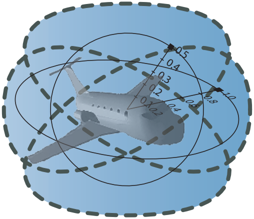
15-819/18-879: Hybrid Systems Analysis & Theorem Proving

12: Differential-algebraic Dynamic Logic & Differential Induction

André Platzer

aplatzer@cs.cmu.edu
Carnegie Mellon University, Pittsburgh, PA



Outline

1. Verification Calculus for Differential-algebraic Dynamic Logic d$\mathcal{L}$
    - Motivation for Differential Induction
    - Derivations and Differentiation
    - Differential Induction
    - Motivation for Differential Saturation
    - Differential Variants
    - Compositional Verification Calculus
    - Differential Transformation
    - Differential Reduction & Differential Elimination
    - Proof Rules
2. Soundness
3. Restricting Differential Invariants
4. Deductive Power

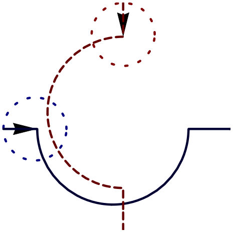
Outline

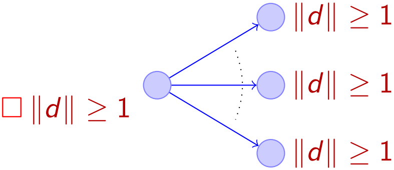
1. Verification Calculus for Differential-algebraic Dynamic Logic d$\mathcal{L}$
   - Motivation for Differential Induction
   - Derivations and Differentiation
   - Differential Induction
   - Motivation for Differential Saturation
   - Differential Variants
   - Compositional Verification Calculus
   - Differential Transformation
   - Differential Reduction & Differential Elimination
   - Proof Rules
2. Soundness
3. Restricting Differential Invariants
4. Deductive Power

Differential-algebraic Dynamic Logic

differential-algebraic dynamic logic

$$\mathrm{DAL} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{ML}$$





$\Box \|d\| \geq 1$

$\|d\| \geq 1$

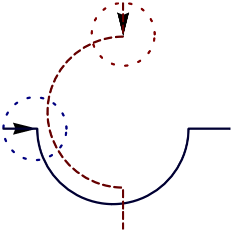
$\|d\| \geq 1$

$\|d\| \geq 1$

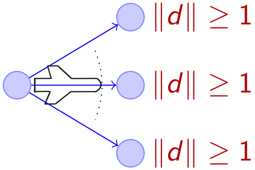
Differential-algebraic Dynamic Logic

differential-algebraic dynamic logic

$$\mathrm{DAL} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL}$$



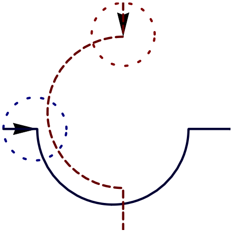
$[✈]\ \|d\| \geq 1$



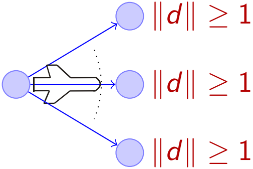
Differential-algebraic Dynamic Logic

differential-algebraic dynamic logic

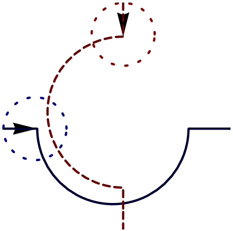
$$\mathrm{DAL} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL} + \mathrm{DAP}$$



$$[d_1' \leq -\omega d_2 \wedge d_2' \leq \omega d_1 \vee d_1' \leq 4]\, \|d\| \geq 1$$



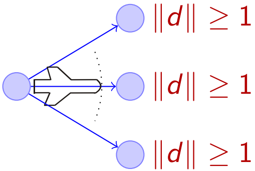
Differential-algebraic Dynamic Logic



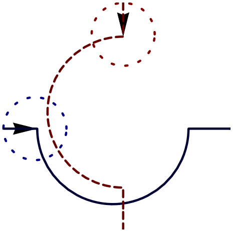
differential-algebraic dynamic logic

$$\mathsf{DAL} = \mathsf{FOL}_{\mathbb{R}} + \mathsf{DL} + \mathsf{DAP}$$

$$[d_1 := -d_2;\ d_1' \leq -\omega d_2 \wedge d_2' \leq \omega d_1 \vee d_1' \leq 4]\,\|d\| \geq 1$$



Differential-algebraic Dynamic Logic



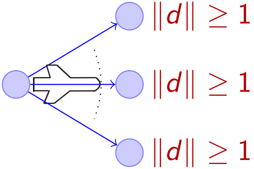
differential-algebraic dynamic logic

$$\mathrm{DAL} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL} + \mathrm{DAP}$$

$$[\underbrace{d_1 := -d_2;\ d_1' \le -\omega d_2 \land d_2' \le \omega d_1 \lor d_1' \le 4}_{\text{differential-algebraic program}}]\,\|d\| \ge 1$$

