13: Differential Invariants & Proof Theory

Logical Foundations of Cyber-Physical Systems

André Platzer

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
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
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

CT
M&C
CPS

Improved analysis
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
Differential Invariant 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

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

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

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

\[
\text{DC} \quad ([x' = f(x) \& Q]F \leftrightarrow [x' = f(x) \& Q \land C]F) \leftrightarrow [x' = f(x) \& Q]C
\]
Differential Invariants for Differential Equations

Differential Weakening

\[ Q \vdash F \]

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

Differential Invariant

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

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

Differential Cut

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

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

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

Differential Weakening

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

Differential Invariant

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

Differential Cut

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

Differential Elimination

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

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

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
Differential Invariant

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

\[ DI_{e=k} \equiv DI_{e=0} \] by considering \((e - k) = 0\)

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

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

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

\(DI_{\Omega}:\) 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
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.

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.

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

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

If $F \iff G$ 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

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

iff

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

Proof.

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

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

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

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

Proof.

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

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

Proof.

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

$F \leftrightarrow G$ 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

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

Proof.

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

\( F \Leftrightarrow G \) propositionally equivalent, so \( (F)' \Leftrightarrow (G)' \) propositionally equivalent since \( (F_1 \land F_2)' \equiv (F_1)' \land (F_2)' \) \ldots

Can use any propositional normal form
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.

Despite 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

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

iff

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

Proof.

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

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

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

iff

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

Proof.

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

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

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

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

Proof.

\[
\frac{\vdash 0 \leq -x \land -x \leq 0}{[\vdash [x' := -x](0 \leq x' \land x' \leq 0)]} \\
\vdash [x' = -x](-5 \leq x \land x \leq 5)
\]
Lemma (Differential invariants and propositional logic)

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

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

iff

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

Proof.

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

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

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

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

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

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

Proof.

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

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

If \( F \leftrightarrow G \) 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.

\[
\begin{align*}
\text{not valid} & \\
\text{\hspace{1cm} } \vdash 0 \leq -x \land -x \leq 0 & \\
\text{\hspace{1cm} } \vdash [x' := -x](0 \leq x' \land x' \leq 0) & \\
\text{\hspace{1cm} } -5 \leq x \land x \leq 5 & \vdash [x' := -x](-5 \leq x \land x \leq 5) & \text{arithmetic equivalence } -5 \leq x \land x \leq 5 \leftrightarrow x^2 \leq 5^2
\end{align*}
\]
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.

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

\[
\begin{align*}
\mathbb{R} & \vdash -x \leq 0 \\
\text{dl} & [x' := -x]2x \Rightarrow 0 \\
x \leq 5^2 & [x' = -x]x^2 \leq 5^2
\end{align*}
\]

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

If $F \iff G$ 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.

Not valid

\[
\begin{align*}
\vdash & 0 \leq -x \land -x \leq 0 \\
\vdash & [x' := -x](0 \leq x' \land x' \leq 0) \\
\vdash & -5 \leq x \land x \leq 5 \\
\vdash & [x' = -x](-5 \leq x \land x \leq 5)
\end{align*}
\]

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 $e = 0$, $e \geq 0$, $e > 0$. 

Andre Platzer (CMU)
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])

\[ DI = DI = \land, \lor \]

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:  \( \mathcal{DI}_\equiv \equiv \mathcal{DI}_{\equiv,\wedge,\lor} \)

Proof core. Full: [6, 2].

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

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

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

### Proof core.

<table>
<thead>
<tr>
<th>Equation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e_1 = e_2 \lor k_1 = k_2 \leftrightarrow (e_1 - e_2)(k_1 - k_2) = 0$</td>
<td>$[x' := f(x)]((e_1)' = (e_2)' \land (k_1)' = (k_2)')$</td>
</tr>
<tr>
<td>$e_1 = e_2 \land k_1 = k_2 \leftrightarrow (e_1 - e_2)^2 + (k_1 - k_2)^2 = 0$</td>
<td></td>
</tr>
</tbody>
</table>
Proposition (Equational deductive power [6, 2])

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

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

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

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

**Proof core.**

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

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

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

**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].

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

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

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

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

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

Proof core. Full: [6, 2].

