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

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

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

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

### Axioms

\begin{align*}
(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 \mathcal{V}
\end{align*}

### ODE

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

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

\[ \ldots \]
Differential Substitution Lemmas

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

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

$$\varphi(z)\llbracket(e)'\rrbracket = \frac{d\varphi(t)\llbracket e \rrbracket}{dt}(z)$$

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

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

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

$$\begin{align*}
(e + k)' &= (e)' + (k)' \\
(e \cdot k)' &= (e)' \cdot k + e \cdot (k)' \\
(c())' &= 0 \\
(x)' &= x'
\end{align*}$$

for constants/numbers $c()$

for variables $x \in \mathcal{V}$
Lemma (Differential lemma) (Differential value vs. Time-derivative)

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

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

Lemma (Differential assignment) (Effect on Differentials)

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

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

<table>
<thead>
<tr>
<th>Lemma (Derivations)</th>
<th>(Equations of Differentials)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$+'$</td>
<td>$(e + k)' = (e)' + (k)'$</td>
</tr>
<tr>
<td>$\cdot'$</td>
<td>$(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$</td>
</tr>
<tr>
<td>$c'$</td>
<td>$(c())' = 0$</td>
</tr>
<tr>
<td>$x'$</td>
<td>$(x)' = x'$</td>
</tr>
</tbody>
</table>

Proof.

$\omega \left[ \left( \frac{e}{2} + \frac{k}{2} \right) \right] = \sum_x \omega(x)' \frac{\partial}{\partial x} \omega(e + k)$

$= \sum_x \omega(x)' \frac{\partial\left( \frac{e}{2} \right)}{\partial x} \frac{\partial \omega}{\partial x} + \sum_x \omega(x)' \frac{\partial\left( \frac{k}{2} \right)}{\partial x} \frac{\partial \omega}{\partial x}$

$= \sum_x \omega(x)' \frac{\partial\left( \frac{e}{2} \right)}{\partial x} \frac{\partial \omega}{\partial x} + \sum_x \omega(x)' \frac{\partial\left( \frac{k}{2} \right)}{\partial x} \frac{\partial \omega}{\partial x}$

$= \omega \left[ \left( \frac{e}{2} \right)' \right] + \omega \left[ \left( \frac{k}{2} \right)' \right] = \omega \left[ \left( \frac{e}{2} \right)' + \left( \frac{k}{2} \right)' \right]$
Soundness: Proof of Derivations Lemma

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

Proof.

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

Lemma (Derivations) (Equations of Differentials)

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

Proof.

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

Lemma (Derivations) (Equations of Differentials)

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

Proof.

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

Lemma (Derivations) (Equations of Differentials)

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

Proof.

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

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

Proof.

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

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

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

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

### Equations of Differentials

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

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

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

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

Lemma (Derivations) (Equations of Differentials)

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

Proof.

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

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

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

\[
= \omega[(e)'] + \omega[(k)'] = \omega[(e)' + (k)']
\]
Lemma (Derivations) (Equations of Differentials)

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

Proof.

\[
\omega[(e + k)'] = \sum_x \omega(x') \frac{\partial[e + k]}{\partial x}(\omega) = \sum_x \omega(x') \frac{\partial(e) + \partial[k]}{\partial x}(\omega) \\
= \sum_x \omega(x') \left( \frac{\partial[e]}{\partial x}(\omega) + \frac{\partial[k]}{\partial x}(\omega) \right) \\
= \sum_x \omega(x') \frac{\partial[e]}{\partial x}(\omega) + \sum_x \omega(x') \frac{\partial[k]}{\partial x}(\omega) \\
= \omega[(e)'] + \omega[(k)'] = \omega[(e)' + (k)']
\]
Lemma (Differential lemma)  (Differential value vs. Time-derivative)

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

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

Lemma (Differential assignment)  (Effect on Differentials)