= first-order completion of

hybrid programs



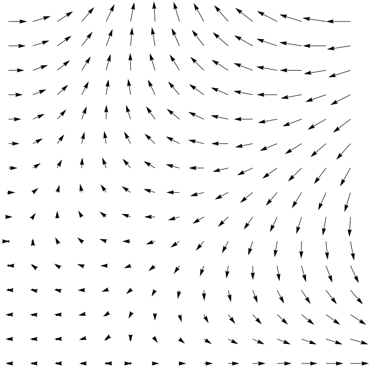
Outline

1. Verification Calculus for Differential-algebraic Dynamic Logic d$\mathcal{L}$
   - Motivation for Differential Induction
   - Derivations and Differentiation
   - Differential Induction
   - Motivation for Differential Saturation
   - Differential Variants
   - Compositional Verification Calculus
   - Differential Transformation
   - Differential Reduction & Differential Elimination
   - Proof Rules
2. Soundness
3. Restricting Differential Invariants
4. Deductive Power

Idea: Exploit Vector Field of Differential Equations

"Definition" (Differential Invariant)

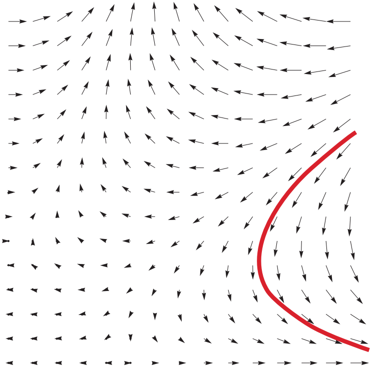
"Property that remains true in the direction of the dynamics"



Idea: Exploit Vector Field of Differential Equations

"Definition" (Differential Invariant)

"Property that remains true in the direction of the dynamics"



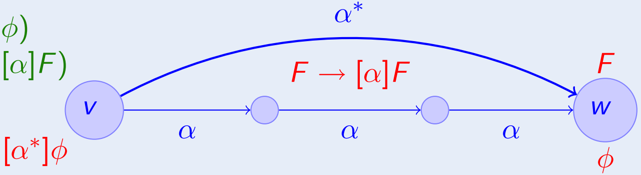
Verification by Discrete and Differential Induction

Definition (Discrete Invariant F)

F

$\forall^\alpha(F \rightarrow \phi)$

$\forall^\alpha(F \rightarrow [\alpha]F)$



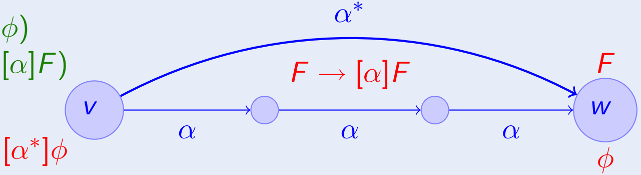
Verification by Discrete and Differential Induction

Definition (Discrete Invariant F)

F

$\forall^{\alpha}(F \rightarrow \phi)$

$\forall^{\alpha}(F \rightarrow [\alpha]F)$

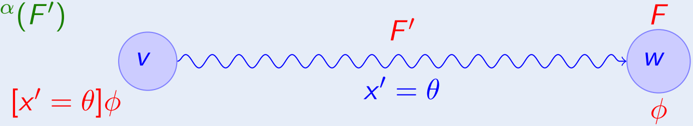


Definition (Differential Invariant F)

F

$\forall^{\alpha}(F \rightarrow \phi)$

$\forall^{\alpha}(F')$



Differential Induction: Local Dynamics w/o Solutions

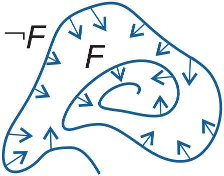
Definition (Differential Invariant)

F closed under total differentiation with respect to differential constraints

Differential Induction: Local Dynamics w/o Solutions

Definition (Differential Invariant)

F closed under total differentiation with respect to differential constraints

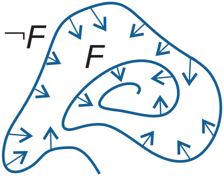


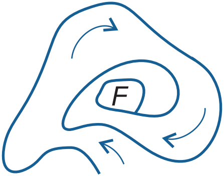
$$\frac{\vdash \forall^\alpha(\chi \to F')}{\chi \to F \vdash [x' = \theta \land \chi]F}$$

Differential Induction: Local Dynamics w/o Solutions

Definition (Differential Invariant)

F closed under total differentiation with respect to differential constraints





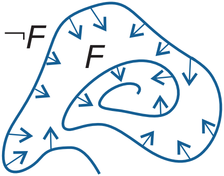
$$\frac{\vdash \forall^\alpha(\chi \rightarrow F')}{\chi \rightarrow F \vdash [x' = \theta \land \chi]F}$$

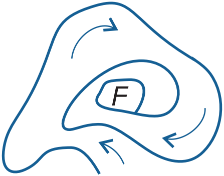
$$\frac{\vdash \forall^\alpha(\neg F \land \chi \rightarrow F'_{\gg})}{[x' = \theta \land \neg F]\chi \vdash \langle x' = \theta \land \chi\rangle F}$$

Differential Induction: Local Dynamics w/o Solutions

Definition (Differential Invariant)

F closed under total differentiation with respect to differential constraints





$$\frac{\vdash \forall^{\alpha}(\chi \rightarrow F')}{\chi \rightarrow F \vdash [x' = \theta \wedge \chi]F}$$

$$\frac{\vdash \forall^{\alpha}(\neg F \wedge \chi \rightarrow F'_{\gg})}{[x' = \theta \wedge \neg F]\chi \vdash \langle x' = \theta \wedge \chi \rangle F}$$

Total differential F' of *formulas*?

