11: Differential Equations & Proofs
15-424: Foundations of Cyber-Physical Systems

André Platzer

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

1. Learning Objectives
2. Differential Invariants
   - Recap: Ingredients for Differential Equation Proofs
   - Soundness: Derivations Lemma
   - Differential Weakening
   - Differential Invariant Equations
   - Example Proof: Damped Oscillator
   - Conjunctive Differential Invariants
   - Disjunctive Differential Invariants
   - Assuming Invariants
3. Differential Cuts
4. Soundness
5. Summary
Outline

1 Learning Objectives

2 Differential Invariants
   - Recap: Ingredients for Differential Equation Proofs
   - Soundness: Derivations Lemma
   - Differential Weakening
   - Differential Invariant Equations
   - Example Proof: Damped Oscillator
   - Conjunctive Differential Invariants
   - Disjunctive Differential Invariants
   - Assuming Invariants

3 Differential Cuts

4 Soundness

5 Summary
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 $A \land B$, syntactically? If $A$ is true, is $A \land B$ true, too? Conversely?
Outline

1 Learning Objectives

2 Differential Invariants
   - Recap: Ingredients for Differential Equation Proofs
   - Soundness: Derivations Lemma
   - Differential Weakening
   - Differential Invariant Equations
   - Example Proof: Damped Oscillator
   - Conjunctive Differential Invariants
   - Disjunctive Differential Invariants
   - Assuming Invariants

3 Differential Cuts

4 Soundness

5 Summary
Differentials

**Syntax**

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

**Semantics**

\[
\llbracket (e)' \rrbracket_\omega = \sum_x \omega(x') \frac{\partial \llbracket e \rrbracket}{\partial x}(\omega)
\]

\[
(e + k)' = (e)' + (k)'
\]

\[
(e \cdot k)' = (e)' \cdot k + e \cdot (k)'
\]

\[
(c())' = 0 \quad \text{for constants/numbers } c()
\]

\[
(x)' = x' \quad \text{for variables } x \in V
\]

**Axioms**

**ODE**

\[
\llbracket x' = f(x) \land Q \rrbracket = \{ (\varphi(0), \varphi(r)) : \varphi \models x' = f(x) \land Q \land \text{for some } \varphi : [0, r] \to S, \text{ some } r \in \mathbb{R} \}
\]

\[
\varphi(\zeta)(x') = \frac{d\varphi(t)(x)}{dt}(\zeta)
\]

André Platzer (CMU)
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 $0 \leq z \leq r$:

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

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

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

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

\[
\begin{align*}
(e + k)' &= (e)' + (k)' \\
(e \cdot k)' &= (e)' \cdot k + e \cdot (k)' \\
(c())' &= 0 & \text{for constants/numbers } c() \\
(x)' &= x' & \text{for variables } x \in \mathcal{V}
\end{align*}
\]
### Lemma (Differential lemma) (Differential value vs. Time-derivative)

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

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

### 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)

\[
\begin{align*}
+ & \quad (e + k)' = (e)' + (k)' \\
\cdot & \quad (e \cdot k)' = (e)' \cdot k + e \cdot (k)' \\
c & \quad (c())' = 0 \\
x & \quad (x)' = x'
\end{align*}
\]
### Soundness: Proof of Derivations Lemma

#### Lemma (Derivations)

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

#### Equations of Differentials

$$x' = x'$$
<table>
<thead>
<tr>
<th>Lemma (Derivations)</th>
<th>(Equations of Differentials)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(e + k)'$</td>
<td>$(e)' + (k)'$</td>
</tr>
</tbody>
</table>

Proof.

$$\llbracket (e + k)' \rrbracket \omega =$$
Soundness: Proof of Derivations Lemma

Lemma (Derivations) \[(e + k)’ = (e)’ + (k)’\]

Proof.

\[
\llbracket (e + k)’ \rrbracket_\omega = \sum_x \omega(x’) \frac{\partial \llbracket e + k \rrbracket}{\partial x}(\omega)
\]
### Lemma (Derivations) (Equations of Differentials)

\[
(e + k)' = (e)' + (k)'
\]

### Proof.

\[
\frac{d}{dx}(e + k)(\omega) = \sum_x \omega(x') \frac{d}{dx}(e + k)(\omega) = \sum_x \omega(x') \frac{d}{dx}(e + k)(\omega)
\]
### Lemma (Derivations) (Equations of Differentials)

\[ (e + k)' = (e)' + (k)' \]

### Proof.

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

\[
= \sum_x \omega(x') \left( \frac{\partial [e]}{\partial x} (\omega) + \frac{\partial [k]}{\partial x} (\omega) \right)
\]
Lemma (Derivations) \( +' (e + k)' = (e)' + (k)' \)

Proof.

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

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

\[
= \sum_x \omega(x') \frac{\partial [e]}{\partial x} (\omega) + \sum_x \omega(x') \frac{\partial [k]}{\partial x} (\omega)
\]
Lemma (Derivations) (Equations of Differentials)

\[ (e + k)' = (e)' + (k)' \]

Proof.

