{}{e = k \vdash [x' = f(x)]e = k}$$



Differential Invariant Equations

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

$$\varphi \models x' = f(x) \wedge Q \text{ for } r > 0 \;\Rightarrow\; \forall 0 \leq z \leq r \;\; [\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$



Differential Invariant

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

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

Differential Invariant Equations

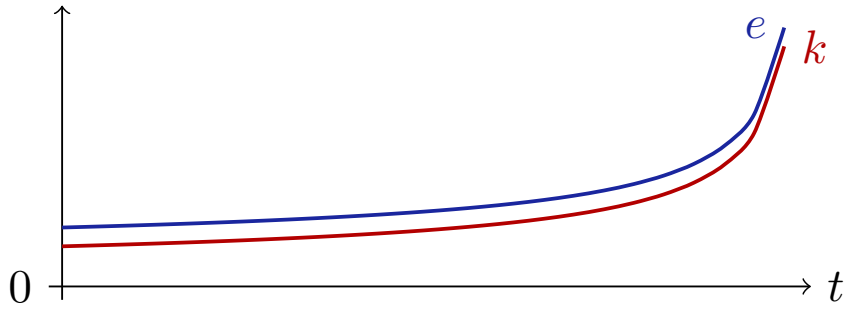
Lemma (Differential lemma) (Differential value vs. Time-derivative)

$$\varphi \models x' = f(x) \wedge Q \text{ for } r > 0 \;\Rightarrow\; \forall 0 \leq z \leq r \;\; [\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

Differential Invariant

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

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



Proof (= rate of change from = initial value. Mean-value theorem).

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

Differential Invariant Inequalities

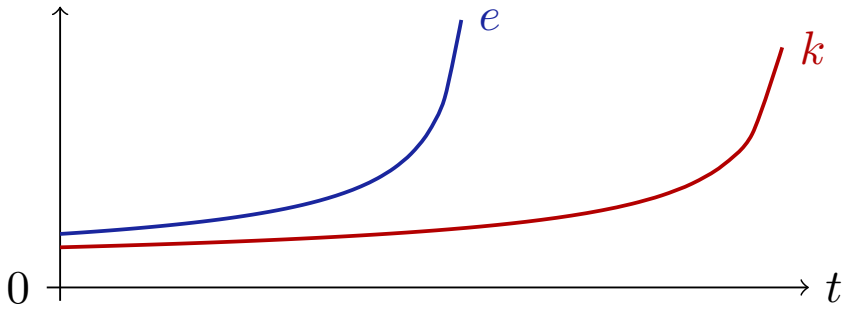
Lemma (Differential lemma) (Differential value vs. Time-derivative)

$$\varphi \models x' = f(x) \wedge Q \text{ for } r > 0 \;\Rightarrow\; \forall 0 \leq z \leq r \;\; [\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

Differential Invariant

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

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



Proof ($\geq$ rate of change from $\geq$ initial value. Mean-value theorem).

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

Differential Invariant Inequalities

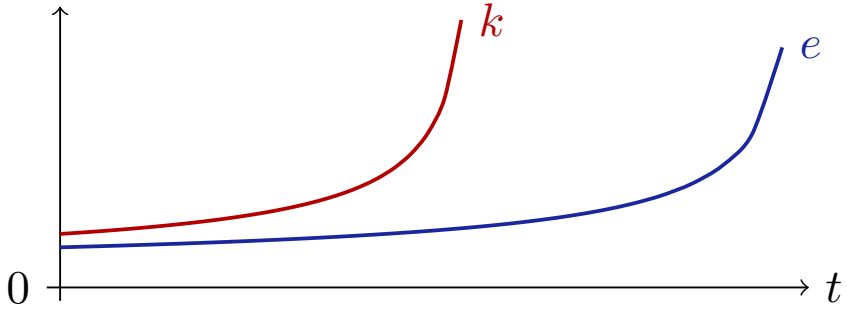
Lemma (Differential lemma) (Differential value vs. Time-derivative)

$$\varphi \models x' = f(x) \wedge Q \text{ for } r > 0 \;\Rightarrow\; \forall 0 \leq z \leq r \;\; [\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

Differential Invariant

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

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



Proof ($\leq$ rate of change from $\leq$ initial value. Mean-value theorem).

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

Differential Invariant Inequalities

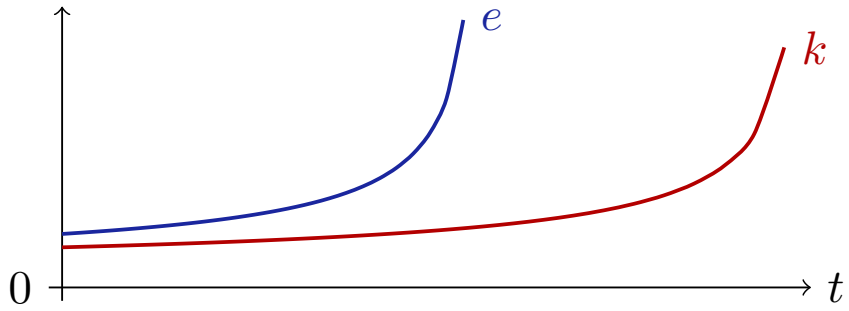
Lemma (Differential lemma) (Differential value vs. Time-derivative)

$$\varphi \models x' = f(x) \wedge Q \text{ for } r > 0 \;\Rightarrow\; \forall 0 \leq z \leq r \;\; [\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

Differential Invariant

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

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



Proof (> rate of change from > initial value. Mean-value theorem).

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

Differential Invariant Inequalities

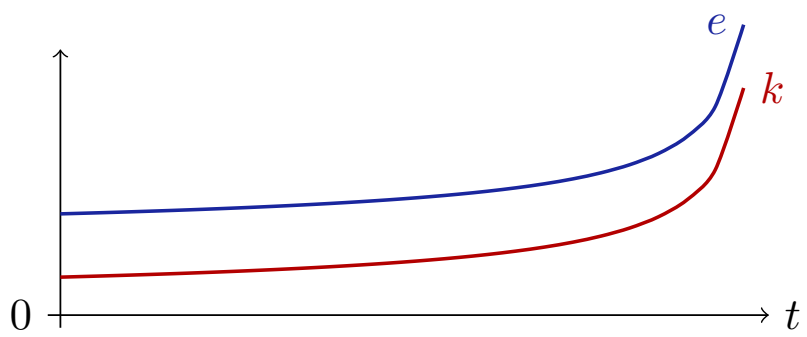
Lemma (Differential lemma) (Differential value vs. Time-derivative)

$$\varphi \models x' = f(x) \wedge Q \text{ for } r > 0 \;\Rightarrow\; \forall 0 \leq z \leq r \;\; [\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

Differential Invariant

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

$$\text{DI} \quad \frac{\vdash [x' = f(x)](e)' \geq (k)'}{e > k \vdash [x' = f(x)]e > k}$$



Proof ($\geq$ rate of change from $>$ initial value. Mean-value theorem).

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

Differential Invariant Inequalities

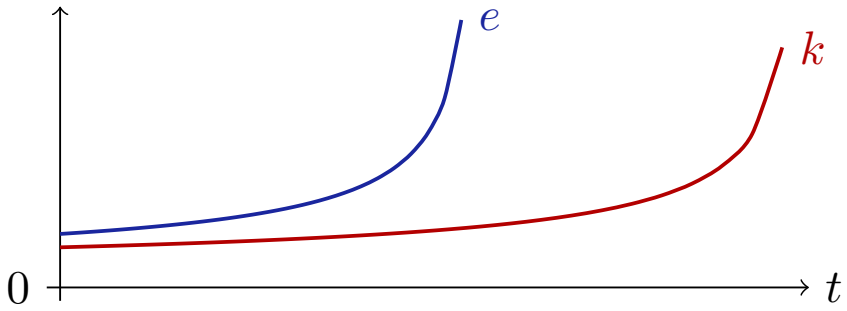
Lemma (Differential lemma) (Differential value vs. Time-derivative)

$$\varphi \models x' = f(x) \wedge Q \text{ for } r > 0 \;\Rightarrow\; \forall 0 \leq z \leq r \;\; [\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

Differential Invariant

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

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



Proof ($\neq$ rate of change from $\neq$ initial value. Mean-value theorem).

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

Differential Invariant Inequalities

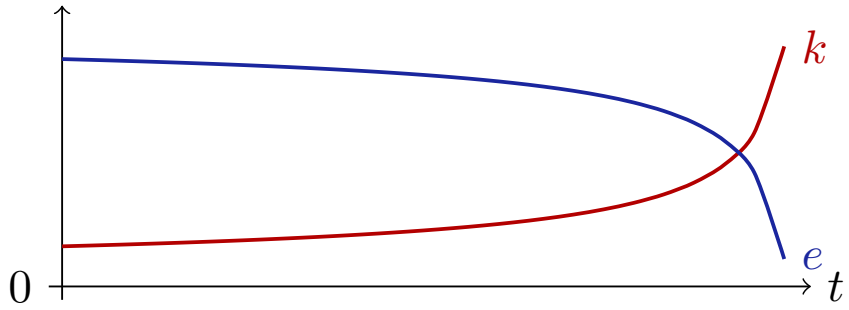
Lemma (Differential lemma) (Differential value vs. Time-derivative)

$$\varphi \models x' = f(x) \wedge Q \text{ for } r > 0 \;\Rightarrow\; \forall 0 \leq z \leq r \;\; [\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

Differential Invariant

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

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



Proof ($\neq$ rate of change from $\neq$ initial value. Mean-value theorem).

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

Differential Invariant Inequalities

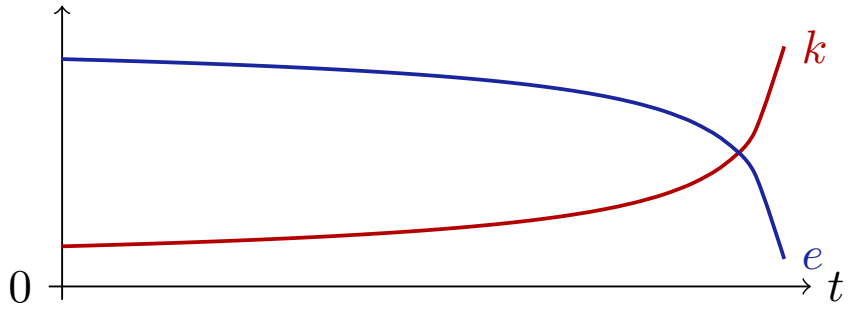
Lemma (Differential lemma) (Differential value vs. Time-derivative)

$$\varphi \models x' = f(x) \wedge Q \text{ for } r > 0 \;\Rightarrow\; \forall 0 \leq z \leq r \;\; [\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

Differential Invariant

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

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



Proof ($\neq$ rate of change from $\neq$ initial value. Mean-value theorem).