Outline

1. Verification Calculus for Differential-algebraic Dynamic Logic d$\mathcal{L}$
   - Motivation for Differential Induction
   - Derivations and Differentiation
   - Differential Induction
   - Motivation for Differential Saturation
   - Differential Variants
   - Compositional Verification Calculus
   - Differential Transformation
   - Differential Reduction & Differential Elimination
   - Proof Rules
2. Soundness
3. Restricting Differential Invariants
4. Deductive Power

Goal for Differential Induction Principle

$$\sigma_1 \quad \mapsto \quad [\![F]\!]_{\sigma_1}$$

Goal for Differential Induction Principle

$$\begin{array}{lcl} \sigma_1 & \mapsto & [\![F]\!]_{\sigma_1} \\ \sigma_2 & \mapsto & [\![F]\!]_{\sigma_2} \end{array}$$

Goal for Differential Induction Principle

$$\begin{array}{ccc}\sigma_1 & \mapsto & [\![F]\!]_{\sigma_1} \\ \sigma_2 & \mapsto & [\![F]\!]_{\sigma_2}\end{array}$$

In the limit:

$$\frac{\mathrm{d}\,[\![F]\!]_{\sigma}}{\mathrm{d}\sigma}$$

Goal for Differential Induction Principle

$$\begin{array}{ccc} \sigma_1 & \mapsto & [\![F]\!]_{\sigma_1} \\ \sigma_2 & \mapsto & [\![F]\!]_{\sigma_2} \end{array}$$

In the limit:

$$\frac{\mathrm{d}\,[\![F]\!]_{\sigma(t)}}{\mathrm{d}t}$$

where $\frac{\mathrm{d}\sigma(t)}{\mathrm{d}t}$ is according to ODE

Goal for Differential Induction Principle

$$\begin{array}{ccc}\sigma_1 & \mapsto & [\![F]\!]_{\sigma_1} \\ \sigma_2 & \mapsto & [\![F]\!]_{\sigma_2}\end{array}$$

In the limit:

$$\frac{\mathrm{d}\,[\![F]\!]_{\sigma(t)}}{\mathrm{d}t}(\zeta) = [\![F']\!]_{\bar{\sigma}(\zeta)}$$

where $\frac{\mathrm{d}\sigma(t)}{\mathrm{d}t}$ is according to ODE

Goal for Differential Induction Principle

$$\begin{aligned} \sigma_1 &\mapsto [\![F]\!]_{\sigma_1} \\ \sigma_2 &\mapsto [\![F]\!]_{\sigma_2} \end{aligned}$$

In the limit:

$$\frac{\mathrm{d}\,[\![F]\!]_{\sigma(t)}}{\mathrm{d}t}(\zeta) = [\![F']\!]_{\bar{\sigma}(\zeta)}$$

where $\frac{\mathrm{d}\sigma(t)}{\mathrm{d}t}$ is according to ODE

Goal (Derivation lemma)

Valuation is a *differential homomorphism*

Derivations and Differentiation

Definition (Syntactic total derivation $D : \mathrm{Trm}(\Sigma \cup \Sigma') \to \mathrm{Trm}(\Sigma \cup \Sigma')$)

$$
\begin{aligned}
D(r) &= 0 && \text{if } r \text{ is a (rigid) number symbol} \\
D(x^{(n)}) &= x^{(n+1)} && \text{if } x \in \Sigma \text{ is flexible, } n \geq 0 \\
D(a + b) &= D(a) + D(b) \\
D(a \cdot b) &= D(a) \cdot b + a \cdot D(b) \\
D(a/b) &= (D(a) \cdot b - a \cdot D(b))/b^2
\end{aligned}
$$

$$
\begin{aligned}
D(F) &\equiv \bigwedge_{i=1}^{m} D(F_i) && \{F_1, \ldots, F_m\} \text{ all literals of } F \\
D(a \geq b) &\equiv D(a) \geq D(b) && \text{accordingly for } <, >, \leq, =
\end{aligned}
$$

$\mathcal{R}$ Derivations and Differentiation

Lemma (Derivation lemma)

Valuation is differential homomorphism: for all flows φ of duration $r > 0$ along which θ is defined, all $\zeta \in [0, r]$

$$\frac{\mathrm{d}\, [\![\theta]\!]_{\varphi(t)}}{\mathrm{d}t}(\zeta) = [\![D(\theta)]\!]_{\bar{\varphi}(\zeta)}$$

Lemma (Differential substitution principle)

If $\varphi \models x_i' = \theta_i \land \chi$, then $\varphi \models \mathcal{D} \leftrightarrow (\chi \rightarrow \mathcal{D}_{x_i'}^{\theta_i})$ for all $\mathcal{D}$.

Definition (Differential Invariant)

$$(\chi \rightarrow F') \;\equiv\; \chi \rightarrow D(F)_{x_i'}^{\theta_i} \qquad \text{for } [x_i' = \theta_i \land \chi]F$$

Derivation Lemma: Proof

Proof (differential symbols fit to analytic derivatives in $\bar{\varphi}(\zeta)$).