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

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

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

\[ = [(e)'] \omega + [(k)'] \omega \]
Soundness: Proof of Derivations Lemma

**Lemma (Derivations)**

\[ (e + k)' = (e)' + (k)' \]

**Proof.**

\[
\begin{align*}
[(e + k)']_\omega &= \sum_x \omega(x') \frac{\partial [e+k]}{\partial x} (\omega) = \sum_x \omega(x') \frac{\partial ([e] + [k])}{\partial x} (\omega) \\
&= \sum_x \omega(x') \left( \frac{\partial [e]}{\partial x} (\omega) + \frac{\partial [k]}{\partial x} (\omega) \right) \\
&= \sum_x \omega(x') \frac{\partial [e]}{\partial x} (\omega) + \sum_x \omega(x') \frac{\partial [k]}{\partial x} (\omega) \\
&= [(e)']_\omega + [(k)']_\omega = [(e)' + (k)']_\omega
\end{align*}
\]
Soundness: Proof of Derivations Lemma

**Lemma (Derivations)**

\[(e + k)' = (e)' + (k)'

**Proof.**

\[
\begin{align*}
[(e + k)'] \omega &= \sum_x \omega(x') \frac{\partial [e + k]}{\partial x} (\omega) = \sum_x \omega(x') \frac{\partial ([e] + [k])}{\partial x} (\omega) \\
&= \sum_x \omega(x') \left( \frac{\partial [e]}{\partial x} (\omega) + \frac{\partial [k]}{\partial x} (\omega) \right) \\
&= \sum_x \omega(x') \frac{\partial [e]}{\partial x} (\omega) + \sum_x \omega(x') \frac{\partial [k]}{\partial x} (\omega) \\
&= [(e)'] \omega + [(k)'] \omega = [(e)' + (k)'] \omega
\end{align*}
\]
Differential Substitution Lemmas \[\rightsquigarrow\] Proofs

Lemma (Differential lemma) \hspace{1cm} (Differential value vs. Time-derivative)

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

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

Lemma (Differential assignment) \hspace{1cm} (Effect on Differentials)

*DE* \( [x' = f(x) \land Q] P \leftrightarrow [x' = f(x) \land Q][x' := f(x)] P \)

Lemma (Derivations) \hspace{1cm} (Equations of Differentials)

\[
\begin{align*}
+ & \quad (e + k)' = (e)' + (k)' \\
\cdot & \quad (e \cdot k)' = (e)' \cdot k + e \cdot (k)' \\
c & \quad (c())' = 0 \\
 x & \quad (x)' = x'
\end{align*}
\]
Differential Weakening

\[ [x' = f(x) \land Q] = \{(\varphi(0), \varphi(r)) : \varphi \models x' = f(x) \land Q \quad \text{for some } \varphi : [0, r] \to S, \text{ some } r \in \mathbb{R} \}\]

\[ \varphi(\zeta)(x') = \frac{d\varphi(t)(x)}{dt}(\zeta) \]
Differential Weakening

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

\[ [x' = f(x) \& Q] = \{ (\varphi(0), \varphi(r)) : \varphi \models x' = f(x) \land Q \]

\[ \text{for some } \varphi : [0, r] \rightarrow S, \text{ some } r \in \mathbb{R} \} \]

\[ \varphi(\zeta)(x') = \frac{d\varphi(t)(x)}{dt}(\zeta) \]

Differential equations cannot leave their domains.
Differential Weakening

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

**Example (Bouncing ball)**

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

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

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

Example (Bouncing ball)

\[
\begin{align*}
\text{G} & \quad \vdash [x' = v, v' = -g \land x \geq 0](x \geq 0 \rightarrow 0 \leq x) \\
\text{DW} & \quad \vdash [x' = v, v' = -g \land x \geq 0]0 \leq x
\end{align*}
\]

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

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

Example (Bouncing ball)

\[
\begin{align*}
\text{R} & \quad \vdash x \geq 0 \rightarrow 0 \leq x \\
\text{G} & \quad \vdash [x' = v, v' = -g & x \geq 0] (x \geq 0 \rightarrow 0 \leq x) \\
\text{DW} & \quad \vdash [x' = v, v' = -g & x \geq 0] 0 \leq x
\end{align*}
\]

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

\[
\text{DW } \quad [x' = f(x) & Q]P \iff [x' = f(x) & Q](Q \implies P)
\]

Example (Bouncing ball)

\[
\begin{array}{c}
\text{*} \\
\mathcal{R} & \vdash x \geq 0 \implies 0 \leq x \\
\mathcal{G} & \vdash [x' = v, v' = -g & x \geq 0](x \geq 0 \implies 0 \leq x) \\
\text{DW} & \vdash [x' = v, v' = -g & x \geq 0]0 \leq x
\end{array}
\]

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

**Differential Weakening**

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

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

**Example (Bouncing ball)**

\[
\text{R} \quad \vdash x \geq 0 \rightarrow 0 \leq x
\]

\[
\text{G} \quad \vdash [x' = v, v' = -g \& x \geq 0](x \geq 0 \rightarrow 0 \leq x)
\]

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

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

**Differential Weakening**

\[
\frac{\Gamma \vdash \forall x (q(x) \rightarrow p(x)), \Delta}{\Gamma \vdash [x' = f(x) \& q(x)]p(x), \Delta}
\]

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

**Example (Bouncing ball)**

\[
\begin{align*}
\Gamma & \vdash x \geq 0 \rightarrow 0 \leq x \\
\Gamma & \vdash [x' = v, v' = -g \& x \geq 0](x \geq 0 \rightarrow 0 \leq x) \\
\text{DW} & \vdash [x' = v, v' = -g \& x \geq 0]0 \leq x
\end{align*}
\]