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

Lemma (Derivations)  (Equations of Differentials)

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

\[ x' = f(x) \land Q \]

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

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

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

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

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

Differential equations cannot leave their domains.
Differential Weakening

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

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

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

Example (Bouncing ball)

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

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

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

**Example (Bouncing ball)**

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

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

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

**Example (Bouncing ball)**

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

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

\[ \frac{\Gamma \vdash [x' = f(x) & Q]P, \Delta}{dW} \]

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

Example (Bouncing ball)

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

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

\[
\text{dW} \quad \frac{Q \vdash P}{\Gamma \vdash [x' = f(x) \& Q] P, \Delta}
\]

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

Example (Bouncing ball)

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

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

**Differential Invariant**

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

\[
\text{DI } ([x' = f(x)]e = 0 \iff e = 0) \iff [x' = f(x)](e)' = 0
\]

\[
\text{DE } [x' = f(x) \& Q]P \iff [x' = f(x) \& Q][x' := f(x)]P
\]

\[
\text{DW } [x' = f(x) \& Q]P \iff [x' = f(x) \& Q](Q \to P)
\]
**Differential Invariant Terms for Differential Equations**

**Differential Invariant**

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

\[
\text{DI} \quad ([x' = f(x) & Q] e = 0 \leftrightarrow [?Q]e = 0) \leftarrow [x' = f(x) & Q] (e)' = 0
\]

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

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

**Differential Invariant**

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

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

**DI** \( ([x' = f(x) \& Q]e = 0 \iff [?Q]e = 0) \leftarrow [x' = f(x) \& Q](e)' = 0 \)

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

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

Proof (dl is a derived rule).
Differential Invariant Terms for Differential Equations

Differential Invariant

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

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

DI  \(([x' = f(x) & Q] e = 0 \leftrightarrow [?Q] e = 0) \leftarrow [x' = f(x) & Q] (e)' = 0\)

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

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

Proof (dl is a derived rule).

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

DI  \(e = 0 \vdash [x' = f(x) & Q]e = 0\)
Differential Invariant Terms for Differential Equations

Differential Invariant

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

\[
\begin{align*}
\text{DI} \quad ([x' = f(x) \& Q] e = 0 \iff [\ ?Q] e = 0) & \iff [x' = f(x) \& Q] (e)' = 0 \\
\text{DE} \quad [x' = f(x) \& Q] P \iff [x' = f(x) \& Q][x' := f(x)] P \\
\text{DW} \quad [x' = f(x) \& Q] P \iff [x' = f(x) \& Q](Q \rightarrow P)
\end{align*}
\]

Proof (dl is a derived rule).

\[
\begin{align*}
\text{DW} \quad & \vdash [x' = f(x) \& Q][x' := f(x)](e)' = 0 \\
\text{DE} \quad & \vdash [x' = f(x) \& Q](e)' = 0 \\
\text{DI} \quad & e = 0 \vdash [x' = f(x) \& Q]e = 0
\end{align*}
\]
Differential Invariant Terms for Differential Equations

Differential Invariant

dl

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

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

DI \ ([x' = f(x) \& Q] e = 0 \iff [?Q]e = 0) \iff [x' = f(x) \& Q](e)' = 0

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

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

Proof (dl is a derived rule).

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

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

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

\[ DI \quad e = 0 \vdash [x' = f(x) \& Q]e = 0 \]
Differential Invariant Terms for Differential Equations

Differential Invariant

\[ \frac{Q \vdash [x' := f(x)](e)' = 0}{\exists e \quad [x' = f(x) \& Q]e = 0} \]

\[ \frac{Q \vdash [x' := f(x)](e)' = 0}{\exists e \quad [x' = f(x) \& Q]e = 0} \]

\[ \exists e \quad [x' = f(x) \& Q]e = 0 \quad \leftrightarrow \quad [x' = f(x) \& Q](e)' = 0 \]

\[ \exists e \quad [x' = f(x) \& Q]e = 0 \quad \leftrightarrow \quad [x' = f(x) \& Q][x' := f(x)]e = 0 \]

\[ \exists e \quad [x' = f(x) \& Q]e = 0 \quad \leftrightarrow \quad [x' = f(x) \& Q](Q \rightarrow P) \]

Proof (dl is a derived rule).