- If θ is a variable x, immediate by $\bar{\varphi}(\zeta)$:

$$\frac{\mathrm{d}\, [\![x]\!]_{\varphi(t)}}{\mathrm{d}t}(\zeta) = \frac{\mathrm{d}\, \varphi(t)(x)}{\mathrm{d}t}(\zeta) = \bar{\varphi}(\zeta)(x') = [\![D(x)]\!]_{\bar{\varphi}(\zeta)}$$

  Derivative exists as φ of order 1 in x, thus, continuously differentiable for x.

Derivation Lemma: Proof

Proof (differential symbols fit to analytic derivatives in $\bar{\varphi}(\zeta)$).

- If θ is of the form $a + b$:

$$\frac{\mathrm{d}}{\mathrm{d}t}([\![a + b]\!]_{\varphi(t)})(\zeta)$$

$\mathcal{R}$ Derivation Lemma: Proof

Proof (differential symbols fit to analytic derivatives in $\bar{\varphi}(\zeta)$).

- If θ is of the form $a + b$:

$$
\begin{aligned}
&\frac{\mathrm{d}}{\mathrm{d}t}(\llbracket a + b \rrbracket_{\varphi(t)})(\zeta) \\
= &\frac{\mathrm{d}}{\mathrm{d}t}(\llbracket a \rrbracket_{\varphi(t)} + \llbracket b \rrbracket_{\varphi(t)})(\zeta) && \llbracket\cdot\rrbracket_v \text{ homomorph for } +
\end{aligned}
$$

Derivation Lemma: Proof

Proof (differential symbols fit to analytic derivatives in $\bar{\varphi}(\zeta)$).

- If θ is of the form $a + b$:

$$\begin{aligned}
&\frac{\mathrm{d}}{\mathrm{d}t}([\![a + b]\!]_{\varphi(t)})(\zeta) \\
&= \frac{\mathrm{d}}{\mathrm{d}t}([\![a]\!]_{\varphi(t)} + [\![b]\!]_{\varphi(t)})(\zeta) && [\![\cdot]\!]_v \text{ homomorph for } + \\
&= \frac{\mathrm{d}}{\mathrm{d}t}([\![a]\!]_{\varphi(t)})(\zeta) + \frac{\mathrm{d}}{\mathrm{d}t}([\![b]\!]_{\varphi(t)})(\zeta) && \frac{\mathrm{d}}{\mathrm{d}t} \text{ is a (linear) derivation}
\end{aligned}$$

Derivation Lemma: Proof

Proof (differential symbols fit to analytic derivatives in $\bar{\varphi}(\zeta)$).

- If θ is of the form $a + b$:

$$\begin{aligned}
&\frac{\mathrm{d}}{\mathrm{d}t}(\llbracket a + b \rrbracket_{\varphi(t)})(\zeta) && \\
&= \frac{\mathrm{d}}{\mathrm{d}t}(\llbracket a \rrbracket_{\varphi(t)} + \llbracket b \rrbracket_{\varphi(t)})(\zeta) && \llbracket\cdot\rrbracket_v \text{ homomorph for } + \\
&= \frac{\mathrm{d}}{\mathrm{d}t}(\llbracket a \rrbracket_{\varphi(t)})(\zeta) + \frac{\mathrm{d}}{\mathrm{d}t}(\llbracket b \rrbracket_{\varphi(t)})(\zeta) && \frac{\mathrm{d}}{\mathrm{d}t} \text{ is a (linear) derivation} \\
&= \llbracket D(a) \rrbracket_{\bar{\varphi}(\zeta)} + \llbracket D(b) \rrbracket_{\bar{\varphi}(\zeta)} && \text{by induction hypothesis}
\end{aligned}$$

Derivation Lemma: Proof

Proof (differential symbols fit to analytic derivatives in $\bar{\varphi}(\zeta)$).

- If θ is of the form $a + b$:

$$
\begin{aligned}
&\frac{\mathrm{d}}{\mathrm{d}t}(\llbracket a+b \rrbracket_{\varphi(t)})(\zeta) \\
&= \frac{\mathrm{d}}{\mathrm{d}t}(\llbracket a \rrbracket_{\varphi(t)} + \llbracket b \rrbracket_{\varphi(t)})(\zeta) && \llbracket\cdot\rrbracket_v \text{ homomorph for } + \\
&= \frac{\mathrm{d}}{\mathrm{d}t}(\llbracket a \rrbracket_{\varphi(t)})(\zeta) + \frac{\mathrm{d}}{\mathrm{d}t}(\llbracket b \rrbracket_{\varphi(t)})(\zeta) && \frac{\mathrm{d}}{\mathrm{d}t} \text{ is a (linear) derivation} \\
&= \llbracket D(a) \rrbracket_{\bar{\varphi}(\zeta)} + \llbracket D(b) \rrbracket_{\bar{\varphi}(\zeta)} && \text{by induction hypothesis} \\
&= \llbracket D(a) + D(b) \rrbracket_{\bar{\varphi}(\zeta)} && \llbracket\cdot\rrbracket_v \text{ homomorph for } +
\end{aligned}
$$

Derivation Lemma: Proof

Proof (differential symbols fit to analytic derivatives in $\bar{\varphi}(\zeta)$).