No need to solve any ODEs to prove that bouncing ball is above ground.
Differential Invariant Terms for Differential Equations

**Differential Invariant**

\[
\begin{align*}
Q \vdash [x' := f(x)](e)' &= 0 \\
\vdash e = 0 \vdash [x' = f(x) \& Q]e = 0
\end{align*}
\]

\[\begin{align*}
\text{DE} & \quad [x' = f(x) \& Q]P \leftrightarrow [x' = f(x) \& Q][x' := f(x)]P \\
\text{DW} & \quad [x' = f(x) \& Q]P \leftrightarrow [x' = f(x) \& Q](Q \rightarrow P)
\end{align*}\]
Differential Invariant Terms for Differential Equations

**Differential Invariant**

\[ \text{di} \quad Q \vdash [x' := f(x)](e)' = 0 \]

\[ e = 0 \vdash [x' = f(x) \& Q]e = 0 \]

\[ \vdash [x' = f(x) \& Q](e)' = 0 \]

\[ e = 0 \vdash [x' = f(x) \& Q]e = 0 \]

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

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

\[ \text{di} \text{ is a derived rule:} \]

\[ Q \vdash [x' := f(x)](e)' = 0 \]

\[ \vdash [x' = f(x) \& Q](Q \rightarrow [x' := f(x)](e)' = 0) \]

\[ \vdash [x' = f(x) \& Q][x' := f(x)](e)' = 0 \]

\[ \vdash [x' = f(x) \& Q](e)' = 0 \]

\[ e = 0 \vdash [x' = f(x) \& Q]e = 0 \]
### Lemma (Differential lemma)

\[ \varphi \models x' = f(x) \land Q \text{ for } r > 0 \implies \forall 0 \leq z \leq r \right\downarrow (e)\varphi(z) = \frac{d[e]\varphi(t)}{dt}(z) \]

### Differential Invariant

\[ dI \quad e = k \vdash [x' = f(x)]e = k \]
Differential Invariant Equations

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

\( \varphi \models x' = f(x) \land Q \text{ for } r > 0 \Rightarrow \forall 0 \leq z \leq r \ [ (e)' ] \varphi(z) = \frac{d[e] \varphi(t)}{dt}(z) \)

Differential Invariant

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

\[
\frac{dI}{\Gamma} \vdash [x' = f(x)][(e)' = (k)']
\]
\[
e = k \vdash [x' = f(x)]e = k
\]
Lemma (Differential lemma) (Differential value vs. Time-derivative)

\[ \varphi \models x' = f(x) \land Q \text{ for } r > 0 \implies \forall 0 \leq z \leq r \quad [(e)'] \varphi(z) = \frac{d[(e)]\varphi(t)}{dt}(z) \]

Differential Invariant

\[ dI \vdash [x' := f(x)](e)' = (k)' \]

\[ e = k \vdash [x' = f(x)]e = k \]

\[ dI \vdash [x' = f(x)](e)' = (k)' \]

\[ e = k \vdash [x' = f(x)]e = k \]

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

\[ \frac{d[(e)]\varphi(t)}{dt}(z) = [(e)'] \varphi(z) = [(k)'] \varphi(z) = \frac{d[(k)]\varphi(t)}{dt}(z) \]
**Differential Invariant Inequalities**

**Lemma (Differential lemma)**

\[ \varphi |\rightarrow x' = f(x) \land Q \text{ for } r > 0 \Rightarrow \forall 0 \leq z \leq r \quad [(e)']\varphi(z) = \frac{d[e]\varphi(t)}{dt}(z) \]

**Differential Invariant**

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

\[ e \geq k \vdash [x' = f(x)]e \geq k \]

**Proof**

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

\[ \square \]
Lemma (Differential lemma)  (Differential value vs. Time-derivative)

\[ \phi \models x' = f(x) \land Q \text{ for } r > 0 \implies \forall 0 \leq z \leq r \quad ((e)')\phi(z) = \frac{d[e] \phi(t)}{dt}(z) \]

Differential Invariant

\[ \vdash [x' := f(x)](e)' \leq (k)' \]

\[ e \leq k \vdash [x' = f(x)]e \leq k \]

Proof \((\leq \text{ rate of change from } \leq \text{ initial value. Mean-value theorem}).\)

\[ \frac{d[e] \phi(t)}{dt}(z) = ((e)')\phi(z) \leq [(k)']\phi(z) = \frac{d[k] \phi(t)}{dt}(z) \]
Lemma (Differential lemma) (Differential value vs. Time-derivative)

\[ \varphi \models x' = f(x) \land Q \text{ for } r > 0 \implies \forall 0 \leq z \leq r \quad [(e)']\varphi(z) = \frac{d\llbracket e \rrbracket \varphi(t)}{dt}(z) \]

Differential Invariant

\[ \vdash [x' := f(x)](e)' > (k)' \]
\[ e > k \vdash [x' = f(x)]e > k \]

\[ \vdash [x' = f(x)](e)' > (k)' \]
\[ e > k \vdash [x' = f(x)]e > k \]