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

Differential Invariant Inequalities

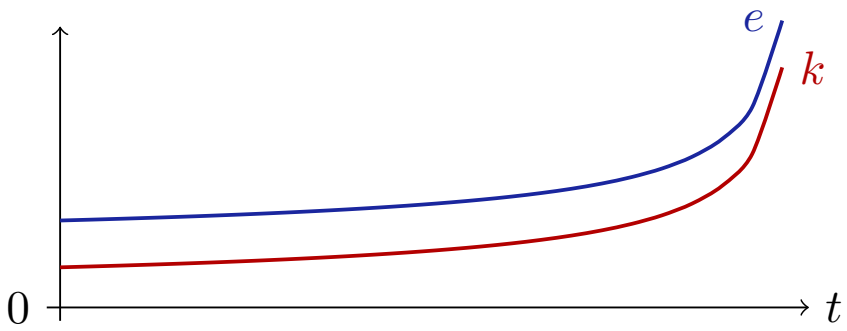
Lemma (Differential lemma) (Differential value vs. Time-derivative)

$$\varphi \models x' = f(x) \wedge Q \text{ for } r > 0 \;\Rightarrow\; \forall 0 \leq z \leq r \;\; [\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

Differential Invariant

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

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

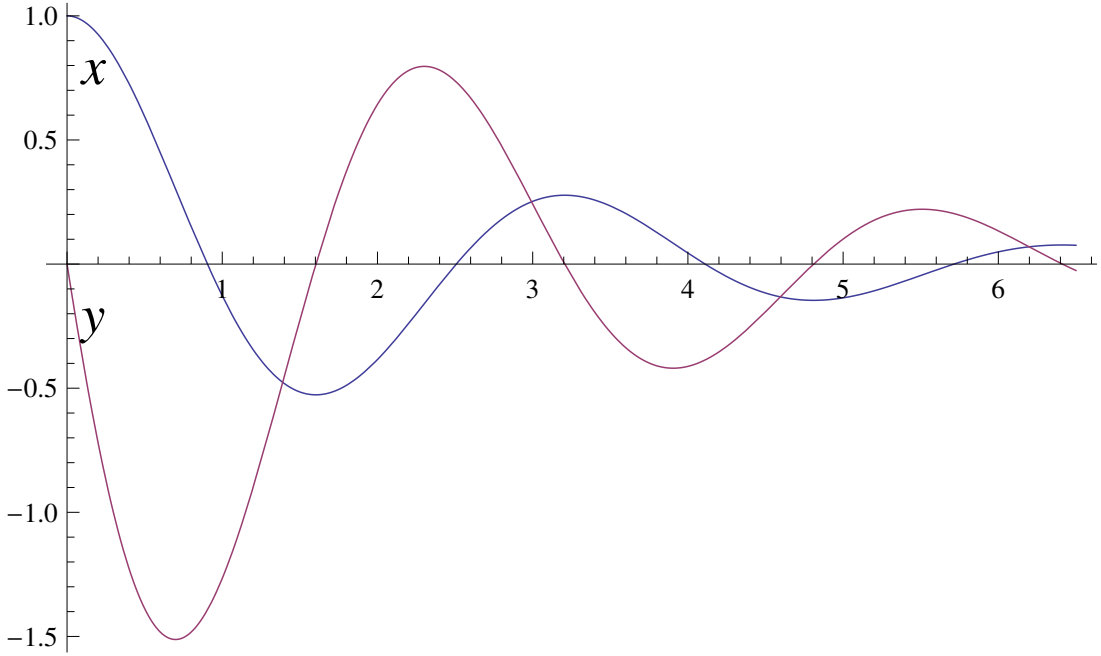


Proof (= rate of change from ≠ initial value. Mean-value theorem).

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

Example: Differential Invariant Inequalities

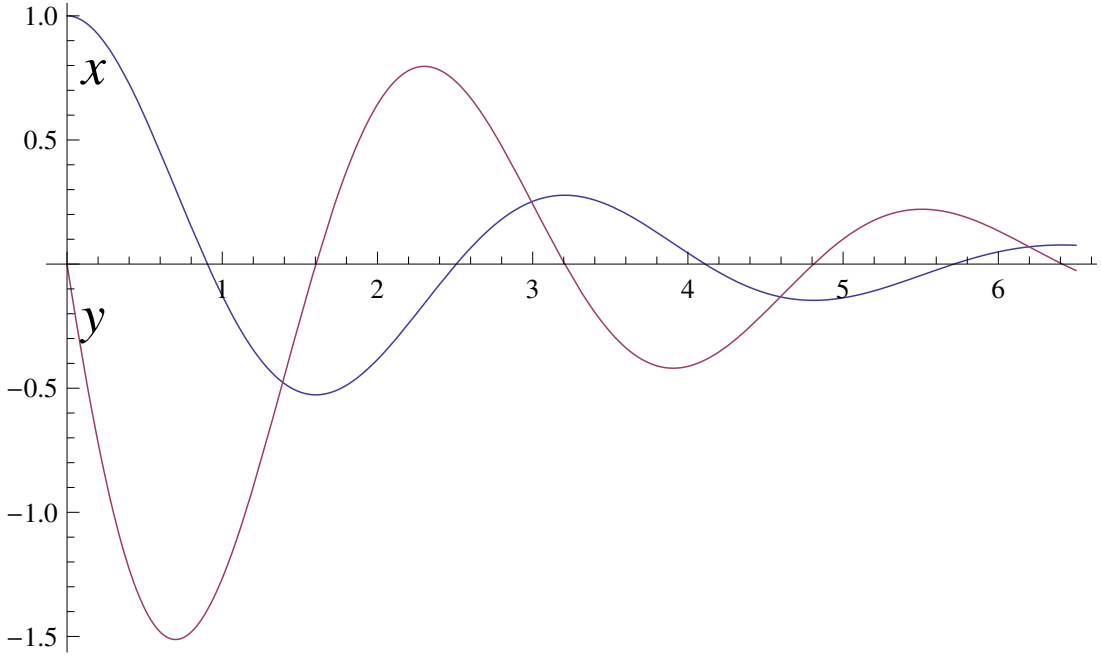
$$\omega^2x^2+y^2\leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, (\omega\geq 0 \wedge d\geq 0)]\, \omega^2x^2+y^2\leq c^2$$



Example: Differential Invariant Inequalities

$$\omega \geq 0 \wedge d \geq 0 \vdash [x' := y][y' := -\omega^2 x - 2d\omega y] 2\omega^2 x x' + 2y y' \leq 0$$

$$\omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, (\omega \geq 0 \wedge d \geq 0)]\, \omega^2 x^2 + y^2 \leq c^2$$

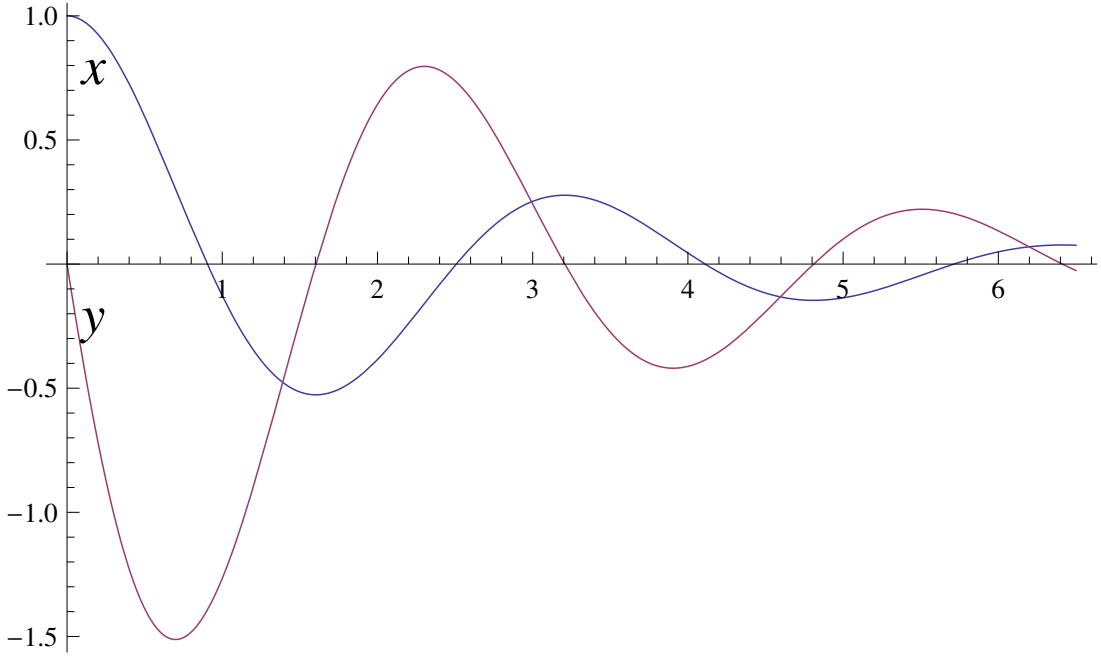


Example: Differential Invariant Inequalities

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

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

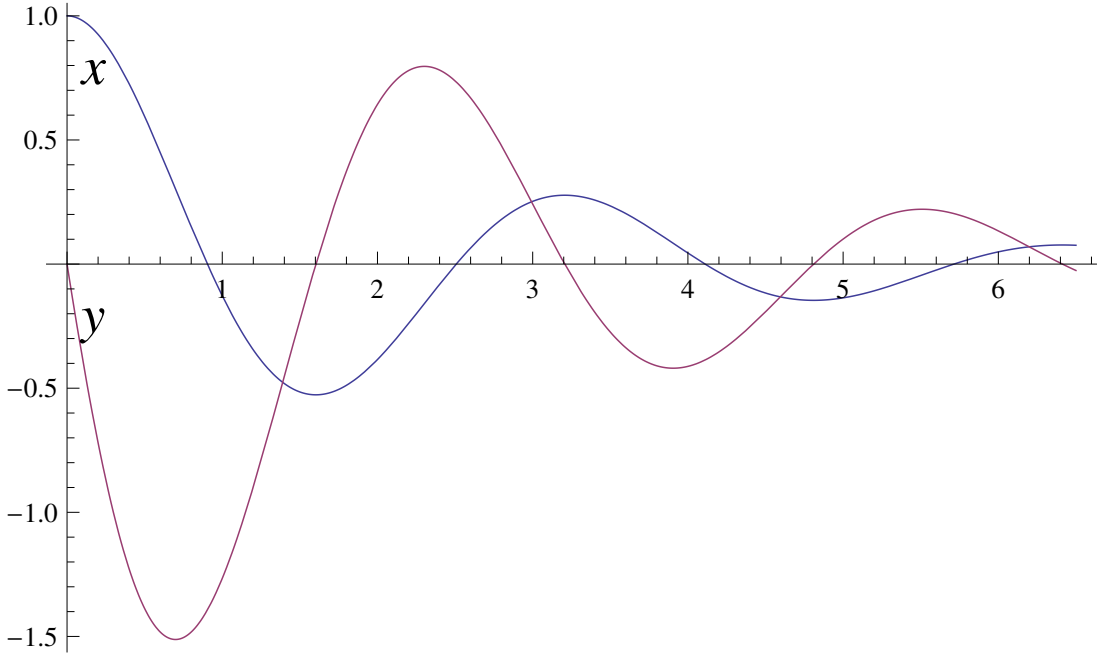
$$\omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, (\omega \geq 0 \land d \geq 0)]\, \omega^2 x^2 + y^2 \leq c^2$$