- If θ is of the form $a + b$:

$$
\begin{aligned}
&\frac{\mathrm{d}}{\mathrm{d}t}(\llbracket a+b \rrbracket_{\varphi(t)})(\zeta) && \\
&= \frac{\mathrm{d}}{\mathrm{d}t}(\llbracket a \rrbracket_{\varphi(t)} + \llbracket b \rrbracket_{\varphi(t)})(\zeta) && \llbracket\cdot\rrbracket_v \text{ homomorph for } + \\
&= \frac{\mathrm{d}}{\mathrm{d}t}(\llbracket a \rrbracket_{\varphi(t)})(\zeta) + \frac{\mathrm{d}}{\mathrm{d}t}(\llbracket b \rrbracket_{\varphi(t)})(\zeta) && \frac{\mathrm{d}}{\mathrm{d}t} \text{ is a (linear) derivation} \\
&= \llbracket D(a) \rrbracket_{\bar{\varphi}(\zeta)} + \llbracket D(b) \rrbracket_{\bar{\varphi}(\zeta)} && \text{by induction hypothesis} \\
&= \llbracket D(a) + D(b) \rrbracket_{\bar{\varphi}(\zeta)} && \llbracket\cdot\rrbracket_v \text{ homomorph for } + \\
&= \llbracket D(a+b) \rrbracket_{\bar{\varphi}(\zeta)} && D(\cdot) \text{ is a syntactic derivation}
\end{aligned}
$$

Derivation Lemma: Proof

Proof (differential symbols fit to analytic derivatives in $\bar{\varphi}(\zeta)$).

- The case where θ is of the form $a \cdot b$ or $a - b$ is accordingly, using Leibniz product rule or subtractiveness of $D()$, respectively.

Derivation Lemma: Proof

Proof (differential symbols fit to analytic derivatives in $\bar{\varphi}(\zeta)$).

- The case where θ is of the form $a \cdot b$ or $a - b$ is accordingly, using Leibniz product rule or subtractiveness of $D()$, respectively.
- The case where θ is of the form a/b uses quotient rule and further depends on the assumption that $b \neq 0$ along φ. This holds as the value of θ is assumed to be defined all along state flow φ.

$\mathcal{R}$ Derivation Lemma: Proof

Proof (differential symbols fit to analytic derivatives in $\bar{\varphi}(\zeta)$).

- The case where θ is of the form $a \cdot b$ or $a - b$ is accordingly, using Leibniz product rule or subtractiveness of $D()$, respectively.
- The case where θ is of the form a/b uses quotient rule and further depends on the assumption that $b \neq 0$ along φ. This holds as the value of θ is assumed to be defined all along state flow φ.
- The values of numbers $r \in \mathbb{Q}$ do not change during a state flow (in fact, they are not affected by the state at all), hence their derivative is $D(r) = 0$. □

Differential Substitution Principle: Proof

Lemma (Differential substitution principle)

If $\varphi \models x_i' = \theta_i \land \chi$*, then* $\varphi \models \mathcal{D} \leftrightarrow (\chi \rightarrow \mathcal{D}_{x_i'}^{\theta_i})$ *for all* $\mathcal{D}$*.*

Proof.

Using substitution lemma for FOL on the basis of $[\![x_i']\!]_{\bar{\varphi}(\zeta)} = [\![\theta_i]\!]_{\bar{\varphi}(\zeta)}$ and $\bar{\varphi}(\zeta) \models \chi$ at each time ζ in the domain of φ. □

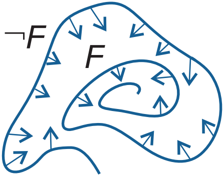
Outline

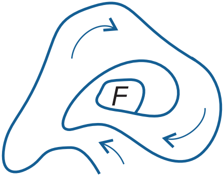
1. Verification Calculus for Differential-algebraic Dynamic Logic d$\mathcal{L}$
   - Motivation for Differential Induction
   - Derivations and Differentiation
   - Differential Induction
   - Motivation for Differential Saturation
   - Differential Variants
   - Compositional Verification Calculus
   - Differential Transformation
   - Differential Reduction & Differential Elimination
   - Proof Rules
2. Soundness
3. Restricting Differential Invariants
4. Deductive Power

Differential Induction: Local Dynamics w/o Solutions

Definition (Differential Invariant)

F closed under total differentiation with respect to differential constraints





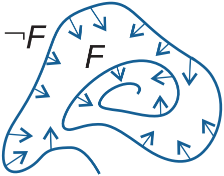
$$\frac{\vdash \forall^{\alpha}(\chi \rightarrow F')}{\chi \rightarrow F \vdash [x' = \theta \land \chi]F}$$

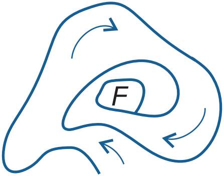
$$\frac{\vdash \forall^{\alpha}(\neg F \land \chi \rightarrow F'_{\gg})}{[x' = \theta \land \neg F]\chi \vdash \langle x' = \theta \land \chi\rangle F}$$

Differential Induction: Local Dynamics w/o Solutions

Definition (Differential Invariant)

F closed under total differentiation with respect to differential constraints





$$\frac{\vdash \forall^{\alpha}(\chi \rightarrow F')}{\chi \rightarrow F \vdash [x' = \theta \land \chi]F}$$

$$\frac{\vdash \forall^{\alpha}(\neg F \land \chi \rightarrow F'_{\gg})}{[x' = \theta \land \neg F]\chi \vdash \langle x' = \theta \land \chi \rangle F}$$

Total differential F' of *formulas*?