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

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

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

**Proof core.**

\[ e_1 = e_2 \lor k_1 = k_2 \iff (e_1 - e_2)(k_1 - k_2) = 0 \]

\[ \left[ x' := f(x) \right] ((e_1)' = (e_2)' \wedge (k_1)' = (k_2)') \]

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

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

\[ e_1 = e_2 \land k_1 = k_2 \iff (e_1 - e_2)^2 + (k_1 - k_2)^2 = 0 \]

\[ \left[ x' := f(x) \right] ((e_1)' = (e_2)' \wedge (k_1)' = (k_2)') \]

So \[ \left[ x' := f(x) \right] (((e_1 - e_2)^2 + (k_1 - k_2)^2)'=0) \]

\[ \equiv \left[ x' := f(x) \right] (2(e_1-e_2)((e_1)'-(e_2)') + 2(k_1-k_2)((k_1)'-(k_2)')=0) \]
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) \quad \square
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 $[x' := f(x)](((e_1 - e_2)^2 + (k_1 - k_2)^2)' = 0)$

  $\equiv [x' := f(x)](2(e_1 - e_2)((e_1)' - (e_2)') + 2(k_1 - k_2)((k_1)' - (k_2))' = 0)$
**Proposition (Equational [2])**

\[ \mathcal{DI}= \equiv \mathcal{DI}=,\wedge,\vee \quad \mathcal{DI} \quad \mathcal{DI}\geq \quad \mathcal{DI}= \]

**Proof core.**
Proposition (Equational incompleteness [2])

*Equations are not enough:*

\[ \mathcal{DI}_= \equiv \mathcal{DI}_{=,\land,\lor} < \mathcal{DI} \text{ because } \mathcal{DI}_\geq \not\subseteq \mathcal{DI}_= \]

Proof core.
Equational Incompleteness

Proposition (Equational incompleteness [2])

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

Proof core.

Provable with \( DI_\geq \) Unprovable with \( DI_\leq \)
Equational Incompleteness

Proposition (Equational incompleteness [2])

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

Proof core.
Provable with \( \mathcal{DI}_\geq \)
Unprovable with \( \mathcal{DI}_- \)

\[
dl x \geq 0 \vdash [x'=5]x \geq 0
\]

Andre Platzer (CMU)  LFCPS/13: Differential Invariants & Proof Theory  LFCPS/13 11 / 23
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.

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

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

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

Proposition (Equational incompleteness [2])

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

Proof core.

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

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

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

Proposition (Equational incompleteness [2])

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

Proof core.

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

Unprovable with $\mathcal{DI}_=$

\[
\begin{align*}
\mathbb{R} & \quad \vdash 5 \geq 0 \\
[=] & \quad \vdash [x' := 5]x' \geq 0 \\
\text{dl} & \quad x \geq 0 \vdash [x' = 5]x \geq 0
\end{align*}
\]
Example (Sets Bijective or Not)

1 ⟷ 2 ⟷ 3 ⟷ 4 ⟷ 5 ⟷ 6

a ⟷ b ⟷ c ⟷ d ⟷ e ⟷ f

criterion: cardinality

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

Need an indirect criterion especially if these sets are infinite

Example (Vector Spaces Isomorphic or Not)

$$y \quad y'$$

$$\uparrow \quad \uparrow$$

$$\quad \quad \quad x \quad \quad \quad x'$$
Example (Sets Bijective or Not)

1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6

\begin{align*}
a & \rightarrow b & c & \rightarrow d & e & \rightarrow 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*}
y & \rightarrow y' \\
\uparrow & \uparrow \\
x & \rightarrow x'
\end{align*}
Example (Sets Bijective or Not)

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

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

Need an indirect criterion especially if these sets are infinite

Example (Vector Spaces Isomorphic or Not)

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

\[\text{criterion: dimension } 3 \neq 2\]
Example (Sets Bijective or Not)

\[ 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \]
\[ a \rightarrow b \rightarrow c \rightarrow d \rightarrow e \rightarrow f \]

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)

\[ y \xrightarrow{f} y' \]
\[ x \xrightarrow{g} x' \]
Example (Sets Bijective or Not)

