13: Differential Invariants & Proof Theory
Logical Foundations of Cyber-Physical Systems

André Platzer

Logical Foundations of Cyber-Physical Systems

Carnegie Mellon University
Computer Science Department
Outline

1. Learning Objectives
2. Recap: Proofs for Differential Equations
3. Differential Equation Proof Theory
   - Propositional Equivalences
   - Differential Invariants & Arithmetic
   - Differential Structure
   - Differential Invariant Equations
   - Equational Incompleteness
   - Strict Differential Invariant Inequalities
   - Differential Invariant Equations to Differential Invariant Inequalities
   - Differential Invariant Atoms
5. Curves Playing with Norms and Degrees
6. Summary
Outline

1. Learning Objectives
2. Recap: Proofs for Differential Equations
3. Differential Equation Proof Theory
   - Propositional Equivalences
   - Differential Invariants & Arithmetic
   - Differential Structure
   - Differential Invariant Equations
   - Equational Incompleteness
   - Strict Differential Invariant Inequalities
   - Differential Invariant Equations to Differential Invariant Inequalities
   - Differential Invariant Atoms
5. Curves Playing with Norms and Degrees
6. Summary
Learning Objectives
Differential Invariants & Proof Theory

- limits of computation
- proof theory for differential equations
- provability of differential equations
- nonprovability of differential equations
- proofs about proofs
- relativity theory of proofs
- inform differential invariant search
- intuition for differential equation proofs

- core argumentative principles
- tame analytic complexity
- improved analysis

André Platzer (CMU)
Outline

1 Learning Objectives

2 Recap: Proofs for Differential Equations

3 Differential Equation Proof Theory
   - Propositional Equivalences
   - Differential Invariants & Arithmetic
   - Differential Structure
   - Differential Invariant Equations
   - Equational Incompleteness
   - Strict Differential Invariant Inequalities
   - Differential Invariant Equations to Differential Invariant Inequalities
   - Differential Invariant Atoms

4 Differential Cut Power & Differential Ghost Power

5 Curves Playing with Norms and Degrees

6 Summary
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

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

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

DI \[ [x' = f(x) & Q]F \leftrightarrow (Q \rightarrow F \land [x' = f(x) & Q](F)') \]

DC \[ ([x' = f(x) & Q]F \leftrightarrow [x' = f(x) & Q \land C]F) \leftrightarrow [x' = f(x) & Q]C \]
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**

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

**Differential Weakening (DW)**

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

**Differential Invariant (DI)**

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

**Differential Cut (DC)**

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

**Differential Elimination (DE)**

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

1. Learning Objectives
2. Recap: Proofs for Differential Equations
3. Differential Equation Proof Theory
   - Propositional Equivalences
   - Differential Invariants & Arithmetic
   - Differential Structure
   - Differential Invariant Equations
   - Equational Incompleteness
   - Strict Differential Invariant Inequalities
   - Differential Invariant Equations to Differential Invariant Inequalities
   - Differential Invariant Atoms
5. Curves Playing with Norms and Degrees
6. Summary
Relativity Theory of Proofs

### Differential Invariant

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

But generalizations are helpful to find the right \( F \) in the first place:

\[
A \vdash F \\
\text{cut,MR} \\
F \vdash [x' = f(x) & Q]F \\
F \vdash B
\]

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

### Compare Provability with Classes \( \Omega \) of Differential Invariants

\( \mathcal{DI}_\Omega \) : properties provable with differential invariants in \( \Omega \subseteq \{\geq, >, =, \land, \lor\} \)

\( A \leq B \) iff all properties provable with \( A \) are also provable somehow with \( B \)

\( A \not\leq B \) otherwise, i.e., some property can be proved with \( A \) but not with \( B \)

\( A \equiv B \) iff \( A \leq B \) and \( B \leq A \) so same deductive power

\( A < B \) iff \( A \leq B \) and \( B \not\leq A \) so \( A \) has strictly less deductive power
Relativity Theory of Proofs

Differential Invariant

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

\[D\mathcal{I}_{e=k} \equiv D\mathcal{I}_{e=0} \text{ by considering } (e - k) = 0\]

But generalizations are helpful to find the right \( F \) in the first place:

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

\[\text{cut,MR} \]

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

Compare Provability with Classes \( \Omega \) of Differential Invariants

\[D\mathcal{I}_\Omega : \text{properties provable with differential invariants in } \Omega \subseteq \{\geq, >, =, \land, \lor\}\]

\( A \leq B \) iff all properties provable with \( A \) are also provable somehow with \( B \)

\( A \not\leq B \) otherwise, i.e., some property can be proved with \( A \) but not with \( B \)

\( A \equiv B \) iff \( A \leq B \) and \( B \leq A \) so same deductive power

\( A < B \) iff \( A \leq B \) and \( B \not\leq A \) so \( A \) has strictly less deductive power
Lemma (Differential invariants and propositional logic)

If \( F \leftrightarrow G \) is a propositional tautology then

\[ F \text{ differential invariant of } x' = f(x) \land Q \]

iff

\[ G \text{ differential invariant of } x' = f(x) \land Q \]

Proof.

Can use any propositional normal form
Lemma (Differential invariants and propositional logic)

If $F \leftrightarrow G$ is a propositional tautology then

$F$ differential invariant of $x' = f(x) \& Q$

iff $G$ differential invariant of $x' = f(x) \& Q$

Proof.

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

Can use any propositional normal form
Lemma (Differential invariants and propositional logic)

If $F \leftrightarrow G$ is a propositional tautology then

$F$ differential invariant of $x' = f(x) \& Q$

iff

$G$ differential invariant of $x' = f(x) \& Q$

Proof.

\[
\begin{align*}
\text{dl} & \quad G \vdash [x' = f(x) \& Q]G \\
\text{MR,cut} & \quad F \vdash [x' = f(x) \& Q]F
\end{align*}
\]

Can use any propositional normal form
Lemma (Differential invariants and propositional logic)

If $F \leftrightarrow G$ is a propositional tautology then

\[
F \text{ differential invariant of } x' = f(x) \& Q \\
iff \quad G \text{ differential invariant of } x' = f(x) \& Q
\]

Proof.

\[
:\equiv \\
Q \vdash [x' := f(x)](G)' \\
dl \\
G \vdash [x' = f(x) \& Q]G \\
MR, cut \\
F \vdash [x' = f(x) \& Q]F
\]

Can use any propositional normal form
Lemma (Differential invariants and propositional logic)

If \( F \leftrightarrow G \) is a propositional tautology then

\( F \) differential invariant of \( x' = f(x) \& Q \)

iff \( G \) differential invariant of \( x' = f(x) \& Q \)

Proof.

\[
\begin{array}{c}
\text{[=]}
\hline
Q \vdash [x':=f(x)](F)'
\hline
\text{dl}
G \vdash [x' = f(x) \& Q]G
\hline
\text{MR,cut}
F \vdash [x' = f(x) \& Q]F
\end{array}
\]

Can use any propositional normal form
Lemma (Differential invariants and propositional logic)

If $F \leftrightarrow G$ is a propositional tautology then

- $F$ differential invariant of $x' = f(x) \& Q$ if
- $G$ differential invariant of $x' = f(x) \& Q$

Proof.

\[
\begin{align*}
\begin{array}{c}
Q \vdash [x' := f(x)](F)' \\
G \vdash [x' = f(x) \& Q]G \\
F \vdash [x' = f(x) \& Q]F
\end{array}
\end{align*}
\]

$F \leftrightarrow G$ propositionally equivalent, so $(F)' \leftrightarrow (G)'$ propositionally equivalent

Can use any propositional normal form
Lemma (Differential invariants and propositional logic)

If $F \leftrightarrow G$ is a propositional tautology then

- $F$ differential invariant of $x' = f(x) \& Q$
- iff $G$ differential invariant of $x' = f(x) \& Q$

Proof.

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

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

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

$F \leftrightarrow G$ propositionally equivalent, so $(F)' \leftrightarrow (G)'$ propositionally equivalent since $(F_1 \land F_2)' \equiv (F_1)' \land (F_2)'$ . . .

Can use any propositional normal form
Lemma (Differential invariants and propositional logic)

If \( F \leftrightarrow G \) is real-arithmetic equivalence then

\[
F \text{ differential invariant of } x' = f(x) \land Q \quad \iff \quad G \text{ differential invariant of } x' = f(x) \land Q
\]

Proof.
Lemma (Differential invariants and propositional logic)

If $F \leftrightarrow G$ is real-arithmetic equivalence then

- $F$ differential invariant of $x' = f(x) \& Q$
- iff $G$ differential invariant of $x' = f(x) \& Q$

Proof.

$$\vdash_{dl} -5 \leq x \land x \leq 5 \vdash [x' = -x](-5 \leq x \land x \leq 5)$$
### Lemma (Differential invariants and propositional logic)

If \( F \leftrightarrow G \) is **real-arithmetic** equivalence then

- \( F \) differential invariant of \( x' = f(x) \) \& \( Q \)
- \( \text{iff} \) \( G \) differential invariant of \( x' = f(x) \) \& \( Q \)

### Proof.

\[
\begin{align*}
\vdash [x' := -x](0 \leq x' \land x' \leq 0) \\
\text{dl} \\
-5 \leq x \land x \leq 5 \vdash [x' = -x](-5 \leq x \land x \leq 5)
\end{align*}
\]
Lemma (Differential invariants and propositional logic)

If \( F \leftrightarrow G \) is real-arithmetic equivalence then

\[ F \text{ differential invariant of } x' = f(x) \land Q \]

iff \[ G \text{ differential invariant of } x' = f(x) \land Q \]

Proof.

\[
\begin{align*}
\vdash & \quad 0 \leq -x \land -x \leq 0 \\
[:=] & \quad \vdash [x' := -x](0 \leq x' \land x' \leq 0) \\
\text{dl} & \quad -5 \leq x \land x \leq 5 \vdash [x' = -x](-5 \leq x \land x \leq 5)
\end{align*}
\]
Lemma (Differential invariants and propositional logic)

If $F \leftrightarrow G$ is real-arithmetic equivalence then

- $F$ differential invariant of $x' = f(x) \& Q$
- iff $G$ differential invariant of $x' = f(x) \& Q$

Proof.