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

\[ \frac{d\llbracket e \rrbracket \varphi(t)}{dt}(z) = [(e)']\varphi(z) > [(k)']\varphi(z) = \frac{d\llbracket k \rrbracket \varphi(t)}{dt}(z) \]
**Lemma (Differential lemma)**

\[ \varphi \models x' = f(x) \land Q \text{ for } r > 0 \Rightarrow \forall 0 \leq z \leq r \left[ (e)' \right] \varphi(z) = \frac{d\left[ e \right] \varphi(t)}{dt}(z) \]

**Differential Invariant**

\[ d \vdash [x' := f(x)](e)' \geq (k)' \]

\[ e > k \vdash [x' = f(x)]e > k \]

\[ d \vdash [x' = f(x)](e)' \geq (k)' \]

\[ e > k \vdash [x' = f(x)]e > k \]

**Proof \((\geq \text{ rate of change from } > \text{ initial value. Mean-value theorem})\).**

\[ \frac{d\left[ e \right] \varphi(t)}{dt}(z) = \left[(e)'\right] \varphi(z) \geq \left[(k)'\right] \varphi(z) = \frac{d\left[ k \right] \varphi(t)}{dt}(z) \]
### Differential Invariant Inequalities

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

\[ \varphi \models x' = f(x) \land Q \text{ for } r > 0 \quad \Rightarrow \quad \forall 0 \leq z \leq r \quad \llbracket (e)' \rrbracket \varphi(z) = \frac{d\llbracket e \rrbracket \varphi(t)}{dt}(z) \]

**Differential Invariant**

\[
\frac{d}{dl} \quad \models [x' := f(x)](e)' \neq (k)'
\]

\[
\frac{e \neq k \models [x' = f(x)]e \neq k}{dI}
\]

\[
\frac{dI}{\models [x' = f(x)](e)' \neq (k)'}
\]

\[
\frac{e \neq k \models [x' = f(x)]e \neq k}{dl}
\]

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

\[
\frac{d\llbracket e \rrbracket \varphi(t)}{dt}(z) = \llbracket (e)' \rrbracket \varphi(z) \neq \llbracket (k)' \rrbracket \varphi(z) = \frac{d\llbracket k \rrbracket \varphi(t)}{dt}(z)
\]
## Differential Invariant Inequalities

**Lemma (Differential lemma)**

\[ \varphi \models x' = f(x) \land Q \text{ for } r > 0 \Rightarrow \forall 0 \leq z \leq r \ (e)' \varphi(z) = \frac{d[e] \varphi(t)}{dt}(z) \]

**Differential Invariant**

\[ \vdash [x' := f(x)](e)' \neq (k)' \]

\[ e \neq k \vdash [x' = f(x)]e \neq k \]

\[ \vdash [x' = f(x)](e)' \neq (k)' \]

\[ e \neq k \vdash [x' = f(x)]e \neq k \]

**Proof**

(\neq \text{ rate of change from } \neq \text{ initial value. Mean-value theorem}).

\[ \frac{d[e] \varphi(t)}{dt}(z) = [(e)'] \varphi(z) \neq [(k)'] \varphi(z) = \frac{d[k] \varphi(t)}{dt}(z) \]
Lemma (Differential lemma) (Differential value vs. Time-derivative)

\[ \varphi \models x' = f(x) \land Q \text{ for } r > 0 \Rightarrow \forall 0 \leq z \leq r \left[ ((e)')\varphi(z) = \frac{d[e]\varphi(t)}{dt}(z) \right] \]

Differential Invariant

\[ \frac{d[e]}{dt}(z) = \left[ (e)'ight]\varphi(z) = \left[ (k)'ight]\varphi(z) = \frac{d[k]}{dt}(z) \]

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

\[ \frac{d[e]}{dt}(z) = \left[ (e)'ight]\varphi(z) \neq \left[ (k)'ight]\varphi(z) = \frac{d[k]}{dt}(z) \]

André Platzer (CMU)
### Differential Invariant Inequalities

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

\[ \varphi \models x' = f(x) \land Q \text{ for } r > 0 \implies \forall 0 \leq z \leq r \quad [(e)'] \varphi(z) = \frac{d[e] \varphi(t)}{dt}(z) \]

**Differential Invariant**

\[
\begin{align*}
\text{dI} & \quad \vdash [x' := f(x)](e)' = (k)' \\
\text{e } \not\equiv k & \quad \vdash [x' = f(x)] e \not\equiv k
\end{align*}
\]

\[
\begin{align*}
\text{DI} & \quad \vdash [x' = f(x)](e)' = (k)'
\end{align*}
\]

\[
\begin{align*}
e \not\equiv k & \quad \vdash [x' = f(x)] e \not\equiv k
\end{align*}
\]

**Proof (\(=\) rate of change from \(\not\equiv\) initial value. Mean-value theorem).**

\[
\frac{d[e] \varphi(t)}{dt}(z) = [(e)'] \varphi(z) = [(k)'] \varphi(z) = \frac{d[k] \varphi(t)}{dt}(z)
\]
Example: Differential Invariant Inequalities

\[
\omega^2 x^2 + y^2 \leq c^2 \models [x' = y, y' = -\omega^2 x - 2d\omega y \land (\omega \geq 0 \land d \geq 0)] \omega^2 x^2 + y^2 \leq c^2
\]
Example: Differential Invariant Inequalities