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

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

\[ \frac{\vdash [x' = f(x) \& Q](Q \rightarrow [x' := f(x)](e)' = 0)}{[\alpha]P} \]

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

\[ [\alpha]P \]

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

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

\[ \exists e \quad [x' = f(x) \& Q]e = 0 \quad \leftrightarrow \quad [x' = f(x) \& Q](e)' = 0 \]

\[ \exists e \quad [x' = f(x) \& Q]e = 0 \quad \leftrightarrow \quad [x' = f(x) \& Q][x' := f(x)]e = 0 \]

\[ \exists e \quad [x' = f(x) \& Q]e = 0 \quad \leftrightarrow \quad [x' = f(x) \& Q](Q \rightarrow P) \]
**Lemma (Differential lemma)**  

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

---

**Differential Invariant**

\[ dI \frac{dl}{e = k} \quad [x' = f(x)]e = k \]
### Lemma (Differential lemma)

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

### Differential Invariant

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

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

\[
\begin{align*}
\text{dl} & \quad \frac{e = k \vdash [x' = f(x)] e = k}{[x' = f(x)] e = k}
\end{align*}
\]
Differential Invariant Equations

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

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

Differential Invariant

\[ \frac{d}{dt} \models [\dot{x} := f(x)](e)' = (k)' \]

\[ e = k \frac{d}{dt} \models [\dot{x} = f(x)]e = k \]

DI \quad ([\dot{x} = f(x)] e = k \leftrightarrow e = k) \leftarrow [\dot{x} = f(x)](e)' = (k)'

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

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

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

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

**Differential Invariant**

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

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

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

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

#### André Platzer (CMU)

**FCPS / 11: Differential Equations & Proofs**
### Differential Invariant Inequalities

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

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

**Differential Invariant**

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

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

**DI**  
\[
([x' = f(x)] e \leq k \iff e \leq k) \iff [x' = f(x)](e)' \leq (k)'
\]

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

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

<table>
<thead>
<tr>
<th>Lemma (Differential lemma)</th>
<th>Differential value vs. Time-derivative</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\varphi \models x' = f(x) \land Q$ for $r &gt; 0 \Rightarrow \forall 0 \leq z \leq r \quad \varphi(z)[(e)'] = \frac{d\varphi(t)[e]}{dt}(z)$</td>
<td></td>
</tr>
</tbody>
</table>

**Differential Invariant**

\[
\text{dl} \quad [x' := f(x)](e)' > (k)'
\]

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

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

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

Lemma (Differential lemma) (Differential value vs. Time-derivative)
\[ \varphi \models x' = f(x) \land Q \text{ for } r > 0 \Rightarrow \forall 0 \leq z \leq r \varphi(z)[(e)'] = \frac{d\varphi(t)[e]}{dt}(z) \]

Differential Invariant
\[ \models [x' := f(x)](e)' \geq (k)' \]
\[ e > k \models [x' = f(x)]e > k \]

DI \ ([x' = f(x)] e > k \iff e > k) \leftarrow [x' = f(x)] (e)' \geq (k)'

Proof (\geq \text{ rate of change from } > \text{ initial value. Mean-value theorem}).
\[ \frac{d\varphi(t)[e]}{dt}(z) = \varphi(z)[(e)'] \geq \varphi(z)[(k)'] = \frac{d\varphi(t)[k]}{dt}(z) \]
## Differential Invariant Inequalities