- not valid
- $\vdash 0 \leq -x \land -x \leq 0$
- $\vdash [x' := -x](0 \leq x' \land x' \leq 0)$
- $-5 \leq x \land x \leq 5 \vdash [x' = -x](-5 \leq x \land x \leq 5)$
Lemma (Differential invariants and propositional logic)

If $F \iff G$ is real-arithmetic equivalence then

- $F$ differential invariant of $x' = f(x) \& Q$
- iff $G$ differential invariant of $x' = f(x) \& Q$

Proof.

\[
\begin{align*}
\text{not valid} & \quad \vdash 0 \leq -x \land -x \leq 0 \\
\text{[=]} & \\
\text{dl} & \\
-5 \leq x \land x \leq 5 & \vdash [x' := -x](0 \leq x' \land x' \leq 0) \\
dl & \\
x^2 \leq 5^2 & \vdash [x' = -x]x^2 \leq 5^2
\end{align*}
\]

arithmetic equivalence $-5 \leq x \land x \leq 5 \iff x^2 \leq 5^2$
Lemma (Differential invariants and propositional logic)

If $F \leftrightarrow G$ is real-arithmetic equivalence then

$F$ differential invariant of $x' = f(x) \land Q$

iff

$G$ differential invariant of $x' = f(x) \land Q$

Proof.

<table>
<thead>
<tr>
<th>$\vdash 0 \leq -x \land -x \leq 0$</th>
</tr>
</thead>
<tbody>
<tr>
<td>[:=]</td>
</tr>
<tr>
<td>$\vdash [x':=-x](0 \leq x' \land x' \leq 0)$</td>
</tr>
<tr>
<td>$\text{dl}$</td>
</tr>
<tr>
<td>$-5 \leq x \land x \leq 5 \vdash [x' = -x](-5 \leq x \land x \leq 5)$</td>
</tr>
</tbody>
</table>

arithmetic equivalence $-5 \leq x \land x \leq 5 \leftrightarrow x^2 \leq 5^2$
Lemma (Differential invariants and propositional logic)

If \( F \leftrightarrow G \) is real-arithmetic equivalence then

\[
F \text{ differential invariant of } x' = f(x) \& Q
\]

iff

\[
G \text{ differential invariant of } x' = f(x) \& Q
\]

Proof.

\[
\begin{align*}
\text{not valid} & \quad \vdash 0 \leq -x \land -x \leq 0 \\
\text{[:=]} & \quad \vdash [x':=-x](0 \leq x' \land x' \leq 0) \\
\text{dl} & \quad -5 \leq x \land x \leq 5 \vdash [x' = -x](-5 \leq x \land x \leq 5)
\end{align*}
\]

\[
\begin{align*}
\text{\(\mathbb{R}\) not valid} & \quad \vdash -x2x \leq 0 \\
\text{[:=]} & \quad \vdash [x':=-x]2xx' \leq 0 \\
\text{dl} & \quad x^2 \leq 5^2 \vdash [x' = -x]x^2 \leq 5^2
\end{align*}
\]

arithmetic equivalence \(-5 \leq x \land x \leq 5 \leftrightarrow x^2 \leq 5^2\)
Lemma (Differential invariants and propositional logic)

If $F \iff G$ is **real-arithmetic** equivalence then

- $F$ differential invariant of $x' = f(x) \land Q$
- iff $G$ differential invariant of $x' = f(x) \land Q$

Proof.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>$[=:]$</td>
<td>$\vdash 0 \leq -x \land -x \leq 0$</td>
<td>$\vdash [x' := -x](0 \leq x' \land x' \leq 0)$</td>
</tr>
<tr>
<td>$dI$</td>
<td>$-5 \leq x \land x \leq 5 \vdash [x' = -x](-5 \leq x \land x \leq 5)$</td>
<td>$\vdash x^2 \leq 5^2$</td>
</tr>
</tbody>
</table>

Arithmetic equivalence $-5 \leq x \land x \leq 5 \iff x^2 \leq 5^2$
**Lemma (Differential invariants and propositional logic)**

If $F \leftrightarrow G$ is real-arithmetic equivalence then:

- $F$ differential invariant of $x' = f(x) \& Q$
- iff $G$ differential invariant of $x' = f(x) \& Q$

**Proof.**

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>not valid</td>
</tr>
<tr>
<td>$\Gamma \vdash 0 \leq -x \land -x \leq 0$</td>
</tr>
<tr>
<td>$\implies [x' := -x](0 \leq x' \land x' \leq 0)$</td>
</tr>
<tr>
<td>$\vdash [x' := -x](0 \leq x' \land x' \leq 0)$</td>
</tr>
<tr>
<td>$\vdash [x' := -x](-5 \leq x \land x \leq 5)$</td>
</tr>
<tr>
<td>$\vdash [-5 \leq x \land x \leq 5 \vdash [x' := -x](-5 \leq x \land x \leq 5)$</td>
</tr>
</tbody>
</table>

Despite arithmetic equivalence $-5 \leq x \land x \leq 5 \iff x^2 \leq 5^2$

Differential structure matters! Higher degree helps here
Different Differential Structure for Equivalent Solutions $\geq 0$

But different $p' \geq 0$.

Can still normalize atomic formulas to $e = 0$, $e \geq 0$, $e > 0$.
Different Differential Structure for Equivalent Solutions $\geq 0$.

Same $p \geq 0$.

But different $p' \geq 0$. 
Different Differential Structure for Equivalent Solutions $\geq 0$

Same $p \geq 0$.
But different $p' \geq 0$.

Can still normalize atomic formulas to $e = 0, e \geq 0, e > 0$.
Proposition (Equational deductive power [6, 2])

\[ DI = DI =, \wedge, \vee \]

Proof core. Full: [6, 2].
Proposition (Equational deductive power [6, 2])

atomic equations are enough:  \( \mathcal{DI}_= \equiv \mathcal{DI}_=,\wedge,\vee \)

Proof core.  Full: [6, 2].
Proposition (Equational deductive power [6, 2])

atomic equations are enough: $\mathcal{DI}_= \equiv \mathcal{DI}_=,\land,\lor$

Proof core. Full: [6, 2].

- $e_1 = e_2 \lor k_1 = k_2$

- $e_1 = e_2 \land k_1 = k_2$
Proposition (Equational deductive power \([6, 2]\))

*atomic equations are enough: \( \mathcal{DI}_= \equiv \mathcal{DI}_{=,\land,\lor} \)*

Proof core.

- \( e_1 = e_2 \lor k_1 = k_2 \leftrightarrow (e_1 - e_2)(k_1 - k_2) = 0 \)

- \( e_1 = e_2 \land k_1 = k_2 \leftrightarrow (e_1 - e_2)^2 + (k_1 - k_2)^2 = 0 \)
Proposition (Equational deductive power [6, 2])

atomic equations are enough:  \[ \mathcal{DI}_= \equiv \mathcal{DI}_{=,\land,\lor} \]

Proof core. Full: [6, 2].

- \( e_1 = e_2 \lor k_1 = k_2 \iff (e_1 - e_2)(k_1 - k_2) = 0 \)
  \[
  [x' := f(x)]((e_1)' = (e_2)' \land (k_1)' = (k_2)')
  \]

- \( e_1 = e_2 \land k_1 = k_2 \iff (e_1 - e_2)^2 + (k_1 - k_2)^2 = 0 \)
Differential Invariant Equations

Proposition (Equational deductive power [6, 2])

*atomic equations are enough:  \( \mathcal{DI}_= \equiv \mathcal{DI}_=,\wedge,\vee \)*

Proof core.  