Example: Differential Invariant Inequalities

$$\frac{\omega\geq 0 \land d\geq 0 \vdash 2\omega^2 xy + 2y(-\omega^2 x - 2d\omega y) \leq 0 \quad *}{\omega\geq 0 \land d\geq 0 \vdash [x':=y][y':=-\omega^2 x - 2d\omega y]2\omega^2 xx' + 2yy' \leq 0}$$

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



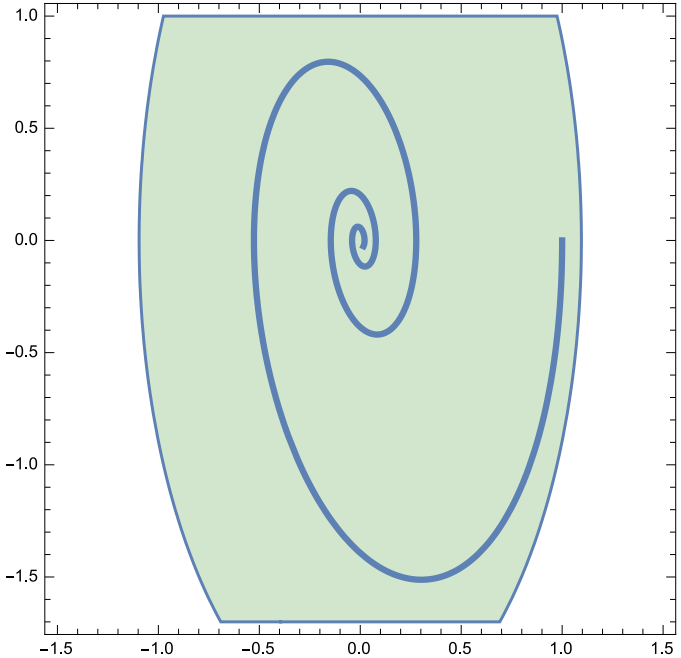
Example: Differential Invariant Inequalities: Oscillator

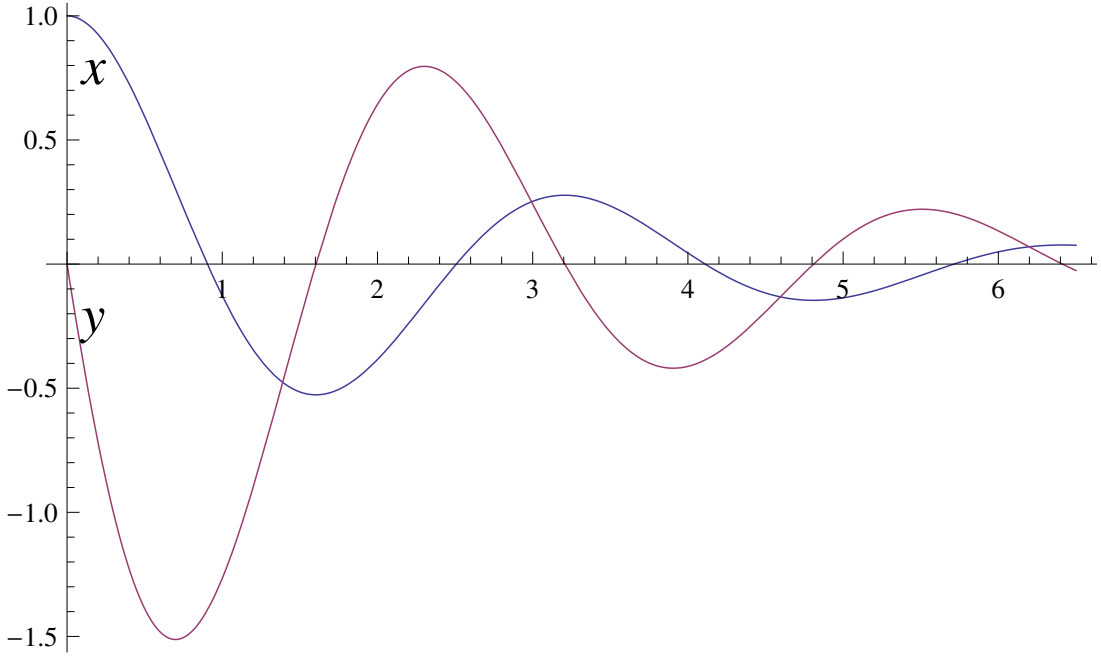
$$*$$

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

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

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

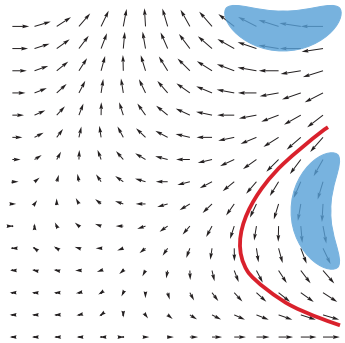




Differential Invariant Conjunctions

Differential Invariant

$$\text{dI}\ \frac{}{P \wedge Q \vdash [x' = f(x)](P \wedge Q)}$$

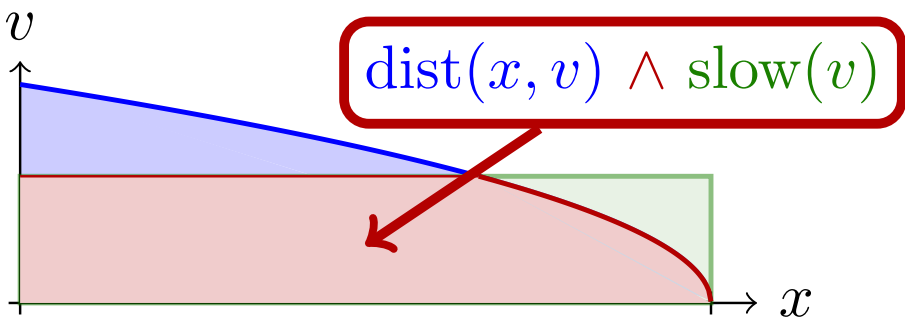


Differential Invariant Conjunctions

Differential Invariant

$$\text{dI}\quad \frac{\vdash [x' := f(x)]((P)' \land (Q)')}{P \land Q \vdash [x' = f(x)](P \land Q)}$$

$$\text{DI}\quad \frac{\vdash [x' = f(x)]((P)' \land (Q)')}{P \land Q \vdash [x' = f(x)](P \land Q)}$$

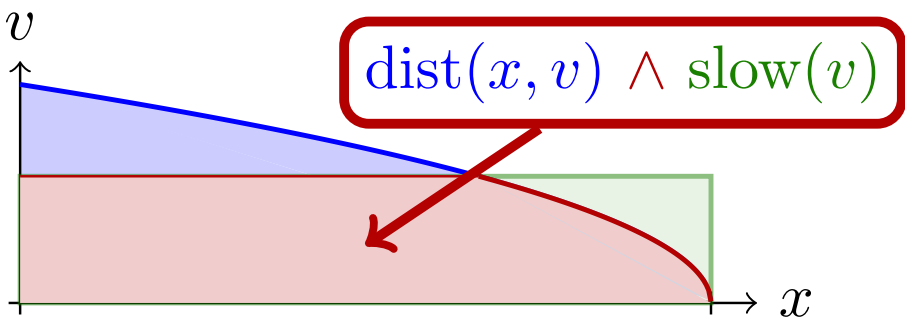


Differential Invariant Conjunctions

Differential Invariant

$$\text{dI}\quad \frac{\vdash [x' := f(x)]((P)' \wedge (Q)')}{P \wedge Q \vdash [x' = f(x)](P \wedge Q)}$$

$$\text{DI}\quad \frac{\vdash [x' = f(x)]((P)' \wedge (Q)')}{P \wedge Q \vdash [x' = f(x)](P \wedge Q)}$$



Proof (separately).

$$[]\wedge,\text{WL}\ \frac{\text{DI}\ \dfrac{\vdash [x' = f(x)](P)'}{P \vdash [x' = f(x)]P} \qquad \text{DI}\ \dfrac{\vdash [x' = f(x)](Q)'}{Q \vdash [x' = f(x)]Q}}{P \wedge Q \vdash [x' = f(x)](P \wedge Q)}$$

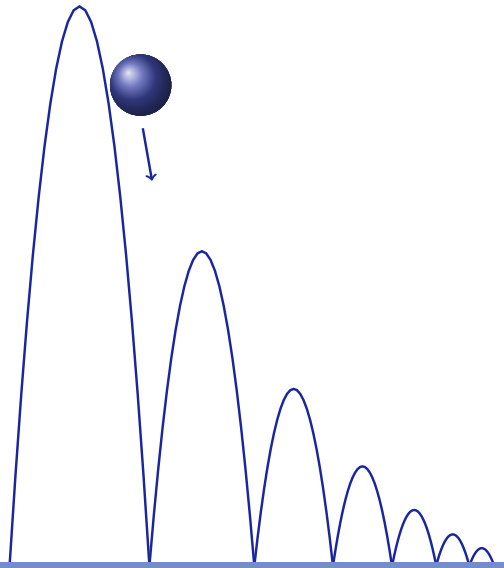
□

$[]\wedge\quad [\alpha](P \wedge Q) \leftrightarrow [\alpha]P \wedge [\alpha]Q$

Quantum's Back for a Differential Invariant Proof

$$2gx{=}2gH{-}v^2 \vdash [x'' = -g \,\&\, x{\geq}0](2gx{=}2gH{-}v^2 \land x{\geq}0)$$

No solutions but still a proof.
Simple proof with simple arithmetic.
Independent proofs for independent questions.