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

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

**Differential Invariant**

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

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

**DI** \( ([x' = f(x)]e \neq k \leftrightarrow e \neq k) \leftarrow [x' = f(x)](e)' \neq (k)' \)

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

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

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

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

**Differential Invariant**

\[
\begin{align*}
\vdash [x' := f(x)](e)' \neq (k)' \\
e \neq k \vdash [x' = f(x)]e \neq k
\end{align*}
\]

**DI**

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

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

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

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

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

**Differential Invariant**

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

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

**DI** \([x' = f(x)] e \neq k \leftrightarrow \neq k) \leftarrow \left[ x' = f(x) \right] (e)' \neq (k)'

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

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

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

Differential Invariant

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

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

Differential Invariant

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

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

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

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

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

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

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

damped oscillator
Example: Differential Invariant Inequalities: Oscillator

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

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

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

damped oscillator
Example: Differential Invariant Inequalities: Oscillator

**

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

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

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

damped oscillator
Example: Differential Invariant Inequalities: Oscillator

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

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

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

damped oscillator
Differential Invariant Conjunctions

Differential Invariant

\[ A \land B \vdash [x' = f(x)](A \land B) \]
Differential Invariant Conjunctions

\[
\text{Differential Invariant}
\]

\[
\frac{\vdash [x' := f(x)]((A)' \land (B)')}{A \land B \vdash [x' = f(x)](A \land B)}
\]

\[
\text{DI} \quad ([x' = f(x)](A \land B) \iff (A \land B)) \iff [x' = f(x)]((A)' \land (B)')
\]

Proof (separately).

\[
\vdash [x' := f(x)]((A)' \land (B)')
\]

\[
A \land B \vdash [x' = f(x)](A \land B)
\]

\[
\vdash [x' = f(x)]((A)' \land (B)')
\]

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

Andrè Platzer (CMU)

FCPS / 11: Differential Equations & Proofs
Differential Invariant Conjunctions

\[ \text{Differential Invariant} \]
\[
\vdash [x' := f(x)]((A)' \land (B)') \quad \frac{A \land B \vdash [x' = f(x)](A \land B)}{\vdash [x' := f(x)]((A)' \land (B)')} \]

\[ \text{DI} \quad ([x' = f(x)](A \land B) \leftrightarrow (A \land B)) \leftarrow [x' = f(x)]((A)' \land (B)') \]

Proof (separately).

\[ \vdash [x' = f(x)](A)' \quad \vdash [x' = f(x)](B)' \]
\[
\frac{\text{DI}}{A \vdash [x' = f(x)]A} \quad \frac{\text{DI}}{B \vdash [x' = f(x)]B} \quad \frac{\text{DIL}}{A \land B \vdash [x' = f(x)](A \land B)}\]

\[ \text{DIL} \quad \vdash [x' = f(x)](A)' \land [x' = f(x)](B)' \]

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

\[ \text{[]} \land ([\alpha](P \land Q) \leftrightarrow [\alpha]P \land [\alpha]Q) \]

\[ \text{Proof (separately).} \]

\[ \vdash [x' = f(x)](A)' \quad \vdash [x' = f(x)](B)' \]
\[
\frac{\text{DI}}{A \vdash [x' = f(x)]A} \quad \frac{\text{DI}}{B \vdash [x' = f(x)]B} \quad \frac{\text{DIL}}{A \land B \vdash [x' = f(x)](A \land B)}\]

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

\[\mathcal{L} \land \left[\alpha\right](P \land Q) \iff \left[\alpha\right]P \land \left[\alpha\right]Q\]

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

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

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

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

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

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

\[ x \geq 0 \vdash 2g v = -2v(-g) \]
\[
\begin{align*}
\text{[\( \prime \):=]} & \quad x \geq 0 \vdash [x' := v][v' := -g] 2gx' = -2vv' \\
\text{\( dl \)} & \quad 2gx = 2gH - v^2 \vdash [x'' = -g \land x \geq 0] 2gx = 2gH - v^2 \\
\text{\( []^\land \)} & \quad \vdash [x'' = -g \land x \geq 0] x \geq 0
\end{align*}
\]

