13: Differential Invariants & Proof Theory
15-424: Foundations of Cyber-Physical Systems

André Platzer

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

1 Learning Objectives
2 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
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
- 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

none
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 Invariants for Differential Equations

#### Differential Weakening

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

#### Differential Invariant

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

#### Differential Cut

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

\[
\text{DW } [\dot{x} = f(x) \land Q]F \leftrightarrow [\dot{x} = f(x) \land Q](Q \rightarrow F)
\]

\[
\text{DI } [\dot{x} = f(x) \land Q]F \leftarrow (Q \rightarrow F \land [\dot{x} = f(x) \land Q](F)')
\]

\[
\text{DC } ([\dot{x} = f(x) \land Q]F \leftrightarrow [\dot{x} = f(x) \land Q \land C]F) \leftarrow [\dot{x} = f(x) \land Q]C
\]

\[
\text{DE } [\dot{x} = f(x) \land Q]F \leftrightarrow [\dot{x} = f(x) \land Q][\dot{x} := f(x)]F
\]
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:

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

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
Relativity Theory of Proofs

### Differential Invariant

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

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

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

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

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

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

\( \mathcal{D}I_{\Omega} \): 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
Propositional Equivalences of Differential Invariants

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.

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

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

iff

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

Proof.

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

Can use any propositional normal form
Propositional Equivalences of Differential Invariants

Lemma (Differential invariants and propositional logic)

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

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

Proof.

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

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.

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

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

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

Proof.

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

\( F \leftrightarrow G \) 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

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

iff

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

Proof.

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

$F \leftrightarrow G$ propositionally equivalent, so

\[
(F)' \leftrightarrow (G)' \text{ propositionally equivalent since } (F_1 \land F_2)' \equiv (F_1)' \land (F_2)' \ldots
\]

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.
Lemma (Differential invariants and propositional logic)

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

\begin{align*}
F \text{ differential invariant of } x' &= f(x) \land Q \\
\text{iff } G \text{ differential invariant of } x' &= f(x) \land Q
\end{align*}

Proof.

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

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

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

iff

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

Proof.

\[
\left[ x' := -x \right] (0 \leq x' \land x' \leq 0) \\
\downarrow \\
-5 \leq x \land x \leq 5 \vdash [x' = -x] (-5 \leq x \land x \leq 5)
\]
Lemma (Differential invariants and propositional logic)

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

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

iff

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

Proof.

\[
\vdash 0 \leq -x \land -x \leq 0
\]

\[
\vdash [x' := -x] (0 \leq x' \land x' \leq 0)
\]

\[
\vdash -5 \leq x \land x \leq 5 \vdash [x' = -x] (-5 \leq x \land x \leq 5)
\]
### 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>Step</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>not valid</td>
</tr>
<tr>
<td>2</td>
<td>$\vdash 0 \leq -x \land -x \leq 0$</td>
</tr>
<tr>
<td>3</td>
<td>$[\cdot :=] \vdash [x' := -x](0 \leq x' \land x' \leq 0)$</td>
</tr>
<tr>
<td>4</td>
<td>$\text{dl} \vdash -5 \leq x \land x \leq 5 \vdash [x' = -x](-5 \leq x \land x \leq 5)$</td>
</tr>
</tbody>
</table>
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.

\[
\begin{align*}
\text{not valid} \\
\not\vdash 0 \leq -x \land -x \leq 0
\end{align*}
\]

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

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

\[
\begin{align*}
dl \quad x^2 \leq 5^2 \vdash [x' = -x]x^2 \leq 5^2
\end{align*}
\]

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

If $F \leftrightarrow G$ 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.

not valid

\[ \vdash 0 \leq -x \land -x \leq 0 \]

\[ ['=] \vdash [x' := -x](0 \leq x' \land x' \leq 0) \]

\[ dl \vdash -5 \leq x \land x \leq 5 \vdash [x' = -x](-5 \leq x \land x \leq 5) \]

\[ ['=] \vdash [x' := -x]2xx' \leq 0 \]

\[ dl \vdash x^2 \leq 5^2 \vdash [x' = -x]x^2 \leq 5^2 \]

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.

\[
\begin{array}{c}
\text{not valid} \\
\text{\quad \hspace{2em} valid}
\end{array}
\]

\[\text{\quad \hspace{2em} valid} \]

\[\text{\quad \hspace{2em} valid} \]

\[\text{\quad \hspace{2em} valid} \]

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.