- \( e_1 = e_2 \lor k_1 = k_2 \iff (e_1 - e_2)(k_1 - k_2) = 0 \)
  
  \[
  [x':=f(x)]((e_1)' = (e_2)' \land (k_1)' = (k_2)')
  \]

  So \( [x':=f(x)]((e_1 - e_2)(k_1 - k_2))' = 0 \)

  \[
  \equiv [x':=f(x)]((e_1)' - (e_2)')(k_1 - k_2) + (e_1 - e_2)((k_1)' - (k_2)') = 0
  \]

- \( e_1 = e_2 \land k_1 = k_2 \iff (e_1 - e_2)^2 + (k_1 - k_2)^2 = 0 \)
Proposition (Equational deductive power [6, 2])

\textit{atomic equations are enough:} \( \mathcal{DI}_= \equiv \mathcal{DI}_{=,\land,\lor} \)

\begin{itemize}
  \item \( e_1 = e_2 \lor k_1 = k_2 \iff (e_1 - e_2)(k_1 - k_2) = 0 \)
  
  \[ [x' := f(x)]((e_1)' = (e_2)' \land (k_1)' = (k_2)') \]

  So \( [x' := f(x)]((e_1 - e_2)(k_1 - k_2))' = 0 \)

  \[ \equiv [x' := f(x)](((e_1)' - (e_2)')(k_1 - k_2) + (e_1 - e_2)((k_1)' - (k_2)')) = 0 \]

  \item \( e_1 = e_2 \land k_1 = k_2 \iff (e_1 - e_2)^2 + (k_1 - k_2)^2 = 0 \)
\end{itemize}
Proposition (Equational deductive power \([6, 2]\))

atomic equations are enough: \[ DI_\equiv \equiv DI_{\equiv, \land, \lor} \]

Proof core.

\[ e_1 = e_2 \lor k_1 = k_2 \iff (e_1 - e_2)(k_1 - k_2) = 0 \]
\[ [x' := f(x)]((e_1)' = (e_2)' \land (k_1)' = (k_2)') \]
So \[ [x' := f(x)]((e_1 - e_2)(k_1 - k_2))' = 0 \]
\[ \equiv [x' := f(x)](((e_1)' - (e_2)')(k_1 - k_2) + (e_1 - e_2)((k_1)' - (k_2)') = 0) \]

\[ e_1 = e_2 \land k_1 = k_2 \iff (e_1 - e_2)^2 + (k_1 - k_2)^2 = 0 \]
Proposition (Equational deductive power [6, 2])

**atomic equations are enough:** \( \mathcal{DI}_= \equiv \mathcal{DI}_{=,\land,\lor} \)

Proof core. 

- \( e_1 = e_2 \lor k_1 = k_2 \iff (e_1 - e_2)(k_1 - k_2) = 0 \)
  
  \[ [x' := f(x)]((e_1)' = (e_2)' \land (k_1)' = (k_2)') \]
  
  So \( [x' := f(x)]((e_1 - e_2)(k_1 - k_2))' = 0 \)
  
  \( \equiv [x' := f(x)](((e_1)' - (e_2)')(k_1 - k_2) + (e_1 - e_2)((k_1)' - (k_2)') = 0) \)

- \( e_1 = e_2 \land k_1 = k_2 \iff (e_1 - e_2)^2 + (k_1 - k_2)^2 = 0 \)
  
  \[ [x' := f(x)]((e_1)' = (e_2)' \land (k_1)' = (k_2)') \]
Differential Invariant Equations

Proposition (Equational deductive power [6, 2])

Atomic equations are enough: \( \mathcal{DI} = \mathcal{DI}_{=, \wedge, \vee} \)

Proof core.

Full: [6, 2].

- \( e_1 = e_2 \lor k_1 = k_2 \iff (e_1 - e_2)(k_1 - k_2) = 0 \)
  \( [x' := f(x)]((e_1)' = (e_2)' \land (k_1)' = (k_2)') \)
  So \( [x' := f(x)]((e_1 - e_2)(k_1 - k_2))' = 0 \)
  \( \equiv [x' := f(x)](((e_1)' - (e_2)')(k_1 - k_2) + (e_1 - e_2)((k_1)' - (k_2)') = 0) \)

- \( e_1 = e_2 \land k_1 = k_2 \iff (e_1 - e_2)^2 + (k_1 - k_2)^2 = 0 \)
  \( [x' := f(x)]((e_1)' = (e_2)' \land (k_1)' = (k_2)') \)
  So \( [x' := f(x)](((e_1 - e_2)^2 + (k_1 - k_2)^2)' = 0) \)
  \( \equiv [x' := f(x)](2(e_1 - e_2)((e_1)' - (e_2)') + 2(k_1 - k_2)((k_1)' - (k_2)') = 0) \)
Differential Invariant Equations

Proposition (Equational deductive power [6, 2])

atomic equations are enough: \( \mathcal{DI}_= \equiv \mathcal{DI}_{=,\wedge,\vee} \)

Proof core. Full: [6, 2].

- \( e_1 = e_2 \lor k_1 = k_2 \iff (e_1 - e_2)(k_1 - k_2) = 0 \)
  
  \([x' := f(x)]((e_1)' = (e_2)' \land (k_1)' = (k_2)')\)
  
  So \([x' := f(x)]((e_1 - e_2)(k_1 - k_2))' = 0\)
  
  \(\equiv [x' := f(x)](((e_1)' - (e_2)')(k_1 - k_2) + (e_1 - e_2)((k_1)' - (k_2)') = 0)\)

- \( e_1 = e_2 \land k_1 = k_2 \iff (e_1 - e_2)^2 + (k_1 - k_2)^2 = 0 \)
  
  \([x' := f(x)]((e_1)' = (e_2)' \land (k_1)' = (k_2)')\)
  
  So \([x' := f(x)](((e_1 - e_2)^2 + (k_1 - k_2)^2)' = 0)\)
  
  \(\equiv [x' := f(x)](2(e_1 - e_2)((e_1)' - (e_2)') + 2(k_1 - k_2)((k_1)' - (k_2)') = 0)\) □
Differential Invariant Equations

Proposition (Equational deductive power [6, 2])

Atomic equations are enough: \( \mathcal{DI}_= \equiv \mathcal{DI}_{=, \wedge, \vee} \)

Proof core. Full: [6, 2].

- \( e_1 = e_2 \lor k_1 = k_2 \leftrightarrow (e_1 - e_2)(k_1 - k_2) = 0 \)
  
  \[
  [x' := f(x)]((e_1)' = (e_2)' \land (k_1)' = (k_2)')
  \]
  
  So \( [x' := f(x)]((e_1 - e_2)(k_1 - k_2))' = 0 \)
  
  \( \equiv [x' := f(x)](((e_1)' - (e_2)')(k_1 - k_2) + (e_1 - e_2)((k_1)' - (k_2)') = 0) \)

- \( e_1 = e_2 \land k_1 = k_2 \leftrightarrow (e_1 - e_2)^2 + (k_1 - k_2)^2 = 0 \)
  
  \[
  [x' := f(x)]((e_1)' = (e_2)' \land (k_1)' = (k_2)')
  \]
  
  So \( [x' := f(x)](((e_1 - e_2)^2 + (k_1 - k_2)^2)'=0) \)
  
  \( \equiv [x' := f(x)](2(e_1 - e_2)((e_1)' - (e_2)') + 2(k_1 - k_2)((k_1)' - (k_2)')=0) \)
Proposition (Equational [2])

\[ DI_= \equiv DI_=,\land,\lor \quad DI \quad DI_\geq \quad DI_= \]

Proof core.
Equational Incompleteness

Proposition (Equational incompleteness [2])

Equations are not enough: \( \mathcal{DI}_= \equiv \mathcal{DI}_{=,\wedge,\vee} < \mathcal{DI} \) because \( \mathcal{DI}_\geq \not\subseteq \mathcal{DI}_= \)

Proof core.
Equational Incompleteness

Proposition (Equational incompleteness [2])

Equations are not enough: \( DI_\equiv \equiv DI_{\equiv,\land,\lor} < DI \) because \( DI_\geq \not\subseteq DI_\equiv \)

Proof core.

Provable with \( DI_\geq \) Unprovable with \( DI_\equiv \)
Proposition (Equational incompleteness [2])

Equations are not enough: \( \mathcal{DI}_= \equiv \mathcal{DI}_=,\&,\lor < \mathcal{DI} \) because \( \mathcal{DI}_\geq \not\subseteq \mathcal{DI}_= \)

Proof core.

Provable with \( \mathcal{DI}_\geq \)

Unprovable with \( \mathcal{DI}_= \)

\[
\text{dl} \quad x \geq 0 \vdash [x' = 5]x \geq 0
\]
Proposition (Equational incompleteness [2])

Equations are not enough: \( \mathcal{DI}_\leq \equiv \mathcal{DI}_\leq, \wedge, \vee < \mathcal{DI} \) because \( \mathcal{DI}_\geq \nleq \mathcal{DI}_\leq \)

Proof core.

Provable with \( \mathcal{DI}_\geq \)

Unprovable with \( \mathcal{DI}_\leq \)

\[
\begin{align*}
\vdash [x' := 5]x' \geq 0 \\
\text{dl} \quad x \geq 0 \vdash [x' = 5]x \geq 0
\end{align*}
\]
Equational Incompleteness

**Proposition (Equational incompleteness [2])**

*Equations are not enough:* \(\mathcal{DI}=\equiv\mathcal{DI}=,\wedge,\vee < \mathcal{DI} \) because \(\mathcal{DI}\geq \not\leq \mathcal{DI}=\)

**Proof core.**

Provable with \(\mathcal{DI}\geq\)  
Unprovable with \(\mathcal{DI}=\)

\[
\begin{array}{c}
\text{R} \\
\vdash 5 \geq 0 \\
\text{[:=]} \\
\vdash [x':=5]x' \geq 0 \\
\text{dl} \\
\vdash x \geq 0 \vdash [x' = 5]x \geq 0
\end{array}
\]
Equational Incompleteness

Proposition (Equational incompleteness [2])

Equations are not enough: \( \mathcal{D} \mathcal{I} = \equiv \mathcal{D} \mathcal{I} =, \wedge, \vee < \mathcal{D} \mathcal{I} \) because \( \mathcal{D} \mathcal{I} \geq \not\leq \mathcal{D} \mathcal{I} = \)

Proof core.