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

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

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

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

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

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

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

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

Differential Invariant

\[ \text{dl} \quad \vdash [x' := f(x)]((A') \land (B')) \]
\[ A \land B \vdash [x' = f(x)](A \land B) \]

Differential Invariant

\[ \text{DI} \quad ([x' = f(x)](A \land B) \leftrightarrow (A \land B)) \leftrightarrow [x' = f(x)]((A') \land (B')) \]
Differential Invariant Disjunctions

Differential Invariant

\[ \vdash [x' := f(x)]((A)' \lor (B)') \]

\[ A \lor B \vdash [x' = f(x)](A \lor B) \]

Differential Invariant (DI)

\[ ([x' = f(x)](A \lor B) \leftrightarrow (A \lor B)) \leftrightarrow [x' = f(x)]((A)' \lor (B)') \]

Proof (separately).

André Platzer (CMU)
Differential Invariant Disjunctions

\[
\begin{align*}
\text{Differential Invariant} & \\
\text{dl} & \quad \vdash [x' := f(x)]((A)' \lor (B)') \\
& \quad A \lor B \vdash [x' := f(x)](A' \lor B') \\
\text{DI} & \quad ([x' = f(x)](A \lor B) \leftrightarrow (A \lor B)) \quad [x' = f(x)]((A)' \lor (B)')
\end{align*}
\]
Differential Invariant Disjunctions

**Differential Invariant**

\[ \vdash [x' := f(x)]((A)' \land (B)') \]

\[ A \lor B \vdash [x' = f(x)](A \lor B) \]

**DI**

\[ ([x' = f(x)](A \lor B) \leftrightarrow (A \lor B)) \leftarrow [x' = f(x)]((A)' \land (B)') \]

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

\[ \frac{dI \vdash [x' := f(x)]((A)' \land (B)')} {A \lor B \vdash [x' = f(x)](A \lor B)} \]

\[ ( [x' = f(x)](A \lor B) \iff (A \lor B) ) \leftarrow [x' = f(x)]((A)' \land (B)') \]

**Proof (separately).**

\[
\begin{array}{ll}
\quad & \vdash [x' = f(x)](A)' \\
MR & A \vdash A \lor B \\
DI & A \vdash [x' = f(x)]A \quad (A' \land (B)')'
\end{array}
\]

\[
\begin{array}{ll}
\quad & \vdash [x' = f(x)](B)' \\
MR & B \vdash A \lor B \\
DI & B \vdash [x' = f(x)]B \quad (A' \land (B)')'
\end{array}
\]

\[
\begin{array}{l}
\therefore A \lor B \vdash [x' = f(x)](A \lor B)
\end{array}
\]

\[
\begin{array}{l}
\therefore A \lor B \vdash [x' = f(x)](A \lor B)
\end{array}
\]
Differential Invariant Disjunctions

**Differential Invariant**

\[ \vdash [x' := f(x)]((A)' \land (B)') \]

\[ A \lor B \vdash [x' = f(x)](A \lor B) \]

**DI** \(([x' = f(x)](A \lor B) \leftrightarrow (A \lor B)) \leftarrow [x' = f(x)]((A)' \land (B)')\)

**Proof (separately).**

\[ A \vdash A \lor B \quad \text{DI} \quad A \vdash [x' = f(x)]A \]

**MR**

\[ A \vdash [x' = f(x)](A \lor B) \]

\[ B \vdash A \lor B \quad \text{DI} \quad B \vdash [x' = f(x)]B \]

**MR**

\[ B \vdash [x' = f(x)](A \lor B) \]

\[ A \lor B \vdash [x' = f(x)](A \lor B) \]