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

|\{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*}
\begin{array}{cccccc}
y & \rightarrow & y' \\
\uparrow & & \uparrow \\
x & \rightarrow & x' \\
\end{array}
\end{align*}
Example (Sets Bijective or Not)

\begin{align*}
1 & \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \\
1 & \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \\
\text{criterion: cardinality } & |\{1, \ldots , 6\}| = 6 \neq |\{a, b, c, d, e\}| = 5
\end{align*}

Need an indirect criterion especially if these sets are infinite

Example (Vector Spaces Isomorphic or Not)
Example (Sets Bijective or Not)

\begin{align*}
1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 & \quad 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \\
\downarrow & \quad \downarrow \\
a \rightarrow b \rightarrow c \rightarrow d \rightarrow e \rightarrow f & \quad a \rightarrow b \rightarrow c \rightarrow d \rightarrow e
\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*}
\begin{array}{c}
\begin{array}{c}
 y \\
\uparrow \\
x
\end{array} & \quad \\
\hline & \\
\begin{array}{c}
 y' \\
\uparrow \\
x'
\end{array}
\end{array}
\end{align*}

criterion: dimension $3 \neq 2$

\begin{align*}
\begin{array}{c}
\begin{array}{c}
y \\
\uparrow \\
x
\end{array} & \quad \\
\hline & \\
\begin{array}{c}
y' \\
\uparrow \\
x'
\end{array}
\end{array}
\end{align*}
Equational Incompleteness

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

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

**Proof core.**

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

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

\[
\begin{array}{c}
\mathbb{R} \quad \star \\
\vdash 5 \geq 0 \\
\land \quad \vdash [x':=5]x' \geq 0 \\
\text{dl} \quad x \geq 0 \vdash [x'=5]x \geq 0
\end{array}
\]
Proposition (Equational incompleteness [2])

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

Proof core.

Provable with $\mathcal{DI} \geq$

Unprovable with $\mathcal{DI}_=$

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

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.

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

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

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

\[
\begin{array}{c}
dl \\
p(x) = 0 \vdash [x' = 5]p(x) = 0 \\
cut, MR \\
x \geq 0 \vdash [x' = 5]x \geq 0
\end{array}
\]
Equational Incompleteness

Proposition (Equational incompleteness [2])

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

Proof core.

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

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

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

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

Proposition (Equational incompleteness [2])

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

Proof core.

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

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

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

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

*Equations are not enough:*

\[ \mathcal{DI}_\equiv \equiv \mathcal{DI}_\equiv,\wedge,\vee \prec \mathcal{DI} \text{ because } \mathcal{DI}_\geq \nmid \mathcal{DI}_\equiv \]

**Proof core.**

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

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

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

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

Univariate polynomial \( p(x) \) is 0 if 0 on all \( x \geq 0 \) \( \square \)
### 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 \( \mathcal{DI} \neq \subseteq \mathcal{DI} > \)*

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

*Strict inequalities are not enough: $\mathcal{DI}_{} > \mathcal{DI}_{}$ because $\mathcal{DI}_{} \not\leq \mathcal{DI}_{} >$

Proof core.

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

Unprovable with $\mathcal{DI}_{}>$
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 $\mathcal{D}I =$

Unprovable with $\mathcal{D}I >$

\[
\frac{d}{dt} v^2 + w^2 = c^2 \vdash [v' = w, w' = -v] v^2 + w^2 = c^2
\]
Proposition (Strict barrier incompleteness)

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

Proof core.

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

\[
\vdash [v':=w][w':=\overline{v}]2vv' + 2ww' = 0
\]

\[
\forall v^2+w^2=c^2 \vdash [v' = w, w' = \overline{v}] v^2+w^2 = c^2
\]

Unprovable with \( \mathcal{DI}> \)

\[
\vdash [v':=w][w':=\overline{v}]2vv' + 2ww' = 0
\]

\[
\forall v^2+w^2=c^2 \vdash [v' = w, w' = \overline{v}] v^2+w^2 = c^2
\]
Proposition (Strict barrier incompleteness)

Strict inequalities are not enough: \( DI_\ast > DI \) because \( DI_\ast \not\leq DI_\ast \)

Proof core.

Provable with \( DI_\ast \)

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

Unprovable with \( DI_\ast \)
Proposition (Strict barrier incompleteness)

\[ \text{Strict inequalities are not enough:} \quad DI > < DI \text{ because } DI = \not< DI > \]

Proof core.