Not valid

$\vdash 0 \leq -x \land -x \leq 0$

$\vdash [x' := -x](0 \leq x' \land x' \leq 0)$

$\vdash [x' = -x](-5 \leq x \land x \leq 5)$

$\vdash -x^2 \leq 0$

$\vdash [x' := -x]2xx' \leq 0$

$\vdash x^2 \leq 5^2$

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.

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

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

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

Differential structure matters! Higher degree helps here
Different Differential Structure for Equivalent Solutions $\geq 0$
Can still normalize atomic formulas to $e = 0, e \geq 0, e > 0$
Proposition (Equational deductive power [5, 1])

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

Proof core.

- 

Generalizations see [5, 1]
Proposition (Equational deductive power [5, 1])

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

Proof core.

Generalizations see [5, 1]
Differential Invariant Equations

Proposition (Equational deductive power [5, 1])

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

Proof core.

\( e_1 = e_2 \lor k_1 = k_2 \)

\( e_1 = e_2 \land k_1 = k_2 \)

Generalizations see [5, 1]
Proposition (Equational deductive power [5, 1])

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

Proof core.

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

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

Generalizations see [5, 1]
Proposition (Equational deductive power \([5, 1]\))

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

Proof core.

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

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

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

Generalizations see \([5, 1]\)
Proposition (Equational deductive power \([5, 1]\))

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

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

Generalizations see \([5, 1]\)
Proposition (Equational deductive power [5, 1])

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

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

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

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

Generalizations see [5, 1]
Differential Invariant Equations

Proposition (Equational deductive power [5, 1])

atomic equations are enough: \( DI_\equiv \equiv DI_\equiv, \land, \lor \)

Proof core.

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

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

Generalizations see [5, 1]
Proposition (Equational deductive power [5, 1])

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

Proof core.

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

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

Generalizations see [5, 1]
Proposition (Equational deductive power [5, 1])

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

Proof core.

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

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

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

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

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

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

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

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

Generalizations see [5, 1]
Proposition (Equational deductive power [5, 1])

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

Proof core.

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

2. \( e_1 = e_2 \land k_1 = k_2 \iff (e_1 - e_2)^2 + (k_1 - k_2)^2 = 0 \)
   
   \[ [x'=f(x)]((e_1)' = (e_2)' \wedge (k_1)' = (k_2)') \]
   
   So \([x'=f(x)](((e_1 - e_2)^2 + (k_1 - k_2)^2)'=0 \)
   
   \( \equiv [x'=f(x)](2(e_1-e_2)((e_1)'-(e_2)') + 2(k_1-k_2)((k_1)'-(k_2)')=0) \)

Generalizations see [5, 1]
Proposition (Equational deductive power [5, 1])

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

Proof core.

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

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

Generalizations see [5, 1]
Equational

**Proposition (Equational)**

\[
DI_\leq \equiv DI_{\leq,\wedge,\vee} \quad DI \quad DI_{\geq} \quad DI_\leq
\]

**Proof core.**

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

Likewise for indirect proofs [1].

[1] Andrés Platzer (CMU)
**Equational Incompleteness**

**Proposition (Equational incompleteness [1])**

*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 [1])

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

Proof core.
Provable with \( DI_\geq \)  Unprovable with \( DI_\equiv \)
# Equational Incompleteness

## Proposition (Equational incompleteness [1])

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

## Proof core.

<table>
<thead>
<tr>
<th>Provable with</th>
<th>Unprovable with</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathcal{DI}_{\geq} )</td>
<td>( \mathcal{DI}_{=} )</td>
</tr>
</tbody>
</table>

- Proof: \( x \geq 0 \vdash [x' = 5]x \geq 0 \)
Proposition (Equational incompleteness [1])

Equations are not enough: \( DI_\leq \equiv DI_\leq,\land,\lor < DI \) because \( DI_\geq \nless DI_\leq \)

Proof core.
Provable with \( DI_\geq \) Unprovable with \( DI_\leq \)

\[ ['=] \quad \vdash [x'=5]x' \geq 0 \]
\[ dl \quad \vdash x \geq 0 \quad \vdash [x'=5]x \geq 0 \]
Equational Incompleteness

Proposition (Equational incompleteness [1])

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

Proof core.