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

André Platzer (CMU)
Assuming Differential Invariance

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

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

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

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

\[
\text{loop}
\]

\[
F \vdash [\alpha]F
\]

\[
F \vdash [\alpha^*]F
\]
Assuming Differential Invariance

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

Example (Restrictions)

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

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

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

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

Example (Restrictions)

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

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

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

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

Example (Restrictions)

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

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

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

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

Example (Restrictions are unsound!)

\[
\begin{align*}
\nu^2 - 2\nu + 1 &= 0 \vdash 2\nu w - 2w = 0 \\
\nu^2 - 2\nu + 1 &= 0 \vdash [\nu' := w][w' := -\nu] 2\nu\nu' - 2\nu' = 0 \\
\nu^2 - 2\nu + 1 &= 0 \vdash [\nu' = w, w' = -\nu] \nu^2 - 2\nu + 1 = 0
\end{align*}
\]
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
Proof (Soundness).

Let $\varphi \models x' = f(x)$ and $Q$ starting in $\omega \in \left[ \left[ F \right] \right]$.

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

Thus, $\varphi(r) \in \left[ \left[ F \right] \right]$ by second premise.
Differential Cuts

Differential Cut

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

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

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, \( \phi(r) \models \llbracket F \rrbracket \) by second premise.
Differential Cuts

Differential Cut

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

Proof (Soundness).
Let \( \phi \models_* x' = f(x) \& Q \) starting in \( \omega \in [\llbracket F \rrbracket] \).
Thus, \( \phi \models_* x' = f(x) \& Q \& C \).
Thus, \( \phi(x) \models_r [\llbracket F \rrbracket] \) by second premise.
Differential Cuts

Differential Cut

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

Proof (Soundness).

Let \( \phi \models x' = f(x) \& Q \) starting in \( \omega \in \square [F] \).

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

Thus, \( \phi(r) \models [F] \) by second premise.
Proof (Soundness).
Let $\varphi \models [x' = f(x) \land Q]C F \models [x' = f(x) \land Q \land C]F$

Thus, $\varphi \models [x' = f(x) \land Q]F$

Thus, $\varphi(r) \models [x' = f(x) \land Q]F$ by second premise.
Differential Cuts

Differential Cut

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

André Platzer (CMU)
Differential Cuts

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

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

Proof (Soundness).

Let \( \varphi \mid \omega = x' = f(x) \land Q \) starting in \( \omega \in \mathbb{F} \).

Thus, \( \varphi \mid \omega = x' = f(x) \land Q \land C \).

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

Differential Cut

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

**Differential Cut**

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

**Proof (Soundness).**

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

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

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

Thus, \( \varphi(r) \in \llbracket F \rrbracket \) by second premise.
\[
\frac{d\omega}{dC} \leq 0 \quad \text{and} \quad \frac{d}{dC} \geq 0 \quad \vdash \quad 2\omega^2 x + 2y (\omega^2 x - 2d\omega y) \leq 0
\]

\[
\frac{dI}{dC} \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2
\]
Differential Cut Example: Increasingly Damped Oscillator

\[ \frac{dC}{dt} \leq \omega^2 x^2 + y^2 \leq c^2 \implies [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \& \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2 \]

Increasingly damped oscillator
Differential Cut Example: Increasingly Damped Oscillator

\[
\begin{align*}
\text{dl} & \quad \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y, d' = 7 \land \omega \geq 0 \land d \geq 0] \quad \omega^2 x^2 + y^2 \leq c^2 \\
\text{dc} & \quad \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y, d' = 7 \land \omega \geq 0] \quad \omega^2 x^2 + y^2 \leq c^2
\end{align*}
\]

increasingly damped oscillator
Differential Cut Example: Increasingly Damped Oscillator

\[ \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 & \omega \geq 0 \land d \geq 0] \omega^2 x^2 + y^2 \leq c^2 \]

\[ \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 & \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2 \]

\[ d \geq 0 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 & \omega \geq 0] d \geq 0 \]