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

\[ \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y \land (\omega \geq 0 \land d \geq 0)] \omega^2 x^2 + y^2 \leq c^2 \]
Example: Differential Invariant Inequalities

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

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

$$\omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y \land (\omega \geq 0 \land d \geq 0)] \omega^2 x^2 + y^2 \leq c^2$$
Example: Differential Invariant Inequalities

\[
\begin{align*}
\omega \geq & 0 \land d \geq 0 \vdash 2\omega^2 xy + 2y(-\omega^2 x - 2d\omega y) \leq 0 \\
\omega \geq & 0 \land d \geq 0 \vdash [x' := y][y' := -\omega^2 x - 2d\omega y] 2\omega^2 xx' + 2yy' \leq 0 \\
\omega^2 x^2 + y^2 \leq & c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y \& (\omega \geq 0 \land d \geq 0)] \omega^2 x^2 + y^2 \leq c^2
\end{align*}
\]
Example: Differential Invariant Inequalities: Oscillator

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

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

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

Differential Invariant

\[ \text{dl} \quad \frac{P \land Q \vdash [x' = f(x)](P \land Q)}{} \]
Differential Invariant Conjunctions

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

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

\[ \text{dist}(x, v) \land \text{slow}(v) \]
Differential Invariant Conjunctions

**Differential Invariant**

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

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

**Proof (separately).**

\[ \frac{\frac{\vdash [x' = f(x)](P)'}{P \vdash [x' = f(x)]P}}{\mathsf{[]}, \mathsf{WL} \quad \frac{\vdash [x' = f(x)](Q)'}{Q \vdash [x' = f(x)]Q}} \]

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

\[ \mathsf{[]} \quad [\alpha](P \land Q) \leftrightarrow [\alpha]P \land [\alpha]Q \]
Quantum’s Back for a Differential Invariant Proof

No solutions but still a proof.
Simple proof with simple arithmetic.
Independent proofs for independent questions.
Quantum’s Back for a Differential Invariant Proof

\[ [\land] \quad [\alpha](P \land Q) \leftrightarrow [\alpha]P \land [\alpha]Q \]

\[
\begin{align*}
2gx = 2gH - v^2 \quad &\vdash [x'' = -g & x \geq 0]2gx = 2gH - v^2 \\
2gx = 2gH - v^2 \quad &\vdash [x'' = -g & x \geq 0][2gx = 2gH - v^2 \land x \geq 0]
\end{align*}
\]

No solutions but still a proof.
Simple proof with simple arithmetic.
Independent proofs for independent questions.
Quantum’s Back for a Differential Invariant Proof

\[ \frac{x \geq 0 \vdash [x' := v][v' := -g]2gx' = -2vv'}{2gx = 2gH - v^2 \vdash [x'' = -g & x \geq 0]2gx = 2gH - v^2} \vdash [x'' = -g & x \geq 0]x \geq 0 \]

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

André Platzer (CMU)
Quantum’s Back for a Differential Invariant Proof

\[ \begin{align*}
\frac{x \geq 0 \vdash 2gv = -2v(-g)}{[':=] x \geq 0 \vdash [x' := v][v' := -g]2gx' = -2vv'} \\
\frac{2gx = 2gH - v^2 \vdash [x'' = -g \& x \geq 0]2gx = 2gH - v^2}{\vdash [x'' = -g \& x \geq 0]x \geq 0}
\end{align*} \]

No solutions but still a proof.
Simple proof with simple arithmetic.
Independent proofs for independent questions.
Quantum’s Back for a Differential Invariant Proof

\[ x \geq 0 \vdash 2gv = -2v(-g) \]
\[ x \geq 0 \vdash [x' := v][v' := -g]2gx' = -2vv' \]
\[ 2gx = 2gH - v^2 \vdash [x'' = -g \& x \geq 0]2gx = 2gH - v^2 \]
\[ 2gx = 2gH - v^2 \vdash [x'' = -g \& x \geq 0](2gx = 2gH - v^2 \land x \geq 0) \]

No solutions but still a proof.
Simple proof with simple arithmetic.
Independent proofs for independent questions.
Quantum’s Back for a Differential Invariant Proof

\[ x \geq 0 \vdash 2gv = -2v(-g) \]

\[ x \geq 0 \vdash [x' = v][v' = -g] 2gx' = -2vv' \]

\[ 2gx = 2gH - v^2 \vdash [x'' = -g \land x \geq 0] 2gx = 2gH - v^2 \]

\[ dW \quad \vdash [x'' = -g \land x \geq 0] x \geq 0 \]

No solutions but still a proof.
Simple proof with simple arithmetic.
Independent proofs for independent questions.
Quantum’s Back for a Differential Invariant Proof

\[\mathbb{R} \quad \text{['}:=] \quad x \geq 0 \vdash 2gv = -2v(-g)\]
\[\quad \text{['}:=] \quad x \geq 0 \vdash [x' := v][v' := -g] 2gx' = -2vv'\]
\[dW \quad \text{id} \quad x \geq 0 \vdash x \geq 0\]
\[\quad \text{id} \quad x \geq 0 \vdash x \geq 0\]
\[2gx = 2gH - v^2 \vdash [x'' = -g \& x \geq 0] 2gx = 2gH - v^2\]
\[\quad \overset{\text{id}}{\vdash} [x'' = -g \& x \geq 0] x \geq 0\]