Provable with \( DI = \)

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

Unprovable with \( DI > \)

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

Strict inequalities are not enough: $\text{DI}_> < \text{DI}$ because $\text{DI}_\leq \not\subseteq \text{DI}_>$

Proof core.

Provable with $\text{DI}_\leq$

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

$v^2 + w^2 = c^2$ is a closed set

closed $v^2 + w^2 \leq 1$ with full boundary

closed $v^2 + w^2 \leq 1$ with full boundary

Unprovable with $\text{DI}_>$

$e > 0$ is open set.

open $v^2 + w^2 < 1$ without boundary

open $v^2 + w^2 < 1$ without boundary
Proposition (Strict barrier incompleteness)

Strict inequalities are not enough: $\mathcal{DI}_\triangleright < \mathcal{DI}$ because $\mathcal{DI}_\leq \not\subseteq \mathcal{DI}_\triangleright$

Proof core.

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

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

$v^2 + w^2 = c^2$ is a closed set

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

Open $v^2 + w^2 < 1$ without boundary

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

$e > 0$ is open set.

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

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

**Proof core.**

Provable with $\mathcal{DI}_=^*$

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

$v^2 + w^2 = c^2$ is a closed set

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

Open $v^2 + w^2 < 1$ without boundary

Unprovable with $\mathcal{DI}_>$

$e > 0$ is open set.

Only *true* and *false* are both but don’t help proof
Proposition (Equational)

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

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

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

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

**Proof core.**

Provable with \( DI_{\leq} \) \hspace{1cm} Provable with \( DI_{\geq} \)

\[
\text{d} \overset{\text{ll}}{\Rightarrow} e = 0 \models [x' = f(x) \& Q] e = 0
\]
Proposition (Equational definability)

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

Proof core.

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

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

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

\[
\frac{e = 0 \vdash [x' = f(x) \& Q]e = 0}{\text{dl}}
\]
Proposition (Equational definability)

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

Proof core.

Provable with \( DI_{\leq} \)  Provable with \( DI_{\geq} \)

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

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

Proof core.

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

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

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

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

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

Proof core.

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

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

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

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

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

Proof core.

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

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

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

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

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

Theorem (Atomic)

\[
\text{DI}_\geq, \text{DI}_\geq, \land, \lor \quad \text{and} \quad \text{DI}_>, \text{DI}_>, \land, \lor
\]

Proof idea.

Provable with

\[
\\vdash x' = 5, y' = y^2 (x' \geq 0 \land y' \geq 0)
\]

Unprovable with

\[
\text{DI}_\geq p(x, y) \geq 0 \iff x \geq 0 \land y \geq 0
\]

impossible since this implies

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

so

\[
p(x, 0)
\]

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

\[
\text{dC still possible here but more involved argument separates.}
\]
Theorem (Atomic incompleteness)

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

Proof idea.
Differential Invariant Atoms

**Theorem (Atomic incompleteness)**

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

**Proof idea.**

Provable with \( DI_{\geq, \land, \lor} \)  

Unprovable with \( DI_{>} \)

[2]

Substantial remaining parts of the proof shown elsewhere.
**Theorem (Atomic incompleteness)**

Atomic inequalities not enough: \( DI \geq < DI \geq, \wedge, \lor \) and \( DI \geq < DI \geq, \wedge, \lor \)

**Proof idea.**

Provable with \( DI \geq, \wedge, \lor \)

Unprovable with \( DI \geq \)

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

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

Proof idea.

Provable with $DI_{\geq,\land,\lor}$

- $\forall \mathbb{R} \vdash 5 \geq 0 \land y^2 \geq 0$

$[\vdash [x':=5][y':=y^2](x'\geq 0 \land y'\geq 0)]$

$dl \ x\geq 0 \land y\geq 0 \vdash [x' = 5, y' = y^2](x\geq 0 \land y\geq 0)$

Unprovable with $DI_{\geq} p(x, y)\geq 0 \iff x\geq 0 \land y\geq 0$

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].
Differential Invariant Atoms

**Theorem (Atomic incompleteness)**

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

**Proof idea.**

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

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

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

\[
p(x, y) \geq 0 \iff x \geq 0 \land y \geq 0
\]
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 \( \mathcal{DI}_> < \mathcal{DI}_{>, \land, \lor} \)

Proof idea.