Differential Invariant Example: Quartic Dynamics

$$\frac{}{2x \geq \frac{1}{4} \vdash [x' = x^2 + x^4]2x \geq \frac{1}{4}}$$

Differential Invariant Example: Quartic Dynamics

$$\dfrac{\dfrac{}{\vdash \forall x\,(D(2x) \geq D(\frac{1}{4}))}}{2x \geq \frac{1}{4} \vdash [x' = x^2 + x^4]2x \geq \frac{1}{4}}$$

Differential Invariant Example: Quartic Dynamics

$$\cfrac{\cfrac{\cfrac{}{\vdash \forall x\,(2x' \geq 0)}}{\vdash \forall x\,(D(2x) \geq D(\frac{1}{4}))}}{2x \geq \frac{1}{4} \vdash [x' = x^2 + x^4]2x \geq \frac{1}{4}}$$

Differential Invariant Example: Quartic Dynamics

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \forall x\,(2(x^2+x^4)\geq 0)}}{\vdash \forall x\,(2x'\geq 0)}}{\vdash \forall x\,(D(2x)\geq D(\frac{1}{4}))}}{2x\geq\frac{1}{4} \vdash [x'=x^2+x^4]2x\geq\frac{1}{4}}$$

Differential Invariant Example: Quartic Dynamics

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash \forall x\,(2(x^2+x^4)\geq 0)}}{\vdash \forall x\,(2x'\geq 0)}}{\vdash \forall x\,(D(2x)\geq D(\frac{1}{4}))}}{2x\geq \frac{1}{4}\vdash [x'=x^2+x^4]2x\geq \frac{1}{4}}$$

Differential Invariant Example: Linear vs Angular Speed

$$\frac{}{\vdash \forall v\, (d_1^2 + d_2^2 = v^2 \rightarrow [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2)}$$

$$\mathcal{F}(\omega) \;\equiv\; d_1' = -\,\omega d_2 \land d_2' = \omega d_1$$

Differential Invariant Example: Linear vs Angular Speed

$$\dfrac{\overline{\vdash d_1^2 + d_2^2 = v^2 \rightarrow [\exists\omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2}}{\vdash \forall v\, (d_1^2 + d_2^2 = v^2 \rightarrow [\exists\omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2)}$$

$$\mathcal{F}(\omega) \;\equiv\; d_1' = -\omega d_2 \wedge d_2' = \omega d_1$$

Differential Invariant Example: Linear vs Angular Speed

$$
\begin{array}{l}
\hline
d_1^2 + d_2^2 = v^2 \vdash [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2 \\
\hline
\qquad\qquad\qquad\quad \vdash d_1^2 + d_2^2 = v^2 \rightarrow [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2 \\
\hline
\qquad\qquad\qquad\quad \vdash \forall v\, (d_1^2 + d_2^2 = v^2 \rightarrow [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2)
\end{array}
$$

$$\mathcal{F}(\omega) \;\equiv\; d_1' = -\omega d_2 \land d_2' = \omega d_1$$

Differential Invariant Example: Linear vs Angular Speed

$$\begin{array}{r@{\;}l}
\hline
 & \vdash \forall x_1, x_2\, \forall d_1, d_2\, \forall \omega\, (2d_1 d_1' + 2d_2 d_2' = 0) \\
\hline
d_1^2 + d_2^2 = v^2 & \vdash [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2 \\
\hline
 & \vdash d_1^2 + d_2^2 = v^2 \rightarrow [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2 \\
\hline
 & \vdash \forall v\, (d_1^2 + d_2^2 = v^2 \rightarrow [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2)
\end{array}$$

$$\mathcal{F}(\omega) \;\equiv\; d_1' = -\omega d_2 \wedge d_2' = \omega d_1$$

Differential Invariant Example: Linear vs Angular Speed

$$\begin{array}{rl}
\hline
 & \vdash \forall x_1, x_2\, \forall d_1, d_2\, \forall \omega\, (2d_1(-\omega d_2) + 2d_2 \omega d_1 = 0) \\
\hline
 & \vdash \forall x_1, x_2\, \forall d_1, d_2\, \forall \omega\, (2d_1 d_1' + 2d_2 d_2' = 0) \\
\hline
d_1^2 + d_2^2 = v^2 & \vdash [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2 \\
\hline
 & \vdash d_1^2 + d_2^2 = v^2 \rightarrow [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2 \\
\hline
 & \vdash \forall v\, (d_1^2 + d_2^2 = v^2 \rightarrow [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2)
\end{array}$$

$$\mathcal{F}(\omega) \;\equiv\; d_1' = -\omega d_2 \wedge d_2' = \omega d_1$$

Differential Invariant Example: Linear vs Angular Speed

$$
\begin{array}{rl}
\hline
 & \vdash \mathrm{QE}(\forall x_1, x_2\, \forall d_1, d_2\, \forall \omega\, (2d_1(-\omega d_2) + 2d_2 \omega d_1 = 0)) \\
\hline
 & \vdash \forall x_1, x_2\, \forall d_1, d_2\, \forall \omega\, (2d_1(\,-\,\omega d_2) + 2d_2 \omega d_1 = 0) \\
\hline
 & \vdash \forall x_1, x_2\, \forall d_1, d_2\, \forall \omega\, (2d_1 d_1' + 2d_2 d_2' = 0) \\
\hline
d_1^2 + d_2^2 = v^2 & \vdash [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2 \\
\hline
 & \vdash d_1^2 + d_2^2 = v^2 \rightarrow [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2 \\
\hline
 & \vdash \forall v\, (d_1^2 + d_2^2 = v^2 \rightarrow [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2)
\end{array}
$$

$$\mathcal{F}(\omega) \;\equiv\; d_1' = \,-\,\omega d_2 \wedge d_2' = \omega d_1$$