Provable with \( \mathcal{D} \mathcal{I} \geq \)

Unprovable with \( \mathcal{D} \mathcal{I} = \)

\[
\begin{array}{l}
\mathbb{R} [\mathbb{R}] \quad \vdash 5 \geq 0 \\
[dI] \quad \vdash [x' := 5]x' \geq 0 \\
[\vdash] \quad \vdash [x' = 5]x \geq 0
\end{array}
\]
Proving Differences in Set Theory & Linear Algebra

Example (Sets Bijective or Not)

1 → 2 → 3 → 4 → 5 → 6

a → b → c → d → e → f

criterion: cardinality

|{1, . . . , 6}| = 6 ≠ |{a, b, c, d, e}| = 5

Need an indirect criterion especially if these sets are infinite

Example (Vector Spaces Isomorphic or Not)

y

\[\begin{array}{c}
\downarrow \\
\rightarrow x
\end{array}\]

\[\begin{array}{c}
\downarrow \\
\rightarrow x'
\end{array}\]

y'

criterion: dimension 3 ≠ 2
Proving Differences in Set Theory & Linear Algebra

Example (Sets Bijective or Not)

\[ \begin{align*}
1 & \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \\
| & | & | & | & | & |
\text{a} & \rightarrow \text{b} \rightarrow \text{c} \rightarrow \text{d} \rightarrow \text{e} \rightarrow \text{f}
\end{align*} \]

Criterion: cardinality
\[ |\{1, \ldots , 6\}| = 6 \neq |\{a, b, c, d, e\}| = 5 \]

Need an indirect criterion especially if these sets are infinite

Example (Vector Spaces Isomorphic or Not)

\[ \begin{align*}
\text{y} & \uparrow \\
\rightarrow & \text{ x} \\
\text{y}' & \uparrow \\
\rightarrow & \text{ x}'
\end{align*} \]

criterion: dimension 3 \( \neq 2 \)
Example (Sets Bijective or Not)

1 → 2 → 3 → 4 → 5 → 6
\[|\{1, \ldots, 6\}| = 6 \neq |\{a, b, c, d, e\}| = 5\]

1 → 2 → 3 → 4 → 5 → 6
\[|\{a, b, c, d, e\}| = 5 \neq |\{1, \ldots, 6\}| = 6\]

Need an indirect criterion especially if these sets are infinite.

Example (Vector Spaces Isomorphic or Not)

\[\begin{array}{ccc}
  y & \downarrow & y' \\
  \uparrow & & \uparrow \\
  x & \rightarrow & x'
\end{array}\]
Example (Sets Bijective or Not)

1 → 2 → 3 → 4 → 5 → 6  
|   |   |   |   |   |   |
  a → b → c → d → e → f

criterion: cardinality |{1, . . . , 6}| = 6 ≠ |{a, b, c, d, e}| = 5

Need an indirect criterion especially if these sets are infinite

Example (Vector Spaces Isomorphic or Not)

y  
|   |
→ x

y'  
|   |
→ x'

André Platzer (CMU)
Example (Sets Bijective or Not)

1 → 2 → 3 → 4 → 5 → 6
\[\{1, \ldots, 6\}\] = 6 ≠ \[\{a, b, c, d, e\}\] = 5

criterion: cardinality

Need an indirect criterion especially if these sets are infinite

Example (Vector Spaces Isomorphic or Not)

x → y → y' → x'

André Platzer (CMU)
Example (Sets Bijective or Not)

1 → 2 → 3 → 4 → 5 → 6

a → b → c → d → e → f

criterion: cardinality |\{1, \ldots, 6\}| = 6 \neq |\{a, b, c, d, e\}| = 5

Need an indirect criterion especially if these sets are infinite

Example (Vector Spaces Isomorphic or Not)

y

x

y'

x'

criterion: dimension 3

André Platzer (CMU)
Example (Sets Bijective or Not)

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>f</td>
</tr>
</tbody>
</table>

criterion: cardinality $|\{1, \ldots, 6\}| = 6 \neq |\{a, b, c, d, e\}| = 5$

Need an indirect criterion especially if these sets are infinite

Example (Vector Spaces Isomorphic or Not)

criterion: dimension $3 \neq 2$
Proposition (Equational incompleteness [2])

Equations are not enough: \( \mathcal{DI}_= \equiv \mathcal{DI}_{=,\land,\lor} < \mathcal{DI} \) because \( \mathcal{DI}_\geq \not\preceq \mathcal{DI}_= \)

Proof core.

Provable with \( \mathcal{DI}_\geq \):

Unprovable with \( \mathcal{DI}_= \):

\[
\begin{align*}
\mathbb{R} & \quad \ast \\
\vdash & \quad 5 \geq 0 \\
\[=\] & \quad \vdash [x' := 5]x' \geq 0 \\
dl & \quad x \geq 0 \vdash [x' = 5]x \geq 0
\end{align*}
\]
Equational Incompleteness

Proposition (Equational incompleteness [2])

Equations are not enough: $\mathcal{DI}_{\leq} \equiv \mathcal{DI}_{\leq , \wedge, \lor} < \mathcal{DI}$ because $\mathcal{DI}_{\geq} \not\subset \mathcal{DI}_{\leq}$

Proof core.

Provable with $\mathcal{DI}_{\geq}$

Unprovable with $\mathcal{DI}_{\leq}$

\[
\begin{align*}
\text{R} & \quad \ast \\
\vdash & \quad 5 \geq 0 \\
\text{[:=]} & \quad \vdash [x' := 5]x' \geq 0 \\
\text{dl} & \quad x \geq 0 \vdash [x' = 5]x \geq 0 \\
\text{cut, MR} & \quad x \geq 0 \vdash [x' = 5]x \geq 0
\end{align*}
\]
Proposition (Equational incompleteness [2])

Equations are not enough: $\mathcal{DI}_= \equiv \mathcal{DI}_= , \wedge , \vee < \mathcal{DI}$ because $\mathcal{DI}_\geq \not\leq \mathcal{DI}_=$

Proof core.

Provable with $\mathcal{DI}_\geq$

Unprovable with $\mathcal{DI}_=$

\[
\begin{align*}
\mathbb{R} & \quad \ast \quad \vdash 5 \geq 0 \\
\vdash [x' := 5]x' \geq 0 & \quad \vdash [x' = 5]x \geq 0 \\
\vdash p(x) = 0 & \quad \vdash [x' = 5]p(x) = 0 \\
\vdash x \geq 0 & \quad \vdash [x' = 5]x \geq 0
\end{align*}
\]
Equational Incompleteness

Proposition (Equational incompleteness [2])

Equations are not enough: \( DI_\equiv \equiv DI_\equiv, \wedge, \vee \) \(< DI \) because \( DI_\geq \not\subseteq DI_\equiv \)

Proof core.

Provable with \( DI_\geq \)

\[
\begin{align*}
\mathbb{R} & \quad \vdash 5 \geq 0 \\
[\equiv] & \quad \vdash [x' := 5]x' \geq 0 \\
[\geq] & \quad x \geq 0 \vdash [x' = 5]x \geq 0
\end{align*}
\]

Unprovable with \( DI_\equiv \)

\[
\begin{align*}
dl & \quad \vdash [x' := 5](p(x))' = 0 \\
cut,MR & \quad p(x) = 0 \vdash [x' = 5]p(x) = 0 \\
x \geq 0 & \vdash [x' = 5]x \geq 0
\end{align*}
\]
Equational Incompleteness

**Proposition (Equational incompleteness [2])**

*Equations are not enough:* $\mathcal{DI}_\geq \equiv \mathcal{DI}_\geq,\wedge,\vee \nless \mathcal{DI}$ because $\mathcal{DI}_\geq \nsubseteq \mathcal{DI}_=$

**Proof core.**

<table>
<thead>
<tr>
<th>Provable with $\mathcal{DI}_\geq$</th>
<th>Unprovable with $\mathcal{DI}_=$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{R}$</td>
<td>$\mathbb{R}$</td>
</tr>
<tr>
<td>$*$</td>
<td>$*$</td>
</tr>
<tr>
<td>$\vdash 5 \geq 0$</td>
<td>$\vdash 5 \geq 0$</td>
</tr>
<tr>
<td>$[=]$</td>
<td>$[=]$</td>
</tr>
<tr>
<td>$\vdash [x':=5]x' \geq 0$</td>
<td>$\vdash [x':=5]p(x)' = 0$</td>
</tr>
<tr>
<td>$\text{dl}$</td>
<td>$\text{dl}$</td>
</tr>
<tr>
<td>$x \geq 0 \vdash [x' = 5]x \geq 0$</td>
<td>$p(x) = 0 \vdash [x' = 5]p(x) = 0$</td>
</tr>
<tr>
<td>$\text{cut,MR}$</td>
<td>$x \geq 0 \vdash [x' = 5]x \geq 0$</td>
</tr>
</tbody>
</table>