increasingly damped oscillator
Differential Cut Example: Increasingly Damped Oscillator

\[ \omega^2 x'^2 + y'^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \& \omega \geq 0 \& d \geq 0] \omega^2 x'^2 + y'^2 \leq c^2 \]

\[ \omega^2 x'^2 + y'^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \& \omega \geq 0] \omega^2 x'^2 + y'^2 \leq c^2 \]

\[ [\vdash] \omega \geq 0 \vdash [d' := 7] d' \geq 0 \]

\[ \omega^2 x'^2 + y'^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \& \omega \geq 0] d \geq 0 \]

increasingly damped oscillator
Differential Cut Example: Increasingly Damped Oscillator

\[
\begin{align*}
\text{dl} & \quad \omega^2x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2x - 2d\omega y, d' = 7 & \omega \geq 0 \land d \geq 0] \omega^2x^2 + y^2 \leq c^2 \\
\text{dC} & \quad \omega^2x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2x - 2d\omega y, d' = 7 & \omega \geq 0] \omega^2x^2 + y^2 \leq c^2
\end{align*}
\]

\[
\begin{align*}
\mathbb{R} & \quad \omega \geq 0 \vdash 7 \geq 0 \\
[':=] & \quad \omega \geq 0 \vdash [d' := 7] d' \geq 0 \\
\text{dl} & \quad d \geq 0 \vdash [x' = y, y' = -\omega^2x - 2d\omega y, d' = 7 & \omega \geq 0] d \geq 0
\end{align*}
\]

increasingly damped oscillator
Differential Cut Example: Increasingly Damped Oscillator

\[ \begin{align*}
\dC \quad & \quad \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, \; d' = 7 & \land \omega \geq 0 \land d \geq 0] \; \omega^2 x^2 + y^2 \leq c^2 \\
\dI \quad & \quad \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, \; d' = 7 & \land \omega \geq 0] \; \omega^2 x^2 + y^2 \leq c^2
\end{align*} \]

\[ \begin{align*}
\mathbb{R} \quad & \quad \omega \geq 0 \vdash \; 7 \geq 0 \\
[\vdash] \quad & \quad \omega \geq 0 \vdash [d' := 7] \; d' \geq 0 \\
\dI \quad & \quad d \geq 0 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, \; d' = 7 & \land \omega \geq 0] \; d' \geq 0
\end{align*} \]

increasingly damped oscillator
Differential Cut Example: Increasingly Damped Oscillator

\[
\begin{align*}
[\(':='] & \quad \omega \geq 0 \land d \geq 0 \vdash [x' := y][y' := -\omega^2 x - 2d\omega y] \quad 2\omega^2 xx' + 2yy' \leq 0 \\
\text{dl} & \quad \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0 \land d \geq 0] \quad \omega^2 x^2 + y^2 \leq c^2 \\
\text{dC} & \quad \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0] \quad \omega^2 x^2 + y^2 \leq c^2 \\
\mathbb{R} & \quad \omega \geq 0 \vdash 7 \geq 0 \\
[\(':='] & \quad \omega \geq 0 \vdash [d' := 7] \quad d' \geq 0 \\
\text{dl} & \quad d \geq 0 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0] \quad d \geq 0
\end{align*}
\]

increasingly damped oscillator
Differential Cut Example: Increasingly Damped Oscillator