Differential Invariant Example: Linear vs Angular Speed

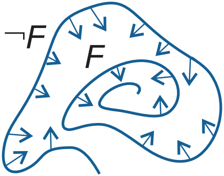
$$
\begin{array}{rl}
 & * \\ \hline
 & \vdash \mathrm{QE}(\forall x_1, x_2\, \forall d_1, d_2\, \forall \omega\, (2d_1(-\omega d_2) + 2d_2\omega d_1 = 0)) \\ \hline
 & \vdash \forall x_1, x_2\, \forall d_1, d_2\, \forall \omega\, (2d_1(- \omega d_2) + 2d_2\omega d_1 = 0) \\ \hline
 & \vdash \forall x_1, x_2\, \forall d_1, d_2\, \forall \omega\, (2d_1 d_1' + 2d_2 d_2' = 0) \\ \hline
d_1^2 + d_2^2 = v^2 & \vdash [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2 \\ \hline
 & \vdash d_1^2 + d_2^2 = v^2 \to [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2 \\ \hline
 & \vdash \forall v\, (d_1^2 + d_2^2 = v^2 \to [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2)
\end{array}
$$

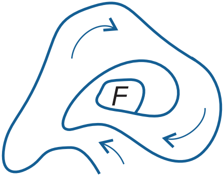
$$\mathcal{F}(\omega) \;\equiv\; d_1' = -\omega d_2 \land d_2' = \omega d_1$$

Differential Induction: Local Dynamics w/o Solutions

Definition (Differential Invariant)

F closed under total differentiation with respect to differential constraints



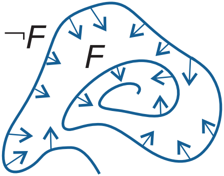


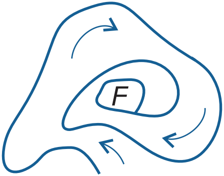
$$
\begin{aligned}
d_1 \geq d_2 \rightarrow [&x := a^2 + 1;\\
&\quad d_1' = -\omega d_2, d_2' = \omega d_1\\
&]\, d_1 \geq d_2
\end{aligned}
$$

Differential Induction: Local Dynamics w/o Solutions

Definition (Differential Invariant)

F closed under total differentiation with respect to differential constraints



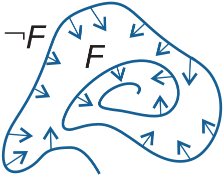


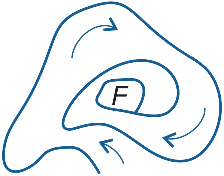
$$\begin{aligned} d_1 \geq d_2 \rightarrow [&x := a^2 + 1;\\ &\quad (d_1' = -\omega d_2 \land d_2' = \omega d_1) \lor (d_1' \leq 2d_1)\\ &]\, d_1 \geq d_2 \end{aligned}$$

Differential Induction: Local Dynamics w/o Solutions

Definition (Differential Invariant)

F closed under total differentiation with respect to differential constraints



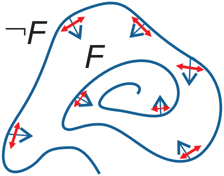


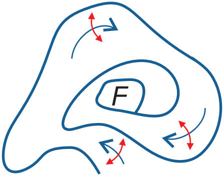
$$
\begin{aligned}
d_1 \geq d_2 \rightarrow [&x := a^2 + 1;\\
&\exists \omega \, (\omega \leq 1 \land d_1' = -\omega d_2 \land d_2' = \omega d_1) \lor (d_1' \leq 2 d_1)\\
&]\, d_1 \geq d_2
\end{aligned}
$$

Differential Induction: Local Dynamics w/o Solutions

Definition (Differential Invariant)

F closed under total differentiation with respect to differential constraints





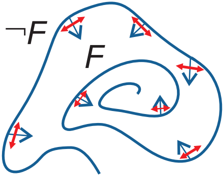
$$
\begin{aligned}
d_1 \geq d_2 \rightarrow [&x := a^2 + 1;\\
&\quad \exists \omega \, (\omega \leq 1 \land d_1' = -\omega d_2 \land d_2' = \omega d_1) \lor (d_1' \leq 2 d_1)\\
&]\, d_1 \geq d_2
\end{aligned}
$$

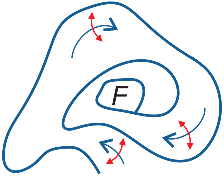
- quantified nondeterminism/disturbance

Differential Induction: Local Dynamics w/o Solutions

Definition (Differential Invariant)