[Univariate polynomial $p(x)$ is 0 if 0 on all $x \geq 0$]
### Proposition (Equational incompleteness [2])

*Equations are not enough:* \( \mathcal{DI}_= \equiv \mathcal{DI}_=,\land,\lor < \mathcal{DI} \) because \( \mathcal{DI}_\geq \not\subseteq \mathcal{DI}_= \)

### Proof core.

<table>
<thead>
<tr>
<th>Provable with ( \mathcal{DI}_\geq )</th>
<th>Unprovable with ( \mathcal{DI}_= )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbb{R} )</td>
<td></td>
</tr>
<tr>
<td>( \vdash 5 \geq 0 )</td>
<td>???</td>
</tr>
<tr>
<td>( [:=] )</td>
<td>( \vdash <a href="p(x)">x':=5</a>' = 0 )</td>
</tr>
<tr>
<td>( \vdash [x':=5]x' \geq 0 )</td>
<td>( \vdash [x':=5]p(x) = 0 )</td>
</tr>
<tr>
<td>( \text{dl} )</td>
<td>( p(x) = 0 \vdash [x' = 5]p(x) = 0 )</td>
</tr>
<tr>
<td>( x \geq 0 \vdash [x'=5]x \geq 0 )</td>
<td>( x \geq 0 \vdash [x' = 5]x \geq 0 )</td>
</tr>
</tbody>
</table>

Univariate polynomial \( p(x) \) is 0 if 0 on all \( x \geq 0 \)
Strict Inequality

Proposition (Strict barrier)

\[ \text{DI}_> \quad \text{DI} \quad \text{DI}_= \quad \text{DI}_> \]

Proof core.
Proposition (Strict barrier incompleteness)

*Strict inequalities are not enough:* \( \mathcal{DI} > \mathcal{DI} \) because \( \mathcal{DI} \neq \mathcal{DI} \)

Proof core.
### Proposition (Strict barrier incompleteness)

**Strict inequalities are not enough:** \( DI_\geq < DI \) because \( DI_\leq \not\subseteq DI_\geq \\

### Proof core.

Provable with \( DI_\leq \)  

Unprovable with \( DI_\geq \)
Strict Inequality Incompleteness

**Proposition (Strict barrier incompleteness)**

*Strict inequalities are not enough:* \( \mathcal{D}I_\succ \not< \mathcal{D}I \) because \( \mathcal{D}I_\preceq \not\leq \mathcal{D}I_\succ \)

**Proof core.**

Provable with \( \mathcal{D}I_\preceq \)

| dl \( \frac{v^2 + w^2 = c^2}{[v' = w, w' = -v]v^2 + w^2 = c^2} \) |

Unprovable with \( \mathcal{D}I_\succ \)
Proposition (Strict barrier incompleteness)

Strict inequalities are not enough:  $\mathcal{DI} > \mathcal{DI} < \mathcal{DI}$ because $\mathcal{DI} = \not\leq \mathcal{DI} >$

Proof core.

Provable with $\mathcal{DI} =$

Unprovable with $\mathcal{DI} >$

\[
\begin{align*}
\vdash [v' := w][w' := -v] & 2v v' + 2w w' = 0 \\
\frac{\vdash v^2 + w^2 = c^2}{\text{dl}} & [v' = w, w' = -v] v^2 + w^2 = c^2
\end{align*}
\]
Proposition (Strict barrier incompleteness)

*Strict inequalities are not enough:* \( D\mathcal{I}_> < D\mathcal{I} \) because \( D\mathcal{I}_= \not\leq D\mathcal{I}_> \)

**Proof core.**
Provable with \( D\mathcal{I}_= \)

Unprovable with \( D\mathcal{I}_> \)

\[
\begin{align*}
\mathbb{R} & \vdash 2v w + 2w(-v) = 0 \\
[:=] & \vdash [v':=w][w':=-v]2vv' + 2ww' = 0 \\
\text{dl} & \vdash v^2 + w^2 = c^2 \vdash [v' = w, w' = -v]v^2 + w^2 = c^2
\end{align*}
\]
Proposition (Strict barrier incompleteness)

Strict inequalities are not enough: \( \mathcal{D}_I > \mathcal{D}_I \) because \( \mathcal{D}_I = \not\leq \mathcal{D}_I > \).

Proof core.

Provable with \( \mathcal{D}_I = \)

\[
\begin{align*}
\mathbb{R} & \quad \vdash 2vw + 2w(-v) = 0 \\
[:=] & \quad \vdash [v' := w][w' := -v]2vv' + 2ww' = 0 \\
dl & \quad \vdash v^2 + w^2 = c^2 \quad \vdash [v' = w, w' = -v]v^2 + w^2 = c^2
\end{align*}
\]

Unprovable with \( \mathcal{D}_I > \).
**Proposition (Strict barrier incompleteness)**

*Strict inequalities are not enough: \( \mathcal{DI}_\prec \prec \mathcal{DI} \) because \( \mathcal{DI}_\prec \nsubseteq \mathcal{DI}_\prec \)

**Proof core.**

Provable with \( \mathcal{DI}_\equiv \)

\[
\begin{align*}
\mathbb{R} & \vdash 2vw + 2w(-v) = 0 \\
[:=] & \vdash [v':=w][w':=-v]2vv' + 2ww' = 0
\end{align*}
\]

\[
\begin{align*}
dl \quad v^2 + w^2 = c^2 & \vdash [v' = w, w' = -v]v^2 + w^2 = c^2
\end{align*}
\]

\( v^2 + w^2 = c^2 \) is a closed set

Closed \( v^2 + w^2 \leq 1 \) with full boundary

Open \( v^2 + w^2 < 1 \) without boundary

Unprovable with \( \mathcal{DI}_\prec \)

\( e > 0 \) is open set.
Proposition (Strict barrier incompleteness)

**Strict inequalities are not enough:** \( DI_\langle \nless DI \) because \( DI_\leq \not\subseteq DI_\rangle \)

Proof core.

Provable with \( DI_\leq \)

\[
egin{array}{l}
\mathbb{R} \vdash 2vw + 2w(-v) = 0 \\
[=] \vdash [v' := w] [w' := -v] 2vv' + 2ww' = 0 \\
dl \vdash v^2 + w^2 = c^2 \vdash [v' = w, w' = -v] v^2 + w^2 = c^2
\end{array}
\]

\( v^2 + w^2 = c^2 \) is a closed set

Closed \( v^2 + w^2 \leq 1 \) with full boundary

Open \( v^2 + w^2 < 1 \) without boundary

Unprovable with \( DI_\rangle \)

\( e > 0 \) is open set.

Only *true* and *false* are both
Proposition (Strict barrier incompleteness)

Strict inequalities are not enough: \(DI_\prec < DI\) because \(DI_\leq \not\subseteq DI_\prec\)

Proof core.

Provable with \(DI_\leq\)

\[
\begin{align*}
\mathbb{R} & \quad \vdash 2vw + 2w(-v) = 0 \\
[:=] & \quad \vdash [v' := w][w' := -v]2vv' + 2ww' = 0 \\
\downarrow & \quad \vdash v^2 + w^2 = c^2 \quad \vdash [v' = w, w' = -v]v^2 + w^2 = c^2
\end{align*}
\]

\(v^2 + w^2 = c^2\) is a closed set

Unprovable with \(DI_\prec\)

\(e > 0\) is open set.

Only true and false are both but don’t help proof

Closed \(v^2 + w^2 \leq 1\) with full boundary

Open \(v^2 + w^2 < 1\) without boundary
Differential Invariant Equations to Inequalities

Proposition (Equational)

\[ \mathcal{DI}_=,\land,\lor \quad \mathcal{DI}_\geq \]

Proof core.
Proposition (Equational definability)

Equations are definable by weak inequalities: \( DI_{=,\wedge,\vee} \leq DI_{\geq} \)

Proof core.
### Proposition (Equational definability)

*Equations are definable by weak inequalities:* \( \mathcal{DI}_{=,\land,\lor} \leq \mathcal{DI}_{\geq} \)

### Proof core.

Provable with \( \mathcal{DI}_{=} \) \hspace{1cm} Provable with \( \mathcal{DI}_{\geq} \)
Proposition (Equational definability)

Equations are definable by weak inequalities: \( \mathcal{DI}_{\leq, \wedge, \vee} \leq \mathcal{DI}_{\geq} \)

Proof core.
Provable with \( \mathcal{DI}_{\leq} \)

\[
\frac{\text{d}x = 0}{\vdash [x' = f(x) \land Q] e = 0}
\]

Provable with \( \mathcal{DI}_{\geq} \)
Proposition (Equational definability)

Equations are definable by weak inequalities: \( \mathcal{DI}_{\leq, \land, \lor} \leq \mathcal{DI}_{\geq} \)

Proof core.