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

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

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

Proposition (Equational incompleteness [1])

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

Proof core.
Provable with \(\mathcal{DI}_\geq\) \hspace{1cm} Unprovable with \(\mathcal{DI}_=\)

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

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

Example (Vector Spaces Isomorphic or Not)

\[
\begin{align*}
y & \quad y' \\
\downarrow & \quad \downarrow \\
x & \quad x'
\end{align*}
\]
Example (Sets Bijective or Not)

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

Example (Vector Spaces Isomorphic or Not)

\[\begin{align*}
y & \rightarrow x \\
y' & \rightarrow x'
\end{align*}\]
Example (Sets Bijective or Not)

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

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

Example (Vector Spaces Isomorphic or Not)

y
\uparrow
y'
\uparrow
\rightarrow x
\rightarrow x'

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

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

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

Need an indirect criterion especially if these sets are infinite

Example (Vector Spaces Isomorphic or Not)

\[
\begin{align*}
y &\quad &y' \\
\uparrow &\quad &\uparrow \\
x &\rightarrow &x'
\end{align*}
\]
Proving Differences in Set Theory & Linear Algebra

Example (Sets Bijective or Not)

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

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

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

Need an indirect criterion especially if these sets are infinite

Example (Vector Spaces Isomorphic or Not)

\[ \begin{align*}
y & \rightarrow y' \\
& \uparrow \\
& x \quad \rightarrow \quad x' \\
\end{align*} \]
Example (Sets Bijective or Not)

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

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

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)

\[ x \rightarrow y \rightarrow x' \]
\[ y' \rightarrow y \rightarrow x' \]

\[ x' \rightarrow z \rightarrow x \]
\[ y' \rightarrow y \rightarrow x' \]
Example (Sets Bijective or Not)

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

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

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)

\[
\begin{align*}
\text{dimension } 3 & \neq 2
\end{align*}
\]
Equational Incompleteness

**Proposition (Equational incompleteness [1])**

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

**Proof core.**

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

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

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

Proposition (Equational incompleteness [1])

*Equations are not enough:* \( \mathcal{D}I_\leq \equiv \mathcal{D}I_\leq,\land,\lor < \mathcal{D}I \) because \( \mathcal{D}I_\geq \not\leq \mathcal{D}I_\leq \)

Proof core.

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

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

Unprovable with \( \mathcal{D}I_\leq \)

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

Proposition (Equational incompleteness [1])

Equations are not enough: \( DI_= \equiv DI_=,\land,\lor \prec DI \) because \( DI_\geq \not\subseteq DI_= \)

Proof core.

Provable with \( DI_\geq \)  

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

Unprovable with \( DI_= \)  

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

Proposition (Equational incompleteness [1])

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

Proof core.

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

\[
\begin{array}{ccc}
\mathbb{R} & \vdash & 5 \geq 0 \\
\begin{array}{c}
\vdash \lbrack x' := 5 \rbrack x' \geq 0 \\
\vdash x \geq 0 \vdash \lbrack x' = 5 \rbrack x \geq 0
\end{array}
\end{array}
\]

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

\[
\begin{align*}
\vdash \lbrack x' := 5 \rbrack (p(x))' &= 0 \\
p(x) &= 0 \vdash \lbrack x' = 5 \rbrack p(x) = 0 \\
x \geq 0 &\vdash \lbrack x' = 5 \rbrack x \geq 0
\end{align*}
\]

\[\text{cut, MR}\]
Equational Incompleteness

Proposition (Equational incompleteness [1])

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

Proof core.

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

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

Unprovable with $\mathcal{DI}_=$

\[\begin{array}{c}
???
\vdash [x':=5](p(x))' = 0 \\
p(x) = 0 \vdash [x' = 5]p(x) = 0 \\
x \geq 0 \vdash [x' = 5]x \geq 0
\end{array}\]
Equational Incompleteness

Proposition (Equational incompleteness [1])

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

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

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

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

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

Univariate polynomial \( p(x) \) is 0 if 0 on all \( x \geq 0 \)
Equational Incompleteness

Proposition (Equational incompleteness [1])

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

Proof core.