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

Differential Invariant

\[
\begin{align*}
\text{dl} & \quad \vdash [x' := f(x)]((P)' \land (Q)') \\
\hline
P \land Q & \vdash [x' = f(x)](P \land Q)
\end{align*}
\]

\[
\begin{align*}
\text{DI} & \quad \vdash [x' = f(x)]((P)' \land (Q)') \\
\hline
P \land Q & \vdash [x' = f(x)](P \land Q)
\end{align*}
\]
Differential Invariant Disjunctions

Differential Invariant

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

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

Proof (separately).

\[\text{dist}(x, v) \lor \text{slow}(v)\]
Differential Invariant Disjunctions

\[ \text{Differential Invariant} \]

\[ \vdash [x' := f(x)]((P)' \lor (Q)') \]

\[ P \lor Q \vdash [x' = f(x)]((P)' \lor (Q)) \]

\[ \vdash [x' = f(x)]((P)' \lor (Q)') \]

\[ P \lor Q \vdash [x' = f(x)](P \lor Q) \]

\[ \text{dist}(x, v) \lor \text{slow}(v) \]
Differential Invariant Disjunctions

Differential Invariant

\[
\begin{align*}
\text{dl} & \quad \vdash [x' := f(x)]((P)' \land (Q)') \\
\text{} & \quad \vdash \frac{P \lor Q}{[x' = f(x)](P \lor Q)}
\end{align*}
\]

\[
\begin{align*}
\text{dl} & \quad \vdash [x' = f(x)]((P)' \land (Q)') \\
\text{} & \quad \vdash \frac{P \lor Q}{[x' = f(x)](P \lor Q)}
\end{align*}
\]
Differential Invariant Disjunctions

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

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

Proof (separately).

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

\[ P \lor Q \vdash [x' = f(x)](P \lor Q) \]
Assuming Differential Invariance

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

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

loop

\[ F \vdash [\alpha]F \]
\[ \frac{F \vdash [\alpha^*]F}{F \vdash [\alpha^*]F} \]
Assuming Differential Invariance

\[ Q \rightarrow [x' := f(x)](F)' \]

\[ F \vdash [x' = f(x) \& Q]F \]

\[ F \land Q \rightarrow [x' := f(x)](F)' \]

\[ F \vdash [x' = f(x) \& Q]F \]

Example (Restrictions)

\[ v^2 - 2v + 1 = 0 \vdash [v' = w, w' = -v]v^2 - 2v + 1 = 0 \]
Assuming Differential Invariance

\[
\neg F \quad \neg F
\]

\[
Q \rightarrow [x' := f(x)](F)'
\]

\[
F \vdash [x' = f(x) & Q]F
\]

\[
F \land Q \rightarrow [x' := f(x)](F)'
\]

\[
F \vdash [x' = f(x) & Q]F
\]

Example (Restrictions)

\[
v^2 - 2v + 1 = 0 \vdash [v' := w][w' := -v]2vw' - 2v' = 0
\]

\[
v^2 - 2v + 1 = 0 \vdash [v' = w, w' = -v]v^2 - 2v + 1 = 0
\]
Assuming Differential Invariance

\[ Q \rightarrow [x' := f(x)](F)' \]
\[ F \vdash [x' = f(x) \& Q]F \]

Example (Restrictions)

\[
\begin{align*}
\nu^2 - 2\nu + 1 &= 0 \\
\vdash 2\nu w - 2w &= 0 \\
\nu^2 - 2\nu + 1 &= 0 \\
\vdash [\nu' := w][w' := -\nu]2\nu\nu' - 2\nu' &= 0 \\
\nu^2 - 2\nu + 1 &= 0 \\
\vdash [\nu' = w, w' = -\nu]\nu^2 - 2\nu + 1 &= 0
\end{align*}
\]
Assuming Differential Invariance

\[ Q \rightarrow [x' := f(x)](F)' \]
\[ \neg F \vdash [x' = f(x) \& Q]F \]

\[ F \wedge Q \rightarrow [x' := f(x)](F)' \]
\[ F \vdash [x' = f(x) \& Q]F \]

Example (Restrictions)

\[ v^2 - 2v + 1 = 0 \vdash 2vw - 2w = 0 \]
\[ v^2 - 2v + 1 = 0 \vdash [v' := w][w' := -v]2vv' - 2v' = 0 \]
\[ v^2 - 2v + 1 = 0 \vdash [v' = w, w' = -v]v^2 - 2v + 1 = 0 \]
Assuming Differential Invariance

\[ Q \rightarrow [x' := f(x)](F)' \]

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

\[ F \land Q \rightarrow [x' := f(x)](F)' \]

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

Example (Restrictions are unsound!)

(unsound)

\[ v^2 - 2v + 1 = 0 \vdash 2vw - 2w = 0 \]

\[ v^2 - 2v + 1 = 0 \vdash [v' := w][w' := -v]2v^2 - 2v' = 0 \]

\[ v^2 - 2v + 1 = 0 \vdash [v' = w, w' = -v]v^2 - 2v + 1 = 0 \]
Outline

1 Learning Objectives

2 Differential Invariants
   ▪ Recap: Ingredients for Differential Equation Proofs
   ▪ Soundness: Derivations Lemma
   ▪ Differential Weakening
   ▪ Differential Invariant Equations
   ▪ Example Proof: Damped Oscillator
   ▪ Conjunctive Differential Invariants
   ▪ Disjunctive Differential Invariants
   ▪ Assuming Invariants

3 Differential Cuts

4 Soundness

5 Summary
Differential Cuts

Differential Cut

\[ F \vdash [x' = f(x)]F \]

Differential Cut

Proof (Soundness).