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

\[ \begin{align*}
\text{\( \star \)} & \quad \vdash 5 \geq 0 \land y^2 \geq 0 \\
\text{[=]} & \quad \vdash [x' := 5][y' := y^2](x' \geq 0 \land y' \geq 0) \\
\text{dl} & \quad 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].

dC still possible here but more involved argument separates.
### Theorem (Gentzen’s Cut Elimination) (1935)

\[ A \vdash B \lor C \quad A \land C \vdash B \quad \frac{}{A \vdash B} \]  
*cut can be eliminated*

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

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

\[ DI + DC > DI \]

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

*Deductive power with differential ghosts exceeds power without.*

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

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

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

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

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

\[ \not \text{valid} \]

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

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

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

not valid

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

[:=]

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

\[ \text{dI} \]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Learning Objectives
2. 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
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.

\[
\begin{align*}
0 \leq -x \land -x \leq 0 & \quad \vdash 0 \leq -x \land -x \leq 0 \\
\vdash [x' := -x] (0 \leq x' \land x' \leq 0) & \quad \vdash [x' := -x] (0 \leq x' \land x' \leq 0) \\
(-5 \leq x \land x \leq 5) & \quad \vdash (-5 \leq x \land x \leq 5) \\
\vdash [x' := -x] (-5 \leq x \land x \leq 5) & \quad \vdash [x' := -x] (-5 \leq x \land x \leq 5) \\
\end{align*}
\]

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

Differential structure matters! Higher degree helps here
Curves Playing with Norms and Degrees

\[ dC \]

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

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

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

\[ \| (x, y) \|_2 \overset{\text{def}}{=} x^2 + y^2 \leq t^2 \quad \text{Euclidean norm} \]
Curves Playing with Norms and Degrees

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

\[ \| (x, y) \|_{\infty} \leq t \equiv -t \leq x \leq t \land -t \leq y \leq t \]  
Supremum norm

\[ \| (x, y) \|_2 \leq t \equiv x^2 + y^2 \leq t^2 \]  
Euclidean norm
\[
A \triangleq v^2 + w^2 \leq 1 \land x = y = t = 0
\]

\[
\| (x, y) \|_\infty \leq t \triangleq -t \leq x \leq t \land -t \leq y \leq t
\]

Supremum norm

\[
\| (x, y) \|_2 \leq t \triangleq x^2 + y^2 \leq t^2
\]

Euclidean norm
Curves Playing with Norms and Degrees

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

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

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

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

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

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

\[ \| (x, y) \|_2 \overset{\text{def}}{=} x^2 + y^2 \leq t^2 \quad \text{Euclidean norm} \]
Curves Playing with Norms and Degrees

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

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

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

\[ dC \]
\[ A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1] \| (x, y) \|_{\infty} \leq t \]

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

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

\[ \| (x, y) \|_2 \overset{\text{def}}{=} x^2 + y^2 \leq t^2 \quad \text{Euclidean norm} \]
### Curves Playing with Norms and Degrees

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{R}$</td>
<td>$v^2 + w^2 \leq 1 \vdash -1 \leq v \leq 1 \land -1 \leq w \leq 1$</td>
</tr>
<tr>
<td>$[=]$</td>
<td>$v^2 + w^2 \leq 1 \vdash [x' := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1][-t' \leq x' \leq t' \land -t' \leq y' \leq t']$</td>
</tr>
<tr>
<td>$\triangleleft$</td>
<td>$A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 &amp; v^2 + w^2 \leq 1] | (x, y) |_\infty \leq t$</td>
</tr>
<tr>
<td>$dC$</td>
<td>$A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1] | (x, y) |_\infty \leq t$</td>
</tr>
</tbody>
</table>

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

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

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

\[ \| (x, y) \|_2 \mathrel{\overset{\text{def}}{\leq}} t \mathrel{\overset{\text{def}}{\equiv}} x^2 + y^2 \leq t^2 \quad \text{Euclidean norm} \]
### Curves Playing with Norms and Degrees