Provable with \( DI_\geq \)

Unprovable with \( DI_\leq \)

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

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

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

Likewise for indirect proofs [1].
Proposition (Strict barrier incompleteness)

Strict inequalities are not enough:

\[ DI_\succ DI = \not\leq DI_\succ \]

Proof core.

Unprovable with \( DI \succ e \succ 0 \) is open set.

Likewise for indirect proofs [1].

\[ v^2 + w^2 \leq 1 \] with boundary

\[ v^2 + w^2 < 1 \] without boundary
Proposition (Strict barrier incompleteness)

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

Proof core.
Strict Inequality Incompleteness

Proposition (Strict barrier incompleteness)

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

Proof core.

Provable with \( DI_\leq \)

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

Strict inequalities are not enough: \( DI_\triangleright < DI \) because \( DI_\models \not\subseteq DI_\triangleright \)

Proof core.
Provable with \( DI_\models \)

Unprovable with \( DI_\triangleright \)

\[
dl \quad \nu^2 + w^2 = c^2 \vdash [\nu' = w, w' = -\nu] \nu^2 + w^2 = c^2
\]
Proposition (Strict barrier incompleteness)

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

Proof core.

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

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

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

\[
\vdash [v' = w, w' = -v]v^2 + w^2 = c^2
\]

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

\[
\vdash [v' = w, w' = -v]v^2 + w^2 = c^2
\]
**Strict Inequality Incompleteness**

**Proposition (Strict barrier incompleteness)**

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

**Proof core.**

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

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

Strict inequalities are not enough: \( DI_\succ < DI \) because \( DI_\preceq \nsubseteq DI_\succ \)

Proof core.

Provable with \( DI_\preceq \)

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

Unprovable with \( DI_\succ \)
**Proposition (Strict barrier incompleteness)**

*Strict inequalities are not enough:* \( \mathcal{DI}_\succ < \mathcal{DI} \) because \( \mathcal{DI}_\preceq \not\subseteq \mathcal{DI}_\succ \)

**Proof core.**

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

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

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

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

\( e > 0 \) is open set.

closed \( v^2 + w^2 \preceq 1 \) with boundary

open \( v^2 + w^2 < 1 \) without boundary
Strict Inequality Incompleteness

**Proposition (Strict barrier incompleteness)**

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

**Proof core.**

Provable with \( DI_\leq \)

\[
\begin{align*}
\mathbb{R} & \vdash 2vw + 2w(-v) = 0 \\
\left[\begin{array}{c}
\mathcal{P} \\
\mathcal{Q}
\end{array}\right] & \vdash [v' := w][w' := -v]2vv' + 2ww' = 0
\end{align*}
\]

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

Unprovable with \( DI_\succ \)

e > 0 is open set.

Only *true* and *false* are both

André Platzer (CMU)

FCPS / 13: Differential Invariants & Proof Theory

14 / 23
Proposition (Strict barrier incompleteness)

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

Proof core.

Provable with $\mathcal{DI}_=$

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

Unprovable with $\mathcal{DI}_>$

e > 0 is open set.

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

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

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

open $v^2 + w^2 < 1$ without boundary
Strict Inequality Incompleteness

Proposition (Strict barrier incompleteness)

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

Proof core.

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

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

\( v^2 + w^2 = c^2 \) is a closed set
Likewise for indirect proofs [1].

Unprovable with \( \mathcal{DI}_\succ \)
e > 0 is open set.
Only true and false are both but don’t help proof.

\[
\begin{align*}
\text{closed } v^2 + w^2 \leq 1 \\
\text{with boundary} \\
\text{open } v^2 + w^2 < 1 \\
\text{without boundary}
\end{align*}
\]
Proposition (Equational)

\[ DI_{=} \land, \lor \quad DI_{\geq} \]

Proof core.
Proposition (Equational definability)

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

Proof core.
Proposition (Equational definability)

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

Proof core.
Provable with \( DI_{=\equiv} \)  Provable with \( DI_{\geq} \)
Proposition (Equational definability)

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

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

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

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

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

Proof core.