Let \( \varphi \models x' = f(x) \land Q \) starting in \( \omega \in \llbracket F \rrbracket \).

Thus, \( \varphi (\omega) \in \llbracket F \rrbracket \) by second premise.

André Platzer (CMU)
Differential Cuts

Differential Cut

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

Differential Cut

Proof (Soundness). Let \( \phi \models [x' = f(x)] \land Q \) starting in \( \omega \in \llbracket F \rrbracket \).

Thus, \( \phi \models x' = f(x) \land Q \land C \).

Thus, \( \phi \models [x' = f(x)]F \) by second premise.
Proof (Soundness).
Let \( \varphi \models x' = f(x) \land Q \) starting in \( \omega \in \{ [F] \} \).
Thus, \( \varphi | = x' = f(x) \land Q \land C \).
Thus, \( \varphi(r) \in \{ [F] \} \) by second premise.
Differential Cuts

Differential Cut

\[ F \vdash [x' = f(x) \& Q] F \quad F \vdash [x' = f(x) \& Q \land C] F \]

\[ F \vdash [x' = f(x) \& Q] F \]
Proof (Soundness).

Let $\phi \models x' = f(x) \land Q$ starting in $\omega \in \mathbb{F}$. Thus, $\phi \models x' = f(x) \land Q \land C$.

Thus, $\phi(r) \in \mathbb{F}$ by second premise.
Differential Cuts

Differential Cut

\[
\begin{align*}
F \vdash [x' = f(x) & Q] & \quad C & \quad F \vdash [x' = f(x) & Q \land C] & \quad F \\
\therefore & \quad F \vdash [x' = f(x) & Q] & \quad F
\end{align*}
\]

Proof (Soundness).

Let \( \phi \models x' = f(x) \land Q \) starting in \( \omega \in \bigcup [\bigcup x' = f(x) \land Q \} \]

Thus, \( \phi \models x' = f(x) \land Q \land C \).

Thus, \( \phi(r) \notin \bigcup [\bigcup F \} \)

André Platzer (CMU)
Proof (Soundness).

Let \( \varphi \models \exists x'. x' = f(x) \land Q \) starting in \( \omega \in \exists x. [F] \).

Thus, \( \varphi \models \exists x'. x' = f(x) \land Q \land C \).

Thus, \( \varphi(\tau) \models \exists x. [F] \) by second premise.
Differential Cuts

Differential Cut

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

Proof (Soundness).

Let \( \varphi \models x' = f(x) \& Q \) starting in \( \omega \in \llbracket F \rrbracket \).

Thus, \( \varphi \models x' = f(x) \& Q \land C \).

Thus, \( \varphi (r) \in \llbracket F \rrbracket \) by second premise.
Proof (Soundness).

Let $\varphi \models x' = f(x) \land Q$ starting in $\omega \in \llbracket F \rrbracket$.

$\omega \in \llbracket [x' = f(x) \land Q] C \rrbracket$ by left premise.

Thus, $\varphi \models x' = f(x) \land Q \land C$.

Thus, $\varphi(r) \in \llbracket F \rrbracket$ by second premise.
\[ DC \quad x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2] x^3 \geq -1 \]
DC \quad x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2] x^3 \geq -1

dl \quad y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2] y^5 \geq 0
Ex: Differential Cuts

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

\[ [':=] \quad \vdash [x' := (x - 2)^4 + y^5][y' := y^2]5y^4y' \geq 0 \]

\[ \text{dl} \quad y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]y^5 \geq 0 \]
Ex: Differential Cuts

\[
\begin{align*}
\text{DC} & \quad x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]x^3 \geq -1 \\
\text{R} & \quad \vdash 5y^4y^2 \geq 0 \\
[':=] & \quad \vdash [x' := (x - 2)^4 + y^5][y' := y^2]5y^4y' \geq 0 \\
dl & \quad y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]y^5 \geq 0
\end{align*}
\]
Differential Cuts

\[ x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]x^3 \geq -1 \]

\[ \vdash 5y^4y'^2 \geq 0 \]

\[ \vdash [x' := (x - 2)^4 + y^5][y' := y^2]5y^4y' \geq 0 \]

\[ y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]y^5 \geq 0 \]
Ex: Differential Cuts

\( x^3 \geq -1 \vdash [x' = (x - 2)^4 + y^5, y' = y^2 \& y^5 \geq 0] x^3 \geq -1 \)

\( x^3 \geq -1 \wedge y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2] x^3 \geq -1 \)

\[ \star \]

\( \mathbb{R} \)

\( \vdash 5y^4 y^2 \geq 0 \)

\( [':=] \)

\( \vdash [x' := (x - 2)^4 + y^5][y' := y^2] 5y^4 y' \geq 0 \)

\( dl \)