Provable with \( \mathcal{DI}_{=} \)

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

Provable with \( \mathcal{DI}_{\geq} \)
Proposition (Equational definability)

Equations are definable by weak inequalities: \( \mathcal{DI}_{=,\wedge,\vee} \leq \mathcal{DI}_{\geq} \)

Proof core.

Provable with \( \mathcal{DI}_{=} \)

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

Provable with \( \mathcal{DI}_{\geq} \)
Proposition (Equational definability)

Equations are definable by weak inequalities: \[ \mathcal{DI}_{\leq, \land, \lor} \leq \mathcal{DI}_{\geq} \]

Proof core.

Provable with \( \mathcal{DI}_{\leq} \)

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

Provable with \( \mathcal{DI}_{\geq} \)

\[
\begin{align*}
\text{dl} \quad -e^2 \geq 0 & \quad \vdash [x' = f(x) \& Q](-e^2 \geq 0)
\end{align*}
\]

Local view of logic on differentials is crucial for this proof.
Proposition (Equational definability)

Equations are definable by weak inequalities: $\mathcal{DI}_{\leq,\land,\lor} \leq \mathcal{DI}_{\geq}$

Proof core.

Provable with $\mathcal{DI}_=$

$\ast$

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

Provable with $\mathcal{DI}_{\geq}$

\[ Q \vdash [x' := f(x)] - 2e(e)' \geq 0 \]
\[ \text{dI} \]
\[ -e^2 \geq 0 \vdash [x' = f(x) \& Q](-e^2 \geq 0) \]
**Proposition (Equational definability)**

Equations are definable by weak inequalities: \[ \mathcal{DI}_{\leq, \wedge, \vee} \leq \mathcal{DI}_{\geq} \]

**Proof core.**

Provable with \( \mathcal{DI}_{\leq} \)

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

Provable with \( \mathcal{DI}_{\geq} \)

\[
\begin{align*}
* & \quad Q \vdash [x' := f(x)] - 2e(e)' \geq 0 \\
\text{dl} & \quad -e^2 \geq 0 \vdash [x' = f(x) \& Q](-e^2 \geq 0)
\end{align*}
\]

Local view of logic on differentials is crucial for this proof. Degree increases
Differential Invariant Atoms

**Theorem (Atomic)**

\[ DI \geq, DI \geq, \wedge, \lor \text{ and } DI >, DI >, \wedge, \lor \]

**Proof idea.**
Theorem (Atomic incompleteness)

Atomic inequalities not enough: \( DI \geq \ LDI \geq, \land, \lor \ and DI > \ RDI \geq, \land, \lor \)

Proof idea.
**Theorem (Atomic incompleteness)**

*Atomic inequalities not enough:* \( DI_\geq < DI_{\geq,\land,\lor} \) and \( DI_\times < DI_{\times,\land,\lor} \)

**Proof idea.**

Provable with \( DI_{\geq,\land,\lor} \)  
Unprovable with \( DI_\geq \)
Theorem (Atomic incompleteness)

Atomic inequalities not enough: \( \mathcal{DI}_\geq < \mathcal{DI}_{\geq,\land,\lor} \) and \( \mathcal{DI}_> < \mathcal{DI}_{>,\land,\lor} \)

Proof idea.

Provable with \( \mathcal{DI}_{\geq,\land,\lor} \)

\[
\begin{align*}
\star & \\
\mathbb{R} & \vdash 5 \geq 0 \land y^2 \geq 0 \\
[\vdash] & \vdash [x' := 5][y' := y^2](x' \geq 0 \land y' \geq 0) \\
dl & x \geq 0 \land y \geq 0 \vdash [x' = 5, y' = y^2](x \geq 0 \land y \geq 0)
\end{align*}
\]

Unprovable with \( \mathcal{DI}_> \)
Theorem (Atomic incompleteness)

**Atomic inequalities not enough:** \( \mathcal{DI}_\geq \not< \mathcal{DI}_\geq,\wedge,\vee \) and \( \mathcal{DI}_> \not< \mathcal{DI}_>,\wedge,\vee \)

Proof idea.

**Provable with** \( \mathcal{DI}_\geq,\wedge,\vee \)

\[
\begin{array}{c}
\vdash 5 \geq 0 \wedge y^2 \geq 0 \\
\vdash [x' := 5][y' := y^2](x' \geq 0 \wedge y' \geq 0)
\end{array}
\]

Unprovable with \( \mathcal{DI}_\geq \)

\[
p(x, y) \geq 0 \iff x \geq 0 \wedge y \geq 0
\]

impossible since this implies \( p(x, 0) \geq 0 \iff x \geq 0 \)

so \( p(x, 0) \) is 0

\[
x \geq 0 \wedge y \geq 0 \vdash [x' = 5, y' = y^2](x \geq 0 \wedge y \geq 0)
\]
**Theorem (Atomic incompleteness)**

Atomic inequalities not enough: \( \mathcal{DI}_\geq < \mathcal{DI}_\geq,\wedge,\vee \) and \( \mathcal{DI}_\leq < \mathcal{DI}_\leq,\wedge,\vee \)

**Proof idea.**

Provable with \( \mathcal{DI}_{\geq,\wedge,\vee} \)

\[
\begin{align*}
\implies &\ 5 \geq 0 \wedge y^2 \geq 0 \\
\iff &\ [x':=5][y':=y^2](x'\geq 0\wedge y'\geq 0)
\end{align*}
\]

Unprovable with \( \mathcal{DI}_{\geq} \)

\[
p(x, y) \geq 0 \iff x \geq 0 \wedge y \geq 0
\]

impossible since this implies

\[
p(x, 0) \geq 0 \iff x \geq 0
\]

so \( p(x, 0) \) is 0

Substantial remaining parts of the proof shown elsewhere [2].
Theorem (Atomic incompleteness)

Atomic inequalities not enough: $\mathcal{DI}_\geq < \mathcal{DI}_{\geq,\land,\lor}$ and $\mathcal{DI}_\geq > \mathcal{DI}_{\geq,\land,\lor}$

Proof idea.

Provable with $\mathcal{DI}_{\geq,\land,\lor}$

\[
\begin{align*}
\mathbb{R} & \vdash 5 \geq 0 \land y^2 \geq 0 \\
\text{[:=]} & \vdash [x' := 5] [y' := y^2] (x' \geq 0 \land y' \geq 0) \\
\text{dI} & \vdash x \geq 0 \land y \geq 0 \vdash [x' = 5, y' = y^2] (x \geq 0 \land y \geq 0)
\end{align*}
\]

Unprovable with $\mathcal{DI}_{\geq}$

\[p(x, y) \geq 0 \leftrightarrow x \geq 0 \land y \geq 0\]

impossible since this implies

\[p(x, 0) \geq 0 \leftrightarrow x \geq 0\]

so $p(x, 0)$ is 0

Substantial remaining parts of the proof shown elsewhere [2].

\[\square\]

dC still possible here but more involved argument separates.
Outline

1. Learning Objectives
2. Recap: Proofs for Differential Equations
3. Differential Equation Proof Theory
   - Propositional Equivalences
   - Differential Invariants & Arithmetic
   - Differential Structure
   - Differential Invariant Equations
   - Equational Incompleteness
   - Strict Differential Invariant Inequalities
   - Differential Invariant Equations to Differential Invariant Inequalities
   - Differential Invariant Atoms
5. Curves Playing with Norms and Degrees
6. Summary
### Theorem (Gentzen’s Cut Elimination) (1935)

\[
\begin{align*}
A & \vdash B \lor C \\
A \land C & \vdash B \\
\hline
A & \vdash B
\end{align*}
\]

*cut can be eliminated*

### Theorem (No Differential Cut Elimination) (LMCS 2012)

*Deductive power with differential cuts exceeds deductive power without.*

\[
\mathcal{DI} + DC > \mathcal{DI}
\]

### Theorem (Auxiliary Differential Variables) (LMCS 2012)

*Deductive power with differential ghosts exceeds power without.*

\[
\mathcal{DI} + DC + DG > \mathcal{DI} + DC
\]
Ex: The Need for Differential Cuts

\[
dx^3 \geq -1 \land y^5 \geq 0 \vdash \left[ x' = (x - 2)^4 + y^5, y' = y^2 \right] x^3 \geq -1
\]
The Need for Differential Cuts

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

\[ \vdash \quad 3x^2((x - 2)^4 + y^5) \geq 0 \]

\[ [::] \quad \vdash \quad [x' := (x - 2)^4 + y^5][y' := \hat{y}^2]3x^2x' \geq 0 \]

\[ \text{dl} \quad x^3 \geq -1 \land y^5 \geq 0 \vdash \quad [x' = (x - 2)^4 + y^5, y' = \hat{y}^2]x^3 \geq -1 \]
Ex: The Need for Differential Cuts

not valid

\[ \vdash 3x^2((x - 2)^4 + y^5) \geq 0 \]

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

\[ dl \quad x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]x^3 \geq -1 \]
not valid

\[ \vdash 3x^2((x - 2)^4 + y^5) \geq 0 \]

\[ [:=] \]

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

\[ \Downarrow \]