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

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

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

Likewise for indirect proofs \[1\]. Local view of logic is crucial for this proof.
Proposition (Equational definability)

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

Proof core.

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

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

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

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

Proof core.

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

\[
\frac{\ast}{\mathcal{dl} \quad Q \models [x' := f(x)](e)' = 0}
\]

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

\[
\frac{\mathcal{dl} \quad e = 0 \models [x' = f(x) \& Q]e = 0}{\mathcal{dl} \quad -e^2 \geq 0 \models [x' = f(x) \& Q](-e^2 \geq 0)}
\]
**Proposition (Equational definability)**

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

**Proof core.**

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

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

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

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

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

Proof core.

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

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

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

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

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

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

Likewise for indirect proofs [1].

Local view of logic is crucial for this proof.
Degree increases
**Theorem (Atomic)**

\[ DI_\geq, DI_{\geq,\wedge,\vee}, \text{and } DI_{>}, DI_{>,\wedge,\vee} \]

**Proof idea.**

Provable with

\[ DI_\geq, \wedge, \vee \vdash 5 \geq 0 \land y^2 \geq 0 \]

\[ x' := 5, y' := y^2 \]

\[ x' \geq 0 \land y' \geq 0 \]

Unprovable with

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

impossible since this implies

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

so

\[ p(x, 0) = 0 \]

Substantial remaining parts of the proof shown elsewhere [1].
Theorem (Atomic incompleteness)

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

Proof idea.
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 $\mathcal{DI} \geq, \land, \lor$

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

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

**Proof idea.**

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

Unprovable with \( DI_\geq \)

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

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

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

\[
\begin{align*}
* & \quad \vdash 5 \geq 0 \wedge y^2 \geq 0 \\
\mathbb{R} & \quad \vdash [x':=5][y':=y^2](x'\geq0\wedge y'\geq0) \\
[':=] & \quad \vdash [x' = 5, y' = y^2](x \geq 0 \wedge y \geq 0)
\end{align*}
\]

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

\( p(x, y) \geq 0 \leftrightarrow x \geq 0 \wedge y \geq 0 \)
impossible since this implies \( p(x, 0) \geq 0 \leftrightarrow x \geq 0 \)
so \( p(x, 0) \) is 0
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 \( \mathcal{DI}_{\geq,\land,\lor} \)

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

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 [1].
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 $DI_{\geq,\land,\lor}$

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

Unprovable with $DI_{\geq}$ $p(x, y)\geq 0 \iff x\geq 0 \land y\geq 0$ 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 [1].

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)

\[
A \vdash B \lor C \quad A \land C \vdash B \\
\hline
A \vdash B
\]

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.
\[
DI + DC + DG > DI + DC
\]
\[
dl x^3 \geq -1 \land y^5 \geq 0 \vdash [x' = (x - 2)^4 + y^5, y' = y^2] x^3 \geq -1
\]
Ex: The Need for Differential Cuts

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

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

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

\[ [\!:=\!] \]

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

\[ \text{dl} \]

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

not valid

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

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

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

not valid

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

\[ \left[ \begin{array}{l}
' := \\
\end{array} \right. \]

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

\[ \downarrow \]

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

Have to know something about $y^5$
Ex: **Differential Cuts**

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

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

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

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

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

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

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

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

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

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

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

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

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

* 

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

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

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

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

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

\[ * \]

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

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

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

Proof.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

\[ \text{Supremum norm} \]

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

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

\[ * \]
\[ \mathbb{R} \]
\[ v^2 + w^2 \leq 1 \vdash -1 \leq v \leq 1 \land -1 \leq w \leq 1 \]