\( y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2] y^5 \geq 0 \)
\[
\begin{align*}
\left[ \vdash \right] & \quad y^5 \geq 0 \vdash [x' := (x - 2)^4 + y^5][y' := y^2]2x^2x' \geq 0 \\
\text{dl} & \quad x^3 \geq -1 \vdash [x' = (x - 2)^4 + y^5, y' = y^2 \land y^5 \geq 0]x^3 \geq -1 \\
\text{DC} & \quad x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]x^3 \geq -1
\end{align*}
\]

\[\star\]

\[
\begin{align*}
\mathbb{R} & \quad \vdash 5y^4y^2 \geq 0 \\
\left[ \vdash \right] & \quad \vdash [x' := (x - 2)^4 + y^5][y' := y^2]5y^4y' \geq 0 \\
\text{dl} & \quad y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]y^5 \geq 0
\end{align*}
\]
\( \mathbb{R} \)

\[ y^5 \geq 0 \vdash 2x^2((x - 2)^4 + y^5) \geq 0 \]

\[ [\vdash] \]

\[ y^5 \geq 0 \vdash [x' := (x - 2)^4 + y^5][y' := y^2]2x^2x' \geq 0 \]

\[ \text{dl} \]

\[ x^3 \geq -1 \vdash [x' = (x - 2)^4 + y^5, y' = y^2 \& y^5 \geq 0]x^3 \geq -1 \]

\[ \text{DC} \]

\[ x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]x^3 \geq -1 \]

\[ * \]

\[ \mathbb{R} \]

\[ \vdash 5y^4y^2 \geq 0 \]

\[ [\vdash] \]

\[ \vdash [x' := (x - 2)^4 + y^5][y' := y^2]5y^4y' \geq 0 \]

\[ \text{dl} \]

\[ y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]y^5 \geq 0 \]
Ex: Differential Cuts

\[
\begin{align*}
\mathbb{R} & \quad y^5 \geq 0 \vdash 2x^2((x - 2)^4 + y^5) \geq 0 \\
[':=] & \quad y^5 \geq 0 \vdash [x' := (x - 2)^4 + y^5][y' := y^2]2x^2x' \geq 0 \\
dl & \quad x^3 \geq -1 \vdash [x' = (x - 2)^4 + y^5, y' = y^2 & y^5 \geq 0]x^3 \geq -1 \triangleright \\
DC & \quad x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]x^3 \geq -1 \\
\end{align*}
\]

\[
\begin{align*}
\mathbb{R} & \quad \vdash 5y^4y^2 \geq 0 \\
[':=] & \quad \vdash [x' := (x - 2)^4 + y^5][y' := y^2]5y^4y' \geq 0 \\
dl & \quad y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]y^5 \geq 0
\end{align*}
\]
Outline

1. Learning Objectives
2. Differential Invariants
   - Recap: Ingredients for Differential Equation Proofs
   - Soundness: Derivations Lemma
   - Differential Weakening
   - Differential Invariant Equations
   - Example Proof: Damped Oscillator
   - Conjunctive Differential Invariants
   - Disjunctive Differential Invariants
   - Assuming Invariants
3. Differential Cuts
4. Soundness
5. Summary
Soundness Proof: Differential Invariants

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

\[ \varphi \models x' = f(x) \land Q \text{ for } r > 0 \Rightarrow \forall 0 \leq z \leq r \ [(e)']\varphi(z) = \frac{\partial [e]\varphi(t)}{dt}(z) \]

Differential Invariant

\[ Dl \quad \vdash [x' = f(x) \land Q](e)' \geq 0 \]

\[ e \geq 0 \vdash [x' = f(x) \land Q]e \geq 0 \]

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

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

\[ \frac{dh(t)}{dt}(z) = \frac{d[e]\varphi(t)}{dt}(z) = [(e)']\varphi(z) \geq 0 \text{ by lemma + premise for all } z. \]

\[ h(r) - h(0) = (r - 0) \frac{dh(t)}{dt}(\xi) \geq 0 \text{ by mean-value theorem for some } \xi. \]
Outline

1 Learning Objectives

2 Differential Invariants
   - Recap: Ingredients for Differential Equation Proofs
   - Soundness: Derivations Lemma
   - Differential Weakening
   - Differential Invariant Equations
   - Example Proof: Damped Oscillator
   - Conjunctive Differential Invariants
   - Disjunctive Differential Invariants
   - Assuming Invariants

3 Differential Cuts

4 Soundness

5 Summary
Differential Invariants for Differential Equations

**Differential Weakening**

\[ Q \vdash F \]

\[ P \vdash [x' = f(x) & Q]F \]

**Differential Invariant**

\[ Q \vdash [x' := f(x)](F)' \]

\[ F \vdash [x' = f(x) & Q]F \]

**Differential Cut**

\[ F \vdash [x' = f(x) & Q]C \]

\[ F \vdash [x' = f(x) & Q \land C]F \]

\[ F \vdash [x' = f(x) & Q]F \]
André Platzer.
Foundations of cyber-physical systems.

André Platzer.
A uniform substitution calculus for differential dynamic logic.
In Amy Felty and Aart Middeldorp, editors, CADE, volume 9195 of
doi:10.1007/978-3-319-21401-6_32.

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

André Platzer.
Logics of dynamical systems.
Andre Platzer.
Differential-algebraic dynamic logic for differential-algebraic programs.

Andre Platzer.
The structure of differential invariants and differential cut elimination.

Andre Platzer.
A differential operator approach to equational differential invariants.
doi:10.1007/978-3-642-32347-8_3.