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

Have to know something about \( y^5 \)
Ex: Differential Cuts

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

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

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

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

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

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

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

\[
\begin{align*}
[=:] & \quad y^5 \geq 0 \vdash [x' := (x - 2)^4 + y^5][y' := y^2]2x^2x' \geq 0 \\
dl & \quad x^3 \geq -1 \vdash [x' = (x - 2)^4 + y^5, y' = y^2 \land y^5 \geq 0]x^3 \geq -1 \triangleright \\
dC & \quad x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]x^3 \geq -1 \\
\ast & \\
\mathbb{R} & \quad \vdash 5y^4y^2 \geq 0 \\
[=:] & \quad \vdash [x' := (x - 2)^4 + y^5][y' := y^2]5y^4y' \geq 0 \\
dl & \quad y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]y^5 \geq 0
\end{align*}
\]
\[
\begin{align*}
\mathbb{R} & \quad y^5 \geq 0 \vdash 2x^2((x - 2)^4 + y^5) \geq 0 \\
[=:] & \quad y^5 \geq 0 \vdash [x' := (x - 2)^4 + y^5][y' := y^2]2x^2x' \geq 0 \\
dl & \quad x^3 \geq -1 \vdash [x' = (x - 2)^4 + y^5, y' = y^2 \& y^5 \geq 0]x^3 \geq -1 \\
dC & \quad x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]x^3 \geq -1 \\
\ast & \quad \vdash 5y^4y^2 \geq 0 \\
[=:] & \quad \vdash [x' := (x - 2)^4 + y^5][y' := y^2]5y^4y' \geq 0 \\
dl & \quad y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]y^5 \geq 0
\end{align*}
\]
<table>
<thead>
<tr>
<th>Differential Cuts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ex:</strong></td>
</tr>
</tbody>
</table>

| **R** | $y^5 \geq 0 \vdash 2x^2((x - 2)^4 + y^5) \geq 0$ |
| **[=]** | $y^5 \geq 0 \vdash [x' := (x - 2)^4 + y^5][y' := y^2]2x^2x' \geq 0$ |
| **dl** | $x^3 \geq -1 \vdash [x' = (x - 2)^4 + y^5, y' = y^2 \& y^5 \geq 0]x^3 \geq -1$ |
| **dC** | $x^3 \geq -1 \& y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]x^3 \geq -1$ |

| **R** | $\vdash 5y^4y^2 \geq 0$ |
| **[=]** | $\vdash [x' := (x - 2)^4 + y^5][y' := y^2]5y^4y' \geq 0$ |
| **dl** | $y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2]y^5 \geq 0$ |
Outline

1 Learning Objectives

2 Recap: Proofs for Differential Equations

3 Differential Equation Proof Theory
   - Propositional Equivalences
   - Differential Invariants & Arithmetic
   - Differential Structure
   - Differential Invariant Equations
   - Equational Incompleteness
   - Strict Differential Invariant Inequalities
   - Differential Invariant Equations to Differential Invariant Inequalities
   - Differential Invariant Atoms

4 Differential Cut Power & Differential Ghost Power

5 Curves Playing with Norms and Degrees

6 Summary
Lemma (Differential invariants and propositional logic)

If $F \leftrightarrow G$ is real-arithmetic equivalence then

$F$ differential invariant of $x' = f(x) \& Q$

iff $G$ differential invariant of $x' = f(x) \& Q$

Proof.

$$\not\quad \vdash \ [x' := -x] (0 \leq x' \land x' \leq 0)$$

Despite arithmetic equivalence $-5 \leq x \land x \leq 5 \leftrightarrow x^2 \leq 5^2$

Differential structure matters! Higher degree helps here
\[
\begin{align*}
A & \equiv v^2 + w^2 \leq 1 \land x = y = t = 0 \\
\| (x, y) \|_\infty & \leq t \equiv -t \leq x \leq t \land -t \leq y \leq t \quad \text{Supremum norm} \\
\| (x, y) \|_2 & \leq t \equiv x^2 + y^2 \leq t^2 \quad \text{Euclidean norm}
\end{align*}
\]
Curves Playing with Norms and Degrees

\[ \begin{align*}
\text{dl} & \quad A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \& v^2 + w^2 \leq 1] \| (x, y) \|_\infty \leq t \\
\text{dC} & \quad A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1] \| (x, y) \|_\infty \leq t
\end{align*} \]

\[ A \overset{\text{def}}{=} v^2 + w^2 \leq 1 \land x = y = t = 0 \]

\[ \| (x, y) \|_\infty \leq t \overset{\text{def}}{=} -t \leq x \leq t \land -t \leq y \leq t \quad \text{Supremum norm} \]

\[ \| (x, y) \|_2 \leq t \overset{\text{def}}{=} x^2 + y^2 \leq t^2 \quad \text{Euclidean norm} \]
\[
\begin{align*}
\vdash v^2 + w^2 \leq 1 & \implies [x' := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1](-t' \leq x' \leq t' \land -t' \leq y' \leq t') \\
\vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 & v^2 + w^2 \leq 1] \|(x, y)\|_\infty \leq t \\
\vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1] \|(x, y)\|_\infty \leq t
\end{align*}
\]

\[A \overset{\text{def}}{=} v^2 + w^2 \leq 1 \land x = y = t = 0\]

\[\|(x, y)\|_\infty \overset{\text{def}}{=} -t \leq x \leq t \land -t \leq y \leq t\]

\[\|(x, y)\|_2 \overset{\text{def}}{=} x^2 + y^2 \leq t^2\]

Supremum norm

Euclidean norm
\[
\begin{align*}
\mathbb{R} &\quad v^2 + w^2 \leq 1 \vdash -1 \leq v \leq 1 \land -1 \leq w \leq 1 \\
\vdash &\quad v^2 + w^2 \leq 1 \quad [x' := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1](-t' \leq x' \leq t' \land -t' \leq y' \leq t') \\
\text{dI} &\quad A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \land v^2 + w^2 \leq 1]\|(x, y)\|_\infty \leq t \\
\text{dC} &\quad A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1]\|(x, y)\|_\infty \leq t
\end{align*}
\]

\[A \overset{\text{def}}{=} v^2 + w^2 \leq 1 \land x = y = t = 0\]

\[\|(x, y)\|_\infty \overset{\text{def}}{=} -t \leq x \leq t \land -t \leq y \leq t \quad \text{Supremum norm}\]

\[\|(x, y)\|_2 \overset{\text{def}}{=} x^2 + y^2 \leq t^2 \quad \text{Euclidean norm}\]
\[
\begin{align*}
\mathbb{R} &\quad v^2 + w^2 \leq 1 \vdash -1 \leq v \leq 1 \land -1 \leq w \leq 1 \quad * \\quad \\
\text{[=]} &\quad v^2 + w^2 \leq 1 \vdash [x := v][y := w][v' := \omega w][w' := -\omega v][t' := 1](-t' \leq x' \leq t' \land -t' \leq y' \leq t') \\
\text{dI} &\quad \triangleright A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \land v^2 + w^2 \leq 1] \| (x, y) \|_\infty \leq t \\
\text{dC} &\quad A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1] \| (x, y) \|_\infty \leq t
\end{align*}
\]

\[
\begin{align*}
A &\equiv v^2 + w^2 \leq 1 \land x = y = t = 0 \\
\| (x, y) \|_\infty &\equiv -t \leq x \leq t \land -t \leq y \leq t \quad \text{Supremum norm} \\
\| (x, y) \|_2 &\equiv x^2 + y^2 \leq t^2 \quad \text{Euclidean norm}
\end{align*}
\]
\[
\begin{align*}
\mathbb{R} & \quad v^2 + w^2 \leq 1 \vdash -1 \leq v \leq 1 \land -1 \leq w \leq 1 \\
\vdash & \quad v^2 + w^2 \leq 1 \quad [x' := v, y' := w, v' := \omega w, w' := -\omega v, t' := 1](-t' \leq x' \leq t' \land -t' \leq y' \leq t') \\
\vdash & \quad A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \land v^2 + w^2 \leq 1] \| (x, y) \|_\infty \leq t \\
\vdash & \quad A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1] \| (x, y) \|_\infty \leq t \\
\vdash & \quad A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1] \| (x, y) \|_2 \leq t \\
A & \equiv v^2 + w^2 \leq 1 \land x = y = t = 0 \\
\| (x, y) \|_\infty \leq t & \equiv -t \leq x \leq t \land -t \leq y \leq t \quad \text{Supremum norm} \\
\| (x, y) \|_2 \leq t & \equiv x^2 + y^2 \leq t^2 \quad \text{Euclidean norm}
\end{align*}
\]
\[
\begin{align*}
\mathbb{R} & \quad v^2 + w^2 \leq 1 \vdash -1 \leq v \leq 1 \land -1 \leq w \leq 1 \\
[=] & \quad v^2 + w^2 \leq 1 \vdash [x' := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1](-t' \leq x' \leq t' \land -t' \leq y' \leq t') \\
\text{dl} & \quad A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \land v^2 + w^2 \leq 1]\|(x, y)\|_\infty \leq t \\
\text{dC} & \quad A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1]\|(x, y)\|_\infty \leq t \\
\text{dl} & \quad A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \land v^2 + w^2 \leq 1]\|(x, y)\|_2 \leq t \\
\text{dC} & \quad A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1]\|(x, y)\|_2 \leq t \\
A & \equiv v^2 + w^2 \leq 1 \land x = y = t = 0 \\
\|(x, y)\|_\infty & \equiv -t \leq x \leq t \land -t \leq y \leq t \quad \text{Supremum norm} \\
\|(x, y)\|_2 & \equiv x^2 + y^2 \leq t^2 \quad \text{Euclidean norm}
\end{align*}
\]
\[
\begin{align*}
\mathbb{R} & \quad v^2 + w^2 \leq 1 \models -1 \leq v \leq 1 \land -1 \leq w \leq 1 \\
[=] & \quad v^2 + w^2 \leq 1 \models [x' := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1](-t' \leq x' \leq t' \land -t' \leq y' \leq t') \\
\triangledown & \quad A \models [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \& v^2 + w^2 \leq 1]\|(x, y)\|_\infty \leq t \\
dC & \quad A \models [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1]\|(x, y)\|_\infty \leq t \\
\end{align*}
\]