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

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

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

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

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

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

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

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

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

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

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

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

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

\[
\begin{align*}
\mathbb{R} &
\begin{aligned}
\nu^2 + \omega^2 &\leq 1 \vdash -1 \leq \nu \leq 1 \land -1 \leq \omega \leq 1 \\
[':=] &
\begin{aligned}
\nu^2 + \omega^2 &\leq 1 \vdash [x' := \nu][y' := \omega][\nu' := \omega \nu][\omega' := -\nu \nu][t' := 1](-t' \leq x' \leq t' \land -t' \leq y' \leq t')
\end{aligned}
\end{aligned}
\end{align*}
\]

\[
\begin{align*}
dl &
\begin{aligned}
\langle &
\begin{aligned}
\mathcal{A} &\vdash [x' = \nu, y' = \omega, \nu' = \omega \nu, \omega' = -\nu \nu, t' = 1 \land \nu^2 + \omega^2 \leq 1] \|(x, y)\|_\infty \leq t
\end{aligned}
\end{aligned}
\end{aligned}
\end{align*}
\]

\[
\begin{align*}
dl &
\begin{aligned}
\langle &
\begin{aligned}
\mathcal{A} &\vdash [x' = \nu, y' = \omega, \nu' = \omega \nu, \omega' = -\nu \nu, t' = 1] \|(x, y)\|_2 \leq t
\end{aligned}
\end{aligned}
\end{aligned}
\end{align*}
\]

\[
\begin{align*}
A &\overset{\text{def}}{=} \nu^2 + \omega^2 \leq 1 \land \nu = \omega = t = 0
\end{align*}
\]

\[
\begin{align*}
\|(x, y)\|_\infty &\overset{\text{def}}{=} -t \leq x \leq t \land -t \leq y \leq t & \text{Supremum norm}
\end{align*}
\]

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

| \( \mathbb{R} \) | \( v^2 + w^2 \leq 1 \vdash [x' := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1](2xx' + 2yy' \leq 2tt') \) |
| \( \triangleright \) | \( A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \& v^2 + w^2 \leq 1] \| (x, y) \|_2 \leq t \) |
| \( \text{DC} \) | \( A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1] \| (x, y) \|_2 \leq t \) |

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

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

\[
\| (x, y) \|_2 \overset{\text{def}}{=} x^2 + y^2 \leq t^2
\quad \text{Euclidean norm}
\]
$\mathbb{R}$

$\nu^2 + w^2 \leq 1 \vdash -1 \leq \nu \leq 1 \land -1 \leq w \leq 1$

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

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

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

$\nu^2 + w^2 \leq 1 \vdash 2xw + 2yw \leq 2t$

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

$\triangleleft A \vdash [x' = \nu, y' = w, \nu' = \omega w, w' = -\omega \nu, t' = 1 \& \nu^2 + w^2 \leq 1] \|(x, y)\|_{2} \leq t$

$A \vdash [x' = \nu, y' = w, \nu' = \omega w, w' = -\omega \nu, t' = 1] \|(x, y)\|_{2} \leq t$

$A \overset{\text{def}}{=} \nu^2 + w^2 \leq 1 \land x = y = t = 0$

$\|(x, y)\|_{\infty} \overset{\text{def}}{=} -t \leq x \leq t \land -t \leq y \leq t$ \hspace{1cm} Supremum norm

$\|(x, y)\|_{2} \overset{\text{def}}{=} x^2 + y^2 \leq t^2$ \hspace{1cm} Euclidean norm
Curves Playing with Norms and Degrees

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

\[ \text{not valid} \]
\[ v^2 + w^2 \leq 1 \vdash 2xv + 2yw \leq 2t \]
\[ \mathbb{R}' := \]
\[ v^2 + w^2 \leq 1 \vdash [x' := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1] (2xx' + 2yy' \leq 2tt') \]
\[ \text{dl} \]
\[ A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1 \& v^2 + w^2 \leq 1] \|(x, y)\|_2 \leq t \]
\[ \text{DC} \]
\[ A \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v, t' = 1] \|(x, y)\|_2 \leq t \]

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

<table>
<thead>
<tr>
<th>[ R ]</th>
<th>[ [':=] ]</th>
<th>[ dl ]</th>
<th>[ DC ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ v^2 + w^2 \leq 1 ]</td>
<td>[ [v'] := v][y' := w][v' := \omega w][w' := -\omega v][t' := 1](-t' \leq x' \leq t' \land -t' \leq y' \leq t') ]</td>
<td>[ 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 ]</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>

not valid

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

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

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

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

Lower degree helps here
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 $n$

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

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

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

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

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
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.

André Platzer.
Foundations of cyber-physical systems.

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

André Platzer.
A differential operator approach to equational differential invariants.
André Platzer.
Differential-algebraic dynamic logic for differential-algebraic programs. 