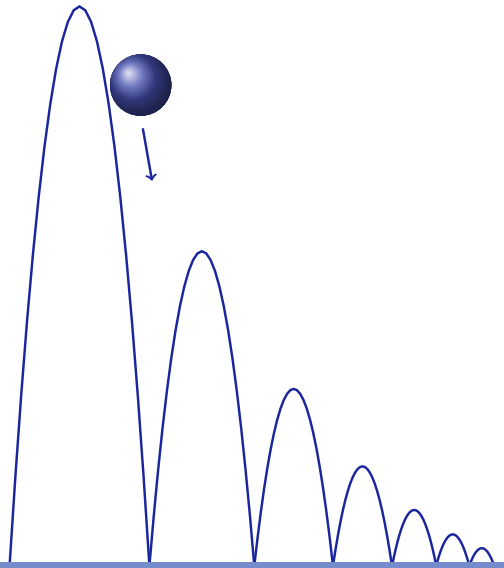


Quantum's Back for a Differential Invariant Proof

$[]\wedge \quad [\alpha](P \wedge Q) \leftrightarrow [\alpha]P \wedge [\alpha]Q$

$$[]\wedge \frac{\dfrac{}{2gx{=}2gH{-}v^2 \vdash [x''{=}{-}g \,\&\, x{\geq}0]2gx{=}2gH{-}v^2} \qquad \dfrac{}{\vdash [x''{=}{-}g \,\&\, x{\geq}0]x{\geq}0}}{2gx{=}2gH{-}v^2 \vdash [x'' = -g \,\&\, x{\geq}0](2gx{=}2gH{-}v^2 \wedge x{\geq}0)}$$

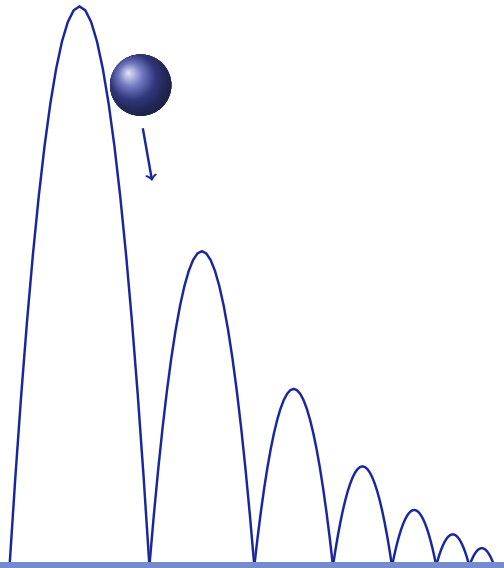
No solutions but still a proof.
Simple proof with simple arithmetic.
Independent proofs for independent questions.



Quantum's Back for a Differential Invariant Proof

$$
[]\wedge\dfrac{\mathrm{dI}\dfrac{\dfrac{}{x\geq 0 \vdash [x':=v][v':=-g]2gx' = -2vv'}}{2gx{=}2gH{-}v^2 \vdash [x''{=}{-}g \,\&\, x\geq 0]2gx{=}2gH{-}v^2} \qquad \dfrac{}{\vdash [x''{=}{-}g \,\&\, x\geq 0]x\geq 0}}{2gx{=}2gH{-}v^2 \vdash [x'' = -g \,\&\, x\geq 0](2gx{=}2gH{-}v^2 \wedge x\geq 0)}
$$

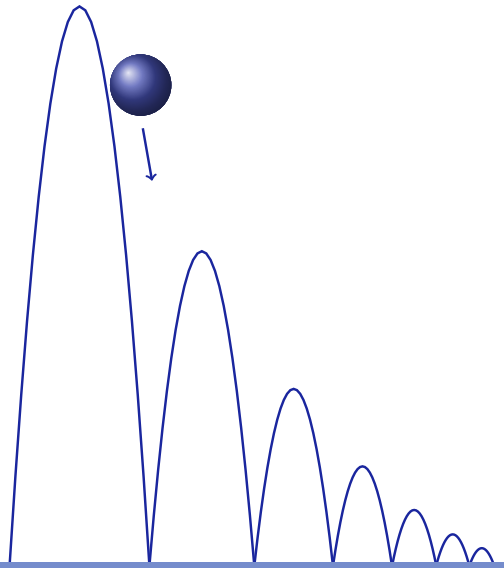
No solutions but still a proof.
Simple proof with simple arithmetic.
Independent proofs for independent questions.



Quantum's Back for a Differential Invariant Proof

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{x{\geq}0 \vdash 2gv = -2v(-g)}}{x{\geq}0 \vdash [x'{:=}v][v'{:=}-g]2gx' = -2vv'}\,[']}{2gx{=}2gH{-}v^2 \vdash [x''{=}{-}g \,\&\, x{\geq}0]2gx{=}2gH{-}v^2}\,\mathsf{dI} \qquad \dfrac{}{\vdash [x''{=}{-}g \,\&\, x{\geq}0]x{\geq}0}}{2gx{=}2gH{-}v^2 \vdash [x'' = -g \,\&\, x{\geq}0](2gx{=}2gH{-}v^2 \land x{\geq}0)}\,[]\land
$$

No solutions but still a proof.
Simple proof with simple arithmetic.
Independent proofs for independent questions.



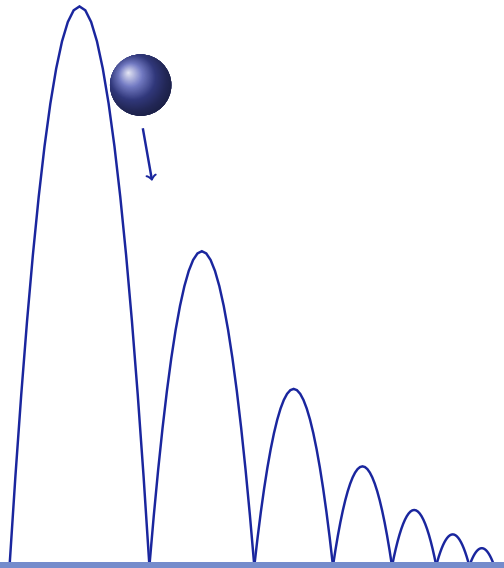
Quantum's Back for a Differential Invariant Proof

$$
\dfrac{\dfrac{\dfrac{\dfrac{*}{x\geq 0 \vdash 2gv = -2v(-g)}\,\mathbb{R}}{x\geq 0 \vdash [x':=v][v':=-g]2gx' = -2vv'}\,[':=]}{2gx{=}2gH{-}v^2 \vdash [x''{=}{-g}\,\&\,x\geq 0]2gx{=}2gH{-}v^2}\,\mathsf{dI} \qquad \dfrac{}{\vdash [x''{=}{-g}\,\&\,x\geq 0]x\geq 0}}{2gx{=}2gH{-}v^2 \vdash [x'' = -g\,\&\,x\geq 0](2gx{=}2gH{-}v^2 \wedge x\geq 0)}\,[]\wedge
$$

No solutions but still a proof.

Simple proof with simple arithmetic.

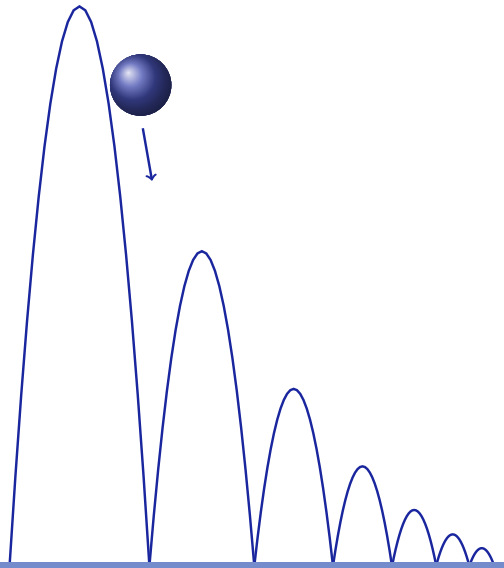
Independent proofs for independent questions.



Quantum's Back for a Differential Invariant Proof

$$
\dfrac{\dfrac{\dfrac{\dfrac{*}{x\geq 0 \vdash 2gv = -2v(-g)}\,\mathbb{R}}{x\geq 0 \vdash [x'{:=}v][v'{:=}-g]2gx' = -2vv'}\,[{}'{:=}]}{2gx{=}2gH{-}v^2 \vdash [x''{=}{-}g \,\&\, x\geq 0]2gx{=}2gH{-}v^2}\,\mathrm{dI} \quad \dfrac{\dfrac{}{x\geq 0 \vdash x\geq 0}}{\vdash [x''{=}{-}g \,\&\, x\geq 0]x\geq 0}\,\mathrm{dW}}{2gx{=}2gH{-}v^2 \vdash [x'' = -g \,\&\, x\geq 0](2gx{=}2gH{-}v^2 \wedge x\geq 0)}\,[]\wedge
$$

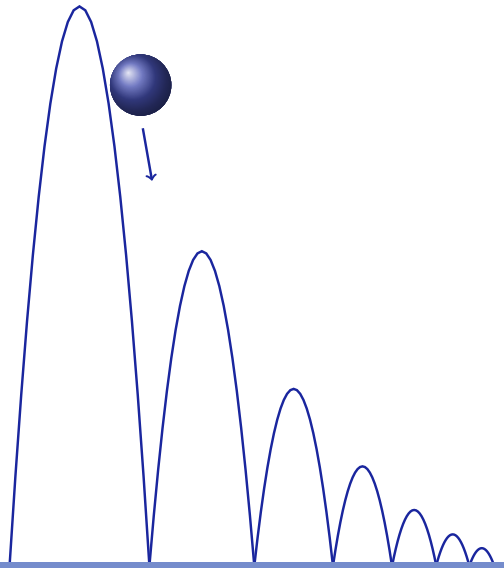
No solutions but still a proof.
Simple proof with simple arithmetic.
Independent proofs for independent questions.



Quantum's Back for a Differential Invariant Proof

$$
\dfrac{\dfrac{\dfrac{\dfrac{*}{x\geq 0 \vdash 2gv = -2v(-g)}\,\mathbb{R}}{x\geq 0 \vdash [x'{:=}v][v'{:=}-g]2gx' = -2vv'}\,[':=]}{2gx{=}2gH{-}v^2 \vdash [x''{=}{-}g \,\&\, x\geq 0]2gx{=}2gH{-}v^2}\,\mathrm{dI} \quad \dfrac{\dfrac{*}{x\geq 0 \vdash x\geq 0}\,\mathrm{id}}{\vdash [x''{=}{-}g \,\&\, x\geq 0]x\geq 0}\,\mathrm{dW}}{2gx{=}2gH{-}v^2 \vdash [x'' = -g \,\&\, x\geq 0](2gx{=}2gH{-}v^2 \wedge x\geq 0)}\,[]\wedge
$$

No solutions but still a proof.
Simple proof with simple arithmetic.
Independent proofs for independent questions.