\[
\begin{align*}
[=] & \quad v^2 + w^2 \leq 1 \models [x' := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1](2xx' + 2yy' \leq 2tt') \\
\triangledown & \quad A \models [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \& v^2 + w^2 \leq 1]\|(x, y)\|_2 \leq t \\
dC & \quad A \models [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1]\|(x, y)\|_2 \leq t \\
A & \quad \text{def} \quad v^2 + w^2 \leq 1 \land x = y = t = 0 \\
\|(x, y)\|_\infty & \quad \text{def} \quad -t \leq x \leq t \land -t \leq y \leq t \quad \text{Supremum norm} \\
\|(x, y)\|_2 & \quad \text{def} \quad x^2 + y^2 \leq t^2 \quad \text{Euclidean norm}
\end{align*}
\]
* \[\mathbb{R} \vdash v^2 + w^2 \leq 1 \supset -1 \leq v \leq 1 \land -1 \leq w \leq 1\]

\[\vdash v^2 + w^2 \leq 1 \supset [x' := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1](-t' \leq x' \leq t' \land -t' \leq y' \leq t')\]

\[\vdash A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \& v^2 + w^2 \leq 1] \parallel (x, y) \parallel_\infty \leq t\]

\[\vdash x^2 + y^2 \leq 1 \supset 2xv + 2yw \leq 2t\]

\[\vdash x^2 + y^2 \leq 1 \supset [x' := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1](2xx' + 2yy' \leq 2tt')\]

\[\vdash A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \& v^2 + w^2 \leq 1] \parallel (x, y) \parallel_2 \leq t\]

\[A \text{ def } \equiv v^2 + w^2 \leq 1 \land x = y = t = 0\]

\[\parallel (x, y) \parallel_\infty \leq t \text{ def } \equiv -t \leq x \leq t \land -t \leq y \leq t\]

\[\text{Supremum norm}\]

\[\parallel (x, y) \parallel_2 \leq t \text{ def } \equiv x^2 + y^2 \leq t^2\]

\[\text{Euclidean norm}\]
Curves Playing with Norms and Degrees

\[ v^2 + w^2 \leq 1 \vdash -1 \leq v \leq 1 \land -1 \leq w \leq 1 \]

\[ v^2 + w^2 \leq 1 \vdash [x' := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1](-t' \leq x' \leq t' \land -t' \leq y' \leq t') \]

\[ A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \land v^2 + w^2 \leq 1] \| (x, y) \| \infty \leq t \]

not valid

\[ v^2 + w^2 \leq 1 \vdash 2xv + 2yw \leq 2t1 \]

\[ v^2 + w^2 \leq 1 \vdash [x' := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1](2xx' + 2yy' \leq 2tt') \]

\[ A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \land v^2 + w^2 \leq 1] \| (x, y) \| \leq t \]

\[ x = y = t = 0 \implies v^2 + w^2 \leq 1 \]

\[ \| (x, y) \| \infty \leq t \implies -t \leq x \leq t \land -t \leq y \leq t \] Supremum norm

\[ \| (x, y) \| \leq t \implies x^2 + y^2 \leq t^2 \] Euclidean norm
Curves Playing with Norms and Degrees

\[ v^2 + w^2 \leq 1 \vdash -1 \leq v \leq 1 \land -1 \leq w \leq 1 \]

\[ v^2 + w^2 \leq 1 \vdash [x' := v] [y' := w] [v' := \omega w] [w' := -\omega v] [t' := 1] (-t' \leq x' \leq t' \land -t' \leq y' \leq t') \]

\[ A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \land v^2 + w^2 \leq 1] \|(x, y)\|_\infty \leq t \]

\[ A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1] \|(x, y)\|_2 \leq t \]

Lower degree helps here

\[ v^2 + w^2 \leq 1 \vdash 2xv + 2yw \leq 2t1 \]

\[ v^2 + w^2 \leq 1 \vdash [x' := v] [y' := w] [v' := \omega w] [w' := -\omega v] [t' := 1] (2xx' + 2yy' \leq 2tt') \]

\[ A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \land v^2 + w^2 \leq 1] \|(x, y)\|_2 \leq t \]

\[ A \overset{\text{def}}{=} v^2 + w^2 \leq 1 \land x = y = t = 0 \]

\[ \|(x, y)\|_\infty \overset{\text{def}}{=} -t \leq x \leq t \land -t \leq y \leq t \quad \text{Supremum norm} \]

\[ \|(x, y)\|_2 \overset{\text{def}}{=} x^2 + y^2 \leq t^2 \quad \text{Euclidean norm} \]
Interreducing Norms in Dimension $n$

$$\forall x \forall y (\| (x, y) \|_\infty \leq \| (x, y) \|_2 \leq \sqrt{n} \| (x, y) \|_\infty)$$

$$\forall x \forall y \left( \frac{1}{\sqrt{n}} \| (x, y) \|_2 \leq \| (x, y) \|_\infty \leq \| (x, y) \|_2 \right)$$
Interreducing Norms in Dimension $n$

$$\forall x \forall y \left( \|(x, y)\|_\infty \leq \|(x, y)\|_2 \leq \sqrt{n} \|(x, y)\|_\infty \right)$$

$$\forall x \forall y \left( \frac{1}{\sqrt{n}} \|(x, y)\|_2 \leq \|(x, y)\|_\infty \leq \|(x, y)\|_2 \right)$$

Benefit from norm relations but be mindful of approximation error factors
Interreducing Norms in Dimension $n$

\[ \forall x \forall y \left( \|(x, y)\|_\infty \leq \|(x, y)\|_2 \leq \sqrt{n} \|(x, y)\|_\infty \right) \]
\[ \forall x \forall y \left( \frac{1}{\sqrt{n}} \|(x, y)\|_2 \leq \|(x, y)\|_\infty \leq \|(x, y)\|_2 \right) \]
Interreducing Norms in Dimension $n$

$$\forall x \forall y \left( \| (x, y) \|_\infty \leq \| (x, y) \|_2 \leq \sqrt{n} \| (x, y) \|_\infty \right)$$

$$\forall x \forall y \left( \frac{1}{\sqrt{n}} \| (x, y) \|_2 \leq \| (x, y) \|_\infty \leq \| (x, y) \|_2 \right)$$

\[\| \cdot \|_\infty \leq 1\]

\[\| \cdot \|_2 \leq 1\]

\[\| \cdot \|_\infty \leq \frac{1}{\sqrt{2}}\]
Interreducing Norms in Dimension $n$

\[ \forall x \forall y \left( \| (x, y) \|_\infty \leq \| (x, y) \|_2 \leq \sqrt{n} \| (x, y) \|_\infty \right) \]

\[ \forall x \forall y \left( \frac{1}{\sqrt{n}} \| (x, y) \|_2 \leq \| (x, y) \|_\infty \leq \| (x, y) \|_2 \right) \]
Interreducing Norms in Dimension $n$

$\forall x \forall y \left( \| (x, y) \|_\infty \leq \| (x, y) \|_2 \leq \sqrt{n} \| (x, y) \|_\infty \right)

$\forall x \forall y \left( \frac{1}{\sqrt{n}} \| (x, y) \|_2 \leq \| (x, y) \|_\infty \leq \| (x, y) \|_2 \right)$

Benefit from norm relations but be mindful of approximation error factors
1. Learning Objectives

2. Recap: Proofs for Differential Equations

3. Differential Equation Proof Theory
   - Propositional Equivalences
   - Differential Invariants & Arithmetic
   - Differential Structure
   - Differential Invariant Equations
   - Equational Incompleteness
   - Strict Differential Invariant Inequalities
   - Differential Invariant Equations to Differential Invariant Inequalities
   - Differential Invariant Atoms


5. Curves Playing with Norms and Degrees

6. Summary
Rich theory and structure behind differential invariants

Scrutinize what property can be proved with what invariant

Use provability sanity checks like open/closed/univariate

Real differential semialgebraic geometry

Exploit differential cuts to obtain more knowledge
André Platzer.
*Logical Foundations of Cyber-Physical Systems.*
URL: http://www.springer.com/978-3-319-63587-3,
doi:10.1007/978-3-319-63588-0.

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

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

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