<table>
<thead>
<tr>
<th>Domain</th>
<th>Assertion</th>
<th>Invariant</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbb{R} )</td>
<td>( v^2 + w^2 \leq 1 )</td>
<td>(-1 \leq v \leq 1 ) &amp; (-1 \leq w \leq 1 )</td>
<td></td>
</tr>
<tr>
<td>([=] )</td>
<td>( v^2 + w^2 \leq 1 )</td>
<td>([x' := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1](-t' \leq x' \leq t' &amp; -t' \leq y' \leq t') )</td>
<td></td>
</tr>
<tr>
<td>( \mathcal{dI} )</td>
<td>( \diamondsuit )</td>
<td>( A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 &amp; v^2 + w^2 \leq 1] | (x, y) |_\infty \leq t )</td>
<td></td>
</tr>
<tr>
<td>( \mathcal{dC} )</td>
<td></td>
<td>( A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1] | (x, y) |_\infty \leq t )</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain</th>
<th>Assertion</th>
<th>Invariant</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathcal{dI} )</td>
<td>( \diamondsuit )</td>
<td>( A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 &amp; v^2 + w^2 \leq 1] | (x, y) |_2 \leq t )</td>
<td></td>
</tr>
<tr>
<td>( \mathcal{dC} )</td>
<td></td>
<td>( A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1] | (x, y) |_2 \leq t )</td>
<td></td>
</tr>
</tbody>
</table>

\( A \overset{\text{def}}{=} v^2 + w^2 \leq 1 \& x = y = t = 0 \)

\( \| (x, y) \|_\infty \overset{\text{def}}{=} -t \leq x \leq t \& -t \leq y \leq t \) \hspace{2cm} \text{Supremum norm}

\( \| (x, y) \|_2 \overset{\text{def}}{=} x^2 + y^2 \leq t^2 \) \hspace{2cm} \text{Euclidean norm}
Curves Playing with Norms and Degrees

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

\[
\begin{align*}
\vdash v^2 + w^2 \leq 1 & \implies [x' := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1](2x x' + 2y y' \leq 2tt') \\
\text{dI} & \implies A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \land v^2 + w^2 \leq 1] \| (x, y) \|_2 \leq t \\
\text{dC} & \implies A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1] \| (x, y) \|_2 \leq t
\end{align*}
\]

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

\[ \mathbb{R} \]

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

\[ [=] \]

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

\[ dI \]

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

\[ dC \]

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

\[ \mathbb{R} \]

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

\[ [=] \]

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

\[ dI \]

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

\[ dC \]

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

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

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

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

not valid
\[
\begin{align*}
\mathbb{R} & \quad v^2 + w^2 \leq 1 \vdash 2xv + 2yw \leq 2t1 \\
[=] & \quad v^2 + w^2 \leq 1 \vdash [x' := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1](2xx' + 2yy' \leq 2tt') \\
\triangleleft & \quad A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \land v^2 + w^2 \leq 1]\| (x, y) \|_2 \leq t \\
dC & \quad A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1]\| (x, y) \|_2 \leq t
\end{align*}
\]

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

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

\[
\| (x, y) \|_2 \overset{\text{def}}{=} x^2 + y^2 \leq t^2 \quad \text{Euclidean norm}
\]
Curves Playing with Norms and Degrees

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

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

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

\[ A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1][(x, y)]_{\infty} \leq t \]

Lower degree helps here

\[ v^2 + w^2 \leq 1 \vdash 2xv + 2yw \leq 2t' \]

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

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

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

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

\[ [(x, y)]_{2} \equiv x^2 + y^2 \leq t^2 \quad \text{Euclidean norm} \]
Interreducing Norms in Dimension $n$

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

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

∀x ∀y (\frac{1}{\sqrt{n}}\|(x, y)\|_2 \leq \|(x, y)\|_\infty \leq \|(x, y)\|_2)
∀x ∀y (‖(x, y)‖_∞ ≤ ‖(x, y)‖_2 ≤ √n‖(x, y)‖_∞)
∀x ∀y (\frac{1}{\sqrt{n}}‖(x, y)‖_2 ≤ ‖(x, y)‖_∞ ≤ ‖(x, y)‖_2)
Interreducing Norms in Dimension $n$

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

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

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

André Platzer (CMU)
Summary: Differential Invariance Chart

Theorem (Differential Invariance Chart)

- 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.