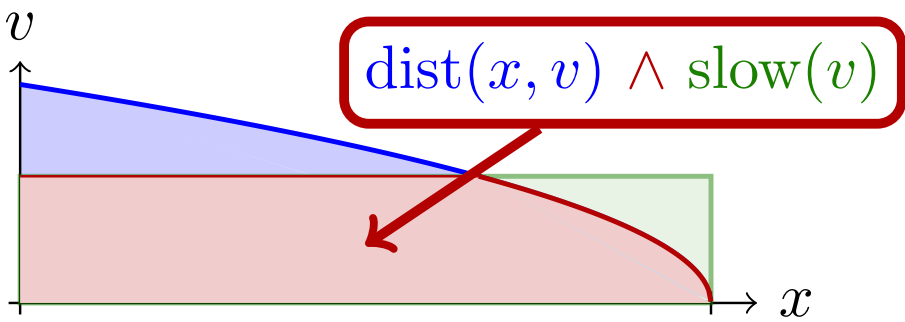


Differential Invariant Conjunctions

Differential Invariant

$$\text{dI}\quad \frac{\vdash [x' := f(x)]((P)' \land (Q)')}{P \land Q \vdash [x' = f(x)](P \land Q)}$$

$$\text{DI}\quad \frac{\vdash [x' = f(x)]((P)' \land (Q)')}{P \land Q \vdash [x' = f(x)](P \land Q)}$$

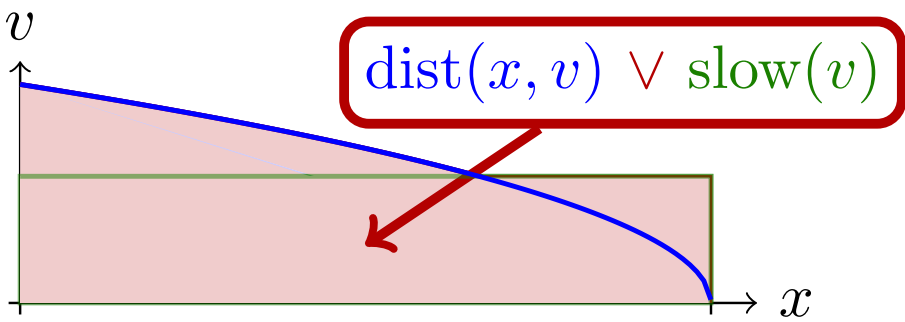


Differential Invariant Disjunctions

Differential Invariant

$$\text{dI}\quad \frac{\vdash [x' := f(x)]((P)' \vee (Q)')}{P \vee Q \vdash [x' = f(x)](P \vee Q)}$$

$$\text{DI}\quad \frac{\vdash [x' = f(x)]((P)' \vee (Q)')}{P \vee Q \vdash [x' = f(x)](P \vee Q)}$$

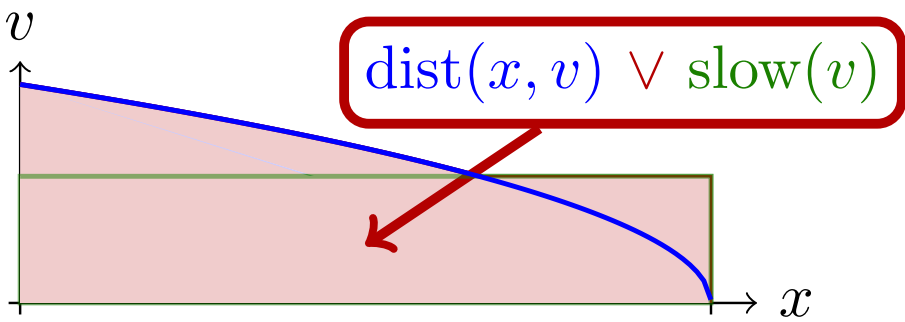


Differential Invariant Disjunctions

Differential Invariant

$$\text{dI}\quad \frac{\vdash [x' := f(x)]((P)' \vee (Q)')}{P \vee Q \vdash [x' = f(x)](P \vee Q)}$$

$$\text{DI}\quad \frac{\vdash [x' = f(x)]((P)' \vee (Q)')}{P \vee Q \vdash [x' = f(x)](P \vee Q)}$$

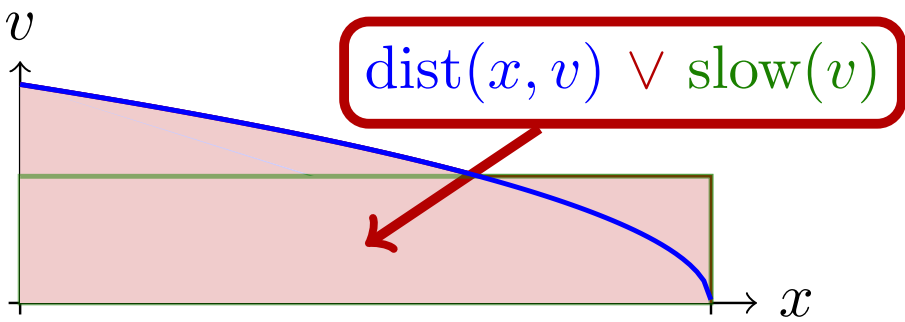


Differential Invariant Disjunctions

Differential Invariant

$$\text{dI}\quad \frac{\vdash [x' := f(x)]((P)' \land (Q)')}{P \lor Q \vdash [x' = f(x)](P \lor Q)}$$

$$\text{DI}\quad \frac{\vdash [x' = f(x)]((P)' \land (Q)')}{P \lor Q \vdash [x' = f(x)](P \lor Q)}$$

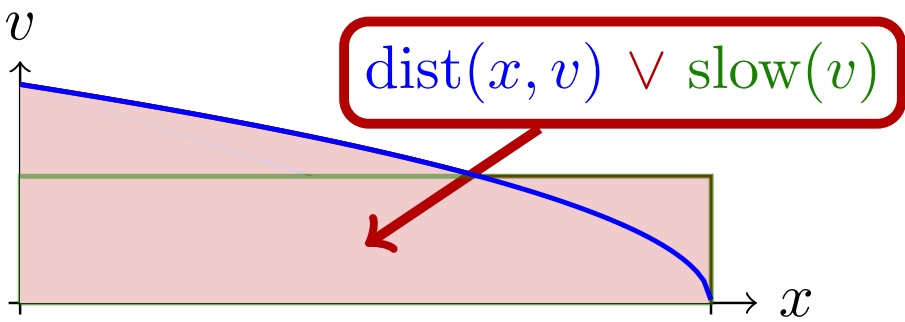


Differential Invariant Disjunctions

Differential Invariant

$$\text{dI}\ \frac{\vdash [x' := f(x)]((P)' \land (Q)')}{P \lor Q \vdash [x' = f(x)](P \lor Q)}$$

$$\text{DI}\ \frac{\vdash [x' = f(x)]((P)' \land (Q)')}{P \lor Q \vdash [x' = f(x)](P \lor Q)}$$

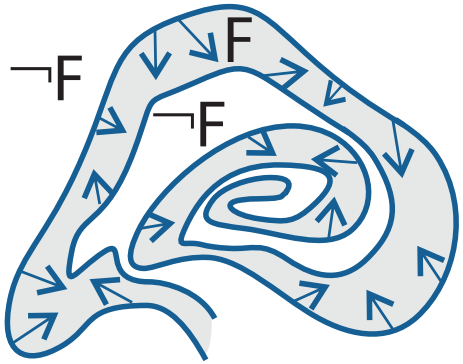


Proof (separately).

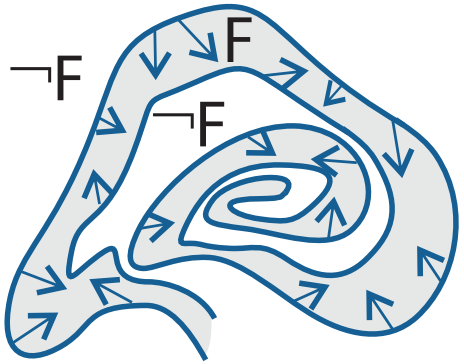
$$\vee\text{L}\ \frac{\text{MR}\ \dfrac{\dfrac{*}{P \vdash P \lor Q} \quad \text{DI}\ \dfrac{\vdash [x'=f(x)](P)'}{P \vdash [x'=f(x)]P}}{P \vdash [x' = f(x)](P \lor Q)} \qquad \text{MR}\ \dfrac{\dfrac{*}{Q \vdash P \lor Q} \quad \text{DI}\ \dfrac{\vdash [x'=f(x)](Q)'}{Q \vdash [x'=f(x)]Q}}{Q \vdash [x' = f(x)](P \lor Q)}}{P \lor Q \vdash [x' = f(x)](P \lor Q)}$$

□

Assuming Differential Invariance



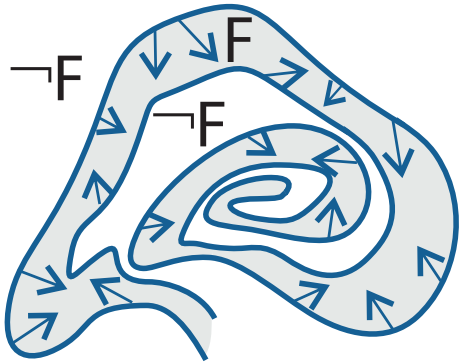
$$\frac{Q \to [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$



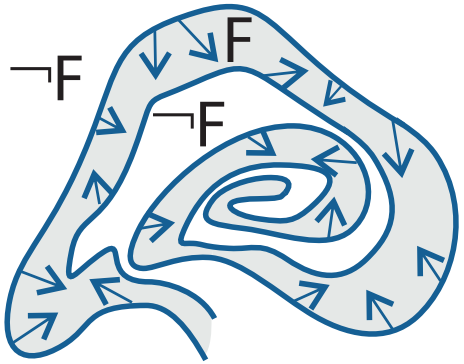
$$\frac{F \land Q \to [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$

$$\text{loop} \quad \frac{F \vdash [\alpha]F}{F \vdash [\alpha^*]F}$$

Assuming Differential Invariance



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

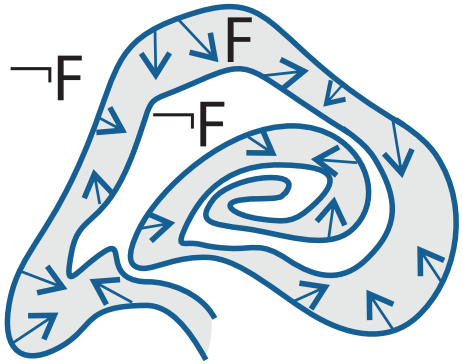


$$\frac{F \land Q \to [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$

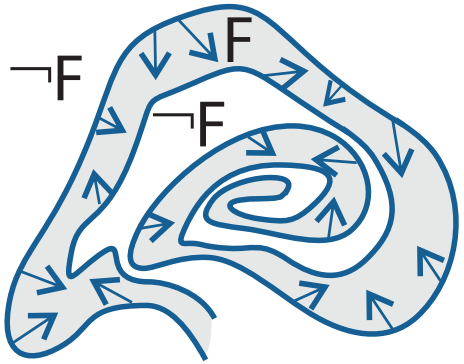
Example (Restrictions)