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

\[ [\vdash \omega \geq 0 \land d \geq 0 \vdash x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0] \quad 2\omega^2 xx' + 2yy' \leq 0 \]

\[ \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0] \quad \omega^2 x^2 + y^2 \leq c^2 \]

\[ [\vdash \omega \geq 0 \vdash 7 \geq 0] \]

\[ [\vdash \omega \geq 0 \vdash d' = 7] \quad d' \geq 0 \]

\[ d \geq 0 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0] \quad d \geq 0 \]

increasingly damped oscillator
Differential Cut Example: Increasingly Damped Oscillator

\[ \begin{align*}
\mathbb{R} & \quad \omega \geq 0 \land d \geq 0 \vdash 2 \omega^2 x y + 2 y(-\omega^2 x - 2 d \omega y) \leq 0 \\
[\leftarrow] & \quad \omega \geq 0 \land d \geq 0 \vdash [x' := y][y' := -\omega^2 x - 2 d \omega y] 2 \omega^2 x x' + 2 y y' \leq 0 \\
\text{dl} & \quad \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2 d \omega y, d' = 7 \land \omega \geq 0 \land d \geq 0] \omega^2 x^2 + y^2 \leq c^2 \\
\text{dC} & \quad \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2 d \omega y, d' = 7 \land \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2 \\
\mathbb{R} & \quad \omega \geq 0 \vdash 7 \geq 0 \\
[\leftarrow] & \quad \omega \geq 0 \vdash [d' := 7] d' \geq 0 \\
\text{dl} & \quad d \geq 0 \vdash [x' = y, y' = -\omega^2 x - 2 d \omega y, d' = 7 \land \omega \geq 0] d \geq 0
\end{align*} \]

increasingly damped oscillator
Differential Cut Example: Increasingly Damped Oscillator

Could repeatedly diffcut in formulas to help the proof
Andr´e Platzer (CMU)  

FCPS / 11: Differential Equations & Proofs  

20 / 22

**Ex:** Differential Cuts

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

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

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

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

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

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

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

\[ * \]

\[ dI \quad \vdash y^5 \geq 0 \]

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

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

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

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

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

\[ \mathbb{R} \vdash 5y^4y^2 \geq 0 \]

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

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

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

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

\[
\begin{align*}
\mathbb{R} & \quad \vdash 5y^4y^2 \geq 0 \\
[\' := ] & \quad \vdash [x' := (x - 2)^4 + y^5][y' := y^2]5y^4y' \geq 0 \\
dl & \quad y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]y^5 \geq 0
\end{align*}
\]
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)
\[ \varphi \models x' = f(x) \land Q \text{ for } r > 0 \Rightarrow \forall 0 \leq z \leq r \quad \varphi(z)[(e)'] = \frac{d\varphi(t)[e]}{dt}(z) \]

Differential Invariant
\[ \text{DI} \quad ([x' = f(x)]e \geq 0 \leftrightarrow e \geq 0) \quad \leftarrow [x' = f(x)](e)' \geq 0 \]

Proof (\( \geq \) rate of change from \( \geq \) initial value. Case \( r = 0 \) is easier.)
\[ h(t) \overset{\text{def}}{=} \varphi(t)[e] \text{ is differentiable on } [0, r] \text{ if } r > 0 \text{ by diff. lemma.} \]
\[ \frac{dh(t)}{dt}(z) = \frac{d\varphi(t)[e]}{dt}(z) = \varphi(z)[(e)'] \geq 0 \text{ by lemma + assume for all } z. \]
\[ h(r) - h(0) = (r - 0) \left( \frac{dh(t)}{dt}(\xi) \right) \geq 0 \text{ by mean-value theorem for some } \xi. \]
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**

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

**Differential Invariant**

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

**Differential Cut**

\[
F \vdash [x' = f(x) \& Q]C \quad F \vdash [x' = f(x) \& Q \land C]F \\
F \vdash [x' = f(x) \& Q]F
\]
André Platzer.
Foundations of cyber-physical systems.
URL: http://lfcps.org/course/fcps17.html.

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

_J. Autom. Reas., 2016._

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.
André Platzer.
Differential-algebraic dynamic logic for differential-algebraic programs. 

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

André Platzer.
A differential operator approach to equational differential invariants. 
In Lennart Beringer and Amy Felty, editors, *ITP*, volume 7406 of 
doi:10.1007/978-3-642-32347-8_3.