F closed under total differentiation with respect to differential constraints





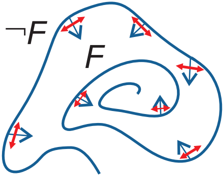
$$
\begin{aligned}
d_1 \geq d_2 \rightarrow [&x := a^2 + 1;\\
&\exists \omega\, (\omega \leq 1 \land d_1' = -\omega d_2 \land d_2' = \omega d_1) \lor (d_1' \leq 2 d_1)\\
&]\, d_1 \geq d_2
\end{aligned}
$$

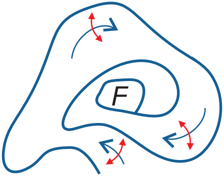
- quantified nondeterminism/disturbance

Differential Induction: Local Dynamics w/o Solutions

Definition (Differential Invariant)

F closed under total differentiation with respect to differential constraints

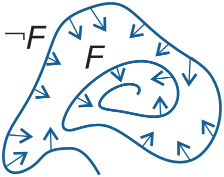


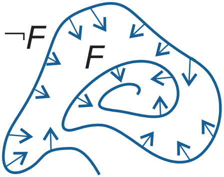


$$
\begin{aligned}
d_1 \geq d_2 \rightarrow [&x > 0 \rightarrow \exists a\,(a < 5 \land x := a^2 + 1);\\
&\quad \exists \omega\,(\omega \leq 1 \land d_1' = -\omega d_2 \land d_2' = \omega d_1) \lor (d_1' \leq 2 d_1)\\
&]\,d_1 \geq d_2
\end{aligned}
$$

- discrete quantified nondeterminism/disturbance

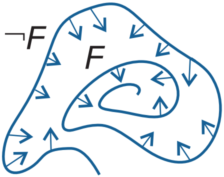
Restricting Differential Invariance



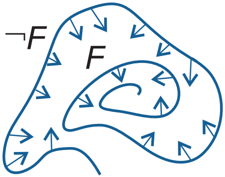


$$\frac{\vdash \forall^{\alpha}(\chi \to F')}{\chi \to F \vdash [x' = \theta \land \chi]F}$$

Restricting Differential Invariance

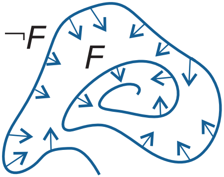


$$\frac{\vdash \forall^{\alpha}(\chi \to F')}{\chi \to F \vdash [x' = \theta \land \chi]F}$$

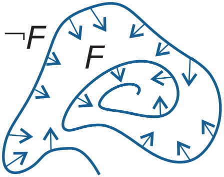


$$\frac{\vdash \forall^{\alpha}(F \land \chi \to F')}{\chi \to F \vdash [x' = \theta \land \chi]F}$$

Restricting Differential Invariance



$$\frac{\vdash \forall^{\alpha}(\chi \to F')}{\chi \to F \vdash [x' = \theta \land \chi]F}$$

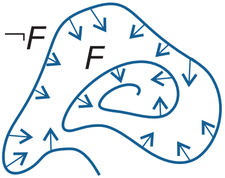


$$\frac{\vdash \forall^{\alpha}(F \land \chi \to F')}{\chi \to F \vdash [x' = \theta \land \chi]F}$$

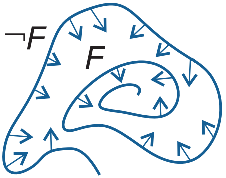
Example (Restrictions)

$$\frac{\vdash \forall x\,(x^2 \le 0 \to 2x \cdot 1 \le 0)}{x^2 \le 0 \vdash [x' = 1]x^2 \le 0}$$

Restricting Differential Invariance



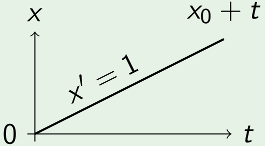
$$\frac{\vdash \forall^{\alpha}(\chi \to F')}{\chi \to F \vdash [x' = \theta \wedge \chi]F}$$



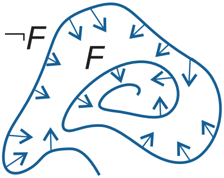
$$\frac{\vdash \forall^{\alpha}(F \wedge \chi \to F')}{\chi \to F \vdash [x' = \theta \wedge \chi]F}$$

Example (Restrictions)

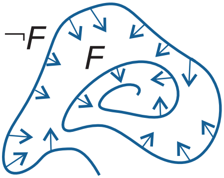
$$\frac{\vdash \forall x\, (x^2 \leq 0 \to 2x \cdot 1 \leq 0)}{x^2 \leq 0 \vdash [x' = 1]x^2 \leq 0}$$



Restricting Differential Invariance



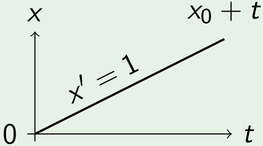
$$\frac{\vdash \forall^{\alpha}(\chi \rightarrow F')}{\chi \rightarrow F \vdash [x' = \theta \wedge \chi]F}$$



$$\cancel{\frac{\vdash \forall^{\alpha}(F \wedge \chi \rightarrow F')}{\chi \rightarrow F \vdash [x' = \theta \wedge \chi]F}}$$

Example (Restrictions are unsound nonsense!)

$$\frac{\vdash \forall x\,(x^2 \leq 0 \rightarrow 2x \cdot 1 \leq 0)}{x^2 \leq 0 \vdash [x' = 1]x^2 \leq 0}$$



Differential Invariance of Negative Equations