$$\frac{}{v^2 - 2v + 1 = 0 \vdash [v' = w, w' = -v]v^2 - 2v + 1 = 0}$$

Assuming Differential Invariance



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

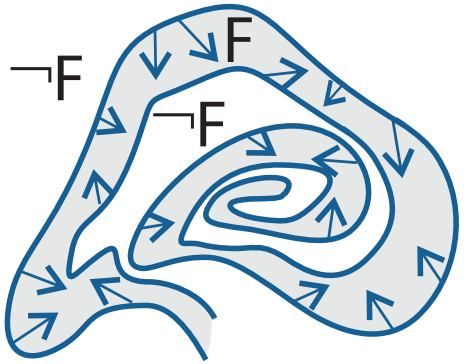


$$\frac{F \land Q \to [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$

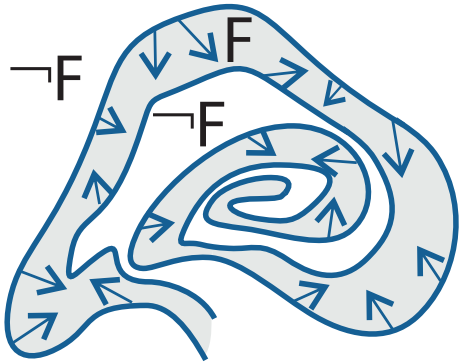
Example (Restrictions)

$$\frac{\dfrac{}{v^2 - 2v + 1 = 0 \vdash [v' := w][w' := -v]2vv' - 2v' = 0}}{v^2 - 2v + 1 = 0 \vdash [v' = w, w' = -v]v^2 - 2v + 1 = 0}$$

Assuming Differential Invariance



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

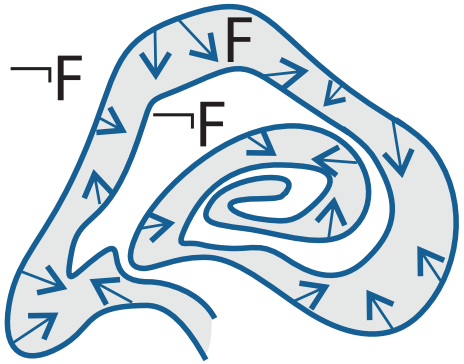


$$\frac{F \land Q \to [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$

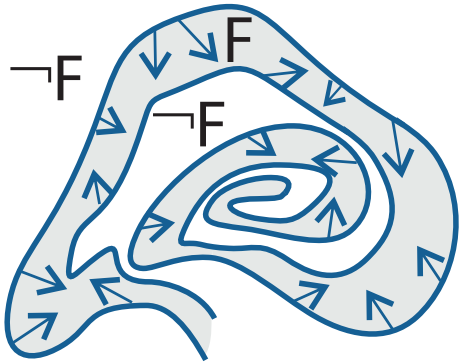
Example (Restrictions)

$$\frac{\dfrac{\dfrac{}{v^2 - 2v + 1 = 0 \vdash 2vw - 2w = 0}}{v^2 - 2v + 1 = 0 \vdash [v' := w][w' := -v]2vv' - 2v' = 0}}{v^2 - 2v + 1 = 0 \vdash [v' = w, w' = -v]v^2 - 2v + 1 = 0}$$

Assuming Differential Invariance



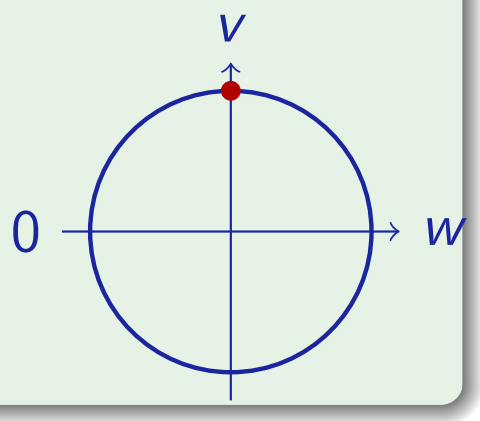
$$\frac{Q \to [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$



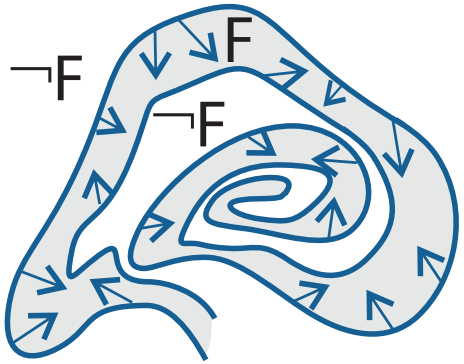
$$\frac{F \land Q \to [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$

Example (Restrictions)

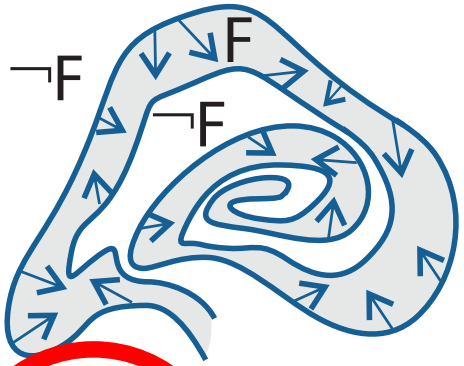
$$\frac{\dfrac{\dfrac{}{v^2 - 2v + 1 = 0 \vdash 2vw - 2w = 0}}{v^2 - 2v + 1 = 0 \vdash [v' := w][w' := -v]2vv' - 2v' = 0}}{v^2 - 2v + 1 = 0 \vdash [v' = w, w' = -v]v^2 - 2v + 1 = 0}$$



Assuming Differential Invariance



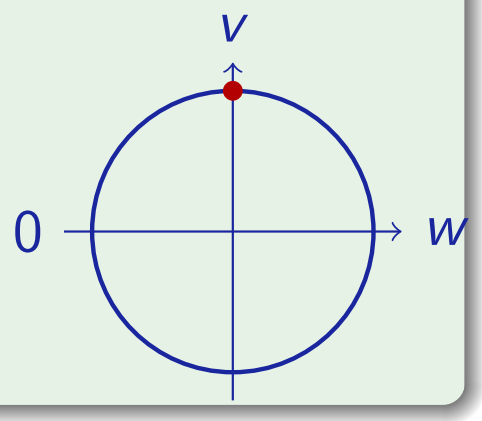
$$\frac{Q \to [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$



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

Example (Restrictions are unsound!)

$$\frac{\dfrac{\dfrac{}{v^2 - 2v + 1 = 0 \vdash 2vw - 2w = 0}\,(\text{unsound})}{v^2 - 2v + 1 = 0 \vdash [v' := w][w' := -v]2vv' - 2v' = 0}}{v^2 - 2v + 1 = 0 \vdash [v' = w, w' = -v]v^2 - 2v + 1 = 0}$$

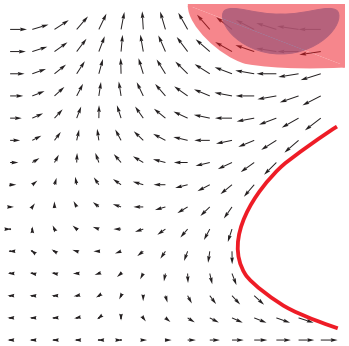


Outline

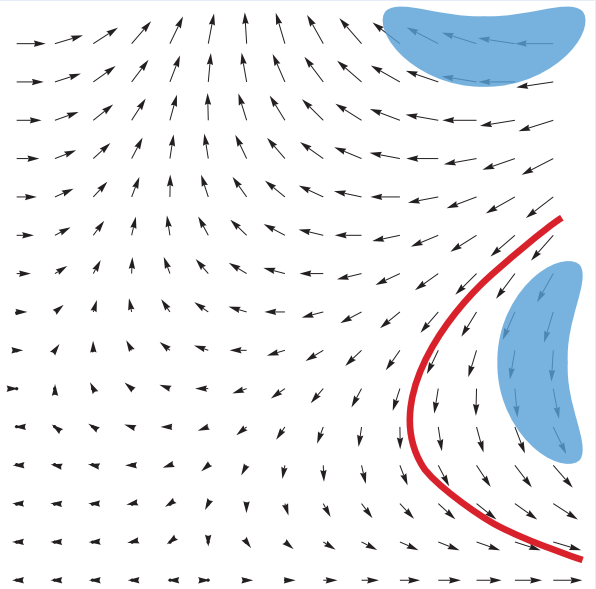
Differential Cuts

Differential Cut

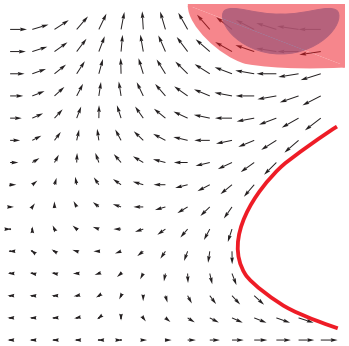
$$\frac{}{F \vdash [x' = f(x)]F}$$



Differential Cut



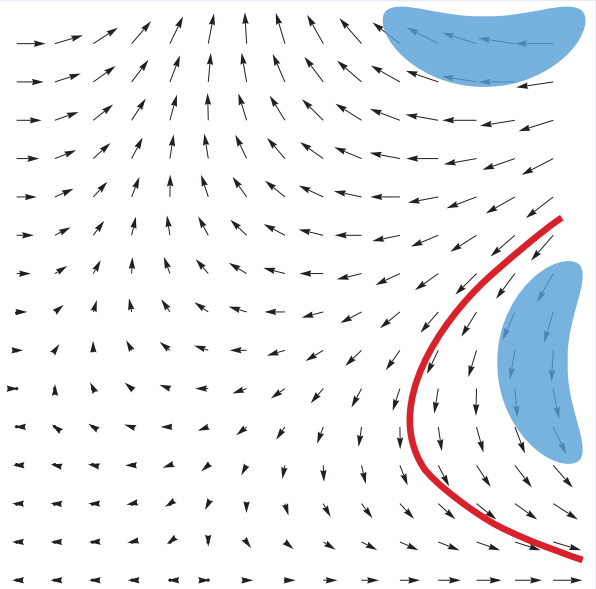
Differential Cuts



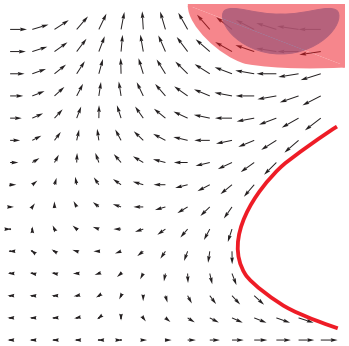
Differential Cut

$$\frac{F \vdash [x' = f(x)]C}{F \vdash [x' = f(x)]F}$$

Differential Cut



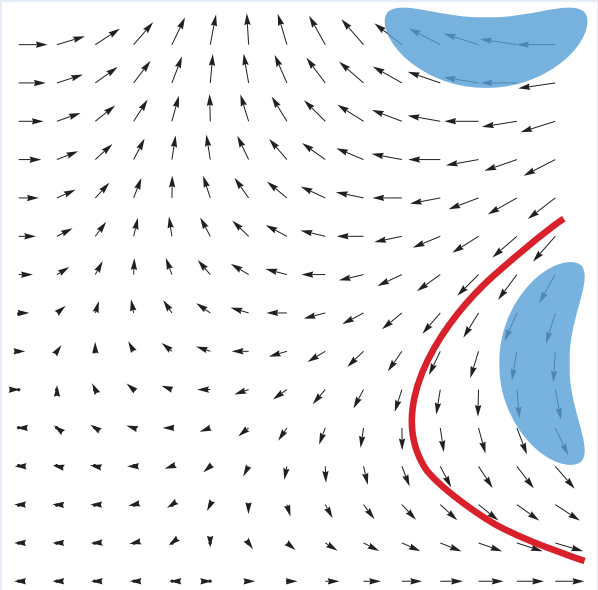
Differential Cuts



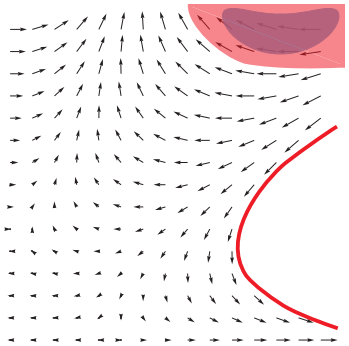
Differential Cut

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

Differential Cut



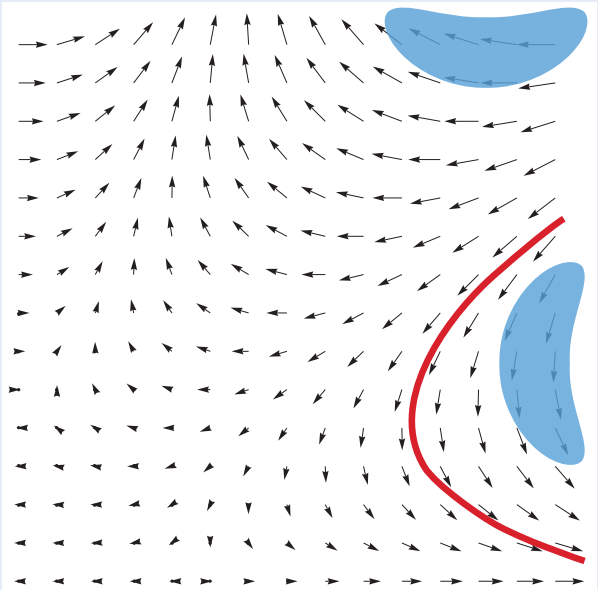
Differential Cuts



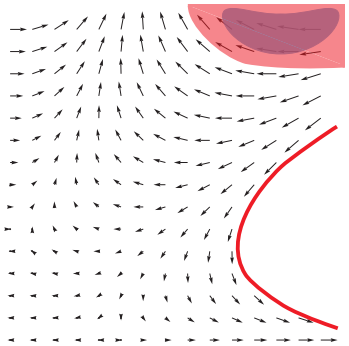
Differential Cut

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

Differential Cut



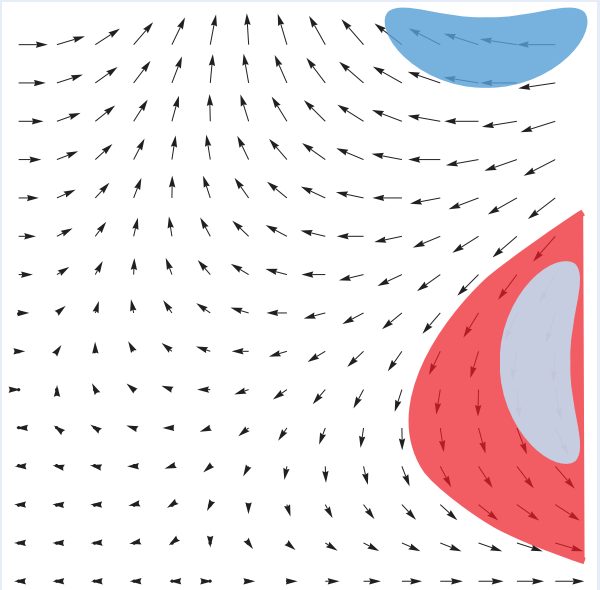
Differential Cuts



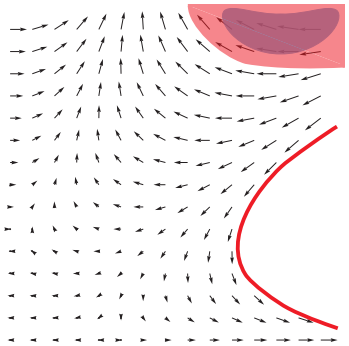
Differential Cut

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

Differential Cut



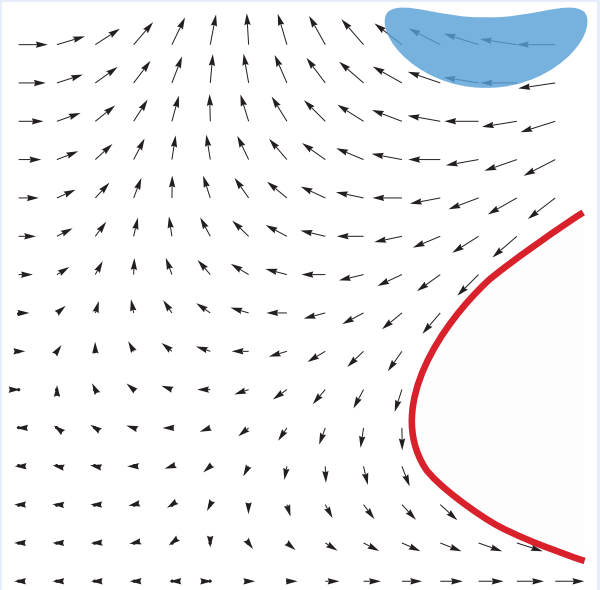
Differential Cuts



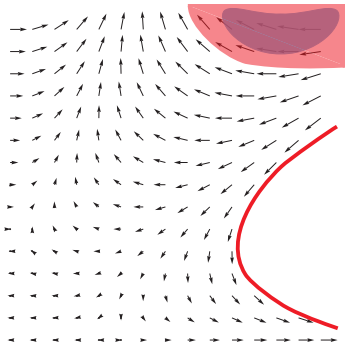
Differential Cut

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

Differential Cut



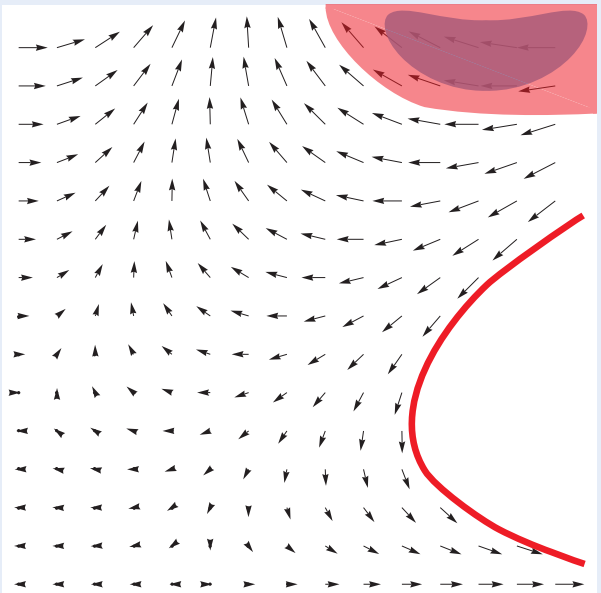
Differential Cuts



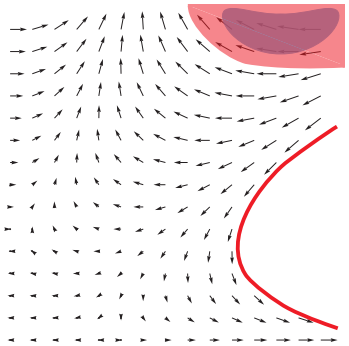
Differential Cut

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

Differential Cut



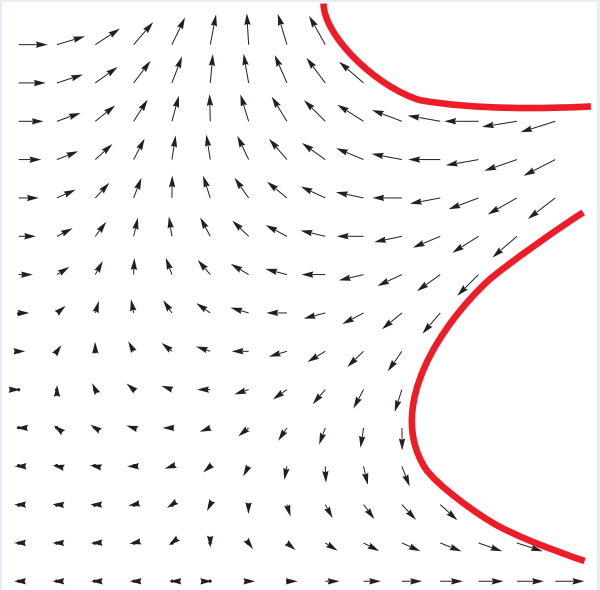
Differential Cuts



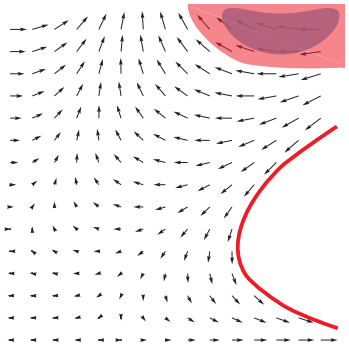
Differential Cut

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

Differential Cut



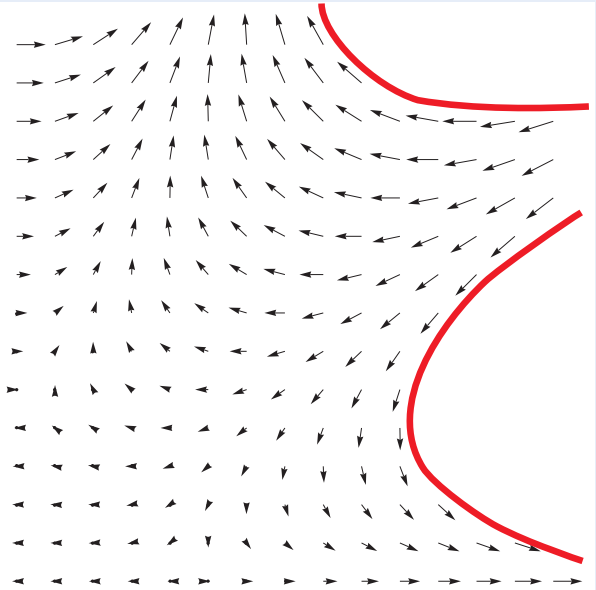
Differential Cuts



Differential Cut

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

Differential Cut



Proof (Soundness).

Let $\varphi \models x' = f(x) \wedge Q$ starting in $\omega \in [\![F]\!]$.
$\omega \in [\![[x' = f(x) \,\&\, Q]C]\!]$ by left premise.
Thus, $\varphi \models x' = f(x) \wedge Q \wedge C$.
Thus, $\varphi(r) \in [\![F]\!]$ by second premise. $\square$

Ex: Differential Cuts

$$\text{DC}\ \frac{}{x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x-2)^4 + y^5, y' = y^2]x^3 \geq -1}$$

Ex: Differential Cuts

$$\text{DC}\ \frac{}{x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x-2)^4 + y^5, y' = y^2]x^3 \geq -1}$$

$$\text{dI}\ \frac{}{y^5 \geq 0 \vdash [x' = (x-2)^4 + y^5, y' = y^2]y^5 \geq 0}$$

Ex: Differential Cuts

$$\text{DC}\ \frac{}{x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x-2)^4 + y^5, y' = y^2]x^3 \geq -1}$$

$$\text{dI}\ \frac{\text{['}:=\text{]}\ \dfrac{}{\vdash [x':=(x-2)^4 + y^5][y':=y^2]5y^4 y' \geq 0}}{y^5 \geq 0 \vdash [x' = (x-2)^4 + y^5, y' = y^2]y^5 \geq 0}$$

Ex: Differential Cuts

$$\text{DC}\ \frac{}{x^3 \geq -1 \wedge y^5 \geq 0 \vdash [x' = (x-2)^4 + y^5, y' = y^2]x^3 \geq -1}$$

$$\text{dI}\ \frac{\text{[}':=\text{]}\ \dfrac{\mathbb{R}\ \dfrac{}{\vdash 5y^4 y^2 \geq 0}}{\vdash [x':=(x-2)^4 + y^5][y':=y^2]5y^4 y' \geq 0}}{y^5 \geq 0 \vdash [x' = (x-2)^4 + y^5, y' = y^2]y^5 \geq 0}$$

Ex: Differential Cuts

$$
\begin{array}{ll}
\text{DC} & x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x-2)^4 + y^5, y' = y^2]x^3 \geq -1 \\
\hline
\mathbb{R} & \qquad * \\
\hline
\mathbb{R} & \qquad \vdash 5y^4 y^2 \geq 0 \\
\hline
[':=] & \qquad \vdash [x':=(x-2)^4 + y^5][y':=y^2]5y^4 y' \geq 0 \\
\hline
\text{dI} & y^5 \geq 0 \vdash [x' = (x-2)^4 + y^5, y' = y^2]y^5 \geq 0
\end{array}
$$

Ex: Differential Cuts

$$\text{dI}\ \frac{}{x^3 \geq -1 \vdash [x' = (x-2)^4 + y^5, y' = y^2 \,\&\, y^5 \geq 0]x^3 \geq -1 \ \triangleright}$$

$$\text{DC}\ \frac{}{x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x-2)^4 + y^5, y' = y^2]x^3 \geq -1}$$

$$\text{dI}\ \frac{\text{[}'{:=}\text{]}\ \frac{\mathbb{R}\ \frac{*}{\vdash 5y^4 y^2 \geq 0}}{\vdash [x'{:=}(x-2)^4 + y^5][y'{:=}y^2]5y^4 y' \geq 0}}{y^5 \geq 0 \vdash [x' = (x-2)^4 + y^5, y' = y^2]y^5 \geq 0}$$

Ex: Differential Cuts

$$
\begin{array}{ll}
[':=] & y^5 \geq 0 \vdash [x':=(x-2)^4+y^5][y':=y^2]2x^2x' \geq 0 \\
\hline
\text{dI} & x^3 \geq -1 \vdash [x' = (x-2)^4+y^5, y' = y^2 \,\&\, y^5 \geq 0]x^3 \geq -1 \quad \triangleright \\
\hline
\text{DC} & x^3 \geq -1 \wedge y^5 \geq 0 \vdash [x' = (x-2)^4+y^5, y' = y^2]x^3 \geq -1
\end{array}
$$

$$
\begin{array}{ll}
 & * \\
\hline
\mathbb{R} & \vdash 5y^4y^2 \geq 0 \\
\hline
[':=] & \vdash [x':=(x-2)^4+y^5][y':=y^2]5y^4y' \geq 0 \\
\hline
\text{dI} & y^5 \geq 0 \vdash [x' = (x-2)^4+y^5, y' = y^2]y^5 \geq 0
\end{array}
$$

Ex: Differential Cuts

$$
\begin{array}{ll}
\mathbb{R} & y^5 \geq 0 \vdash 2x^2((x-2)^4 + y^5) \geq 0 \\
\hline
[':=] & y^5 \geq 0 \vdash [x':=(x-2)^4 + y^5][y':=y^2]2x^2x' \geq 0 \\
\hline
\text{dI} & x^3 \geq -1 \vdash [x' = (x-2)^4 + y^5, y' = y^2 \,\&\, y^5 \geq 0]x^3 \geq -1 \quad \triangleright \\
\hline
\text{DC} & x^3 \geq -1 \wedge y^5 \geq 0 \vdash [x' = (x-2)^4 + y^5, y' = y^2]x^3 \geq -1
\end{array}
$$

$$
\begin{array}{ll}
 & * \\
\hline
\mathbb{R} & \vdash 5y^4y^2 \geq 0 \\
\hline
[':=] & \vdash [x':=(x-2)^4 + y^5][y':=y^2]5y^4y' \geq 0 \\
\hline
\text{dI} & y^5 \geq 0 \vdash [x' = (x-2)^4 + y^5, y' = y^2]y^5 \geq 0
\end{array}
$$

Ex: Differential Cuts

$$
\begin{array}{ll}
 & * \\
\hline
\mathbb{R} & y^5 \geq 0 \vdash 2x^2((x-2)^4 + y^5) \geq 0 \\
\hline
[':=] & y^5 \geq 0 \vdash [x':=(x-2)^4 + y^5][y':=y^2]2x^2x' \geq 0 \\
\hline
\text{dI} & x^3 \geq -1 \vdash [x' = (x-2)^4 + y^5, y' = y^2 \,\&\, y^5 \geq 0]x^3 \geq -1 \quad \triangleright \\
\hline
\text{DC} & x^3 \geq -1 \wedge y^5 \geq 0 \vdash [x' = (x-2)^4 + y^5, y' = y^2]x^3 \geq -1
\end{array}
$$

$$
\begin{array}{ll}
 & * \\
\hline
\mathbb{R} & \vdash 5y^4y^2 \geq 0 \\
\hline
[':=] & \vdash [x':=(x-2)^4 + y^5][y':=y^2]5y^4y' \geq 0 \\
\hline
\text{dI} & y^5 \geq 0 \vdash [x' = (x-2)^4 + y^5, y' = y^2]y^5 \geq 0
\end{array}
$$

Outline

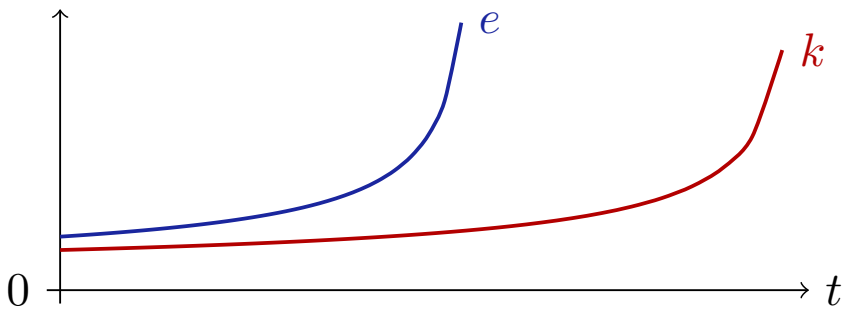
Soundness Proof: Differential Invariants

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

$$\varphi \models x' = f(x) \wedge Q \text{ for } r > 0 \;\Rightarrow\; \forall 0 \leq z \leq r \;\; [\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

Differential Invariant

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



Proof ($\geq$ rate of change from $\geq$ initial value. Case $r = 0$ is easier.)

$h(t) \stackrel{\text{def}}{=} [\![e]\!]\varphi(t)$ is differentiable on $[0, r]$ if $r > 0$.

$\frac{\mathrm{d}h(t)}{\mathrm{d}t}(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z) = [\![(e)']\!]\varphi(z) \geq 0$ by lemma + premise for all z.

$h(r) - \underbrace{h(0)}_{\geq 0} = \underbrace{(r - 0)}_{>0} \underbrace{\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi)}_{\geq 0} \geq 0$ by mean-value theorem for some ξ. $\square$

Outline

Differential Invariants for Differential Equations

Differential Weakening

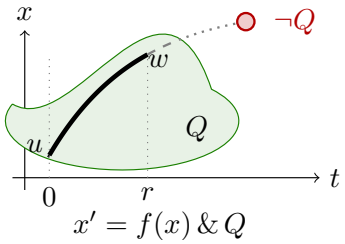
$$\frac{Q \vdash F}{P \vdash [x' = f(x) \,\&\, Q]F}$$

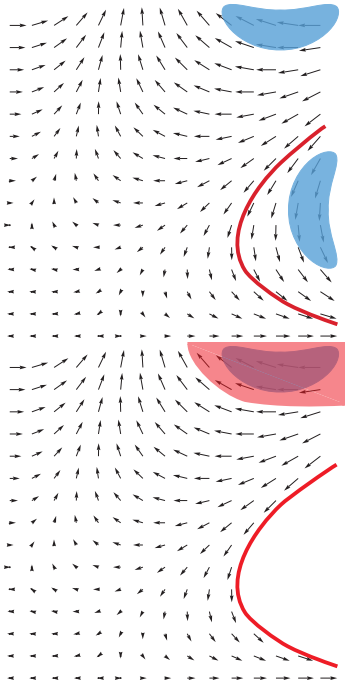
Differential Invariant

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

Differential Cut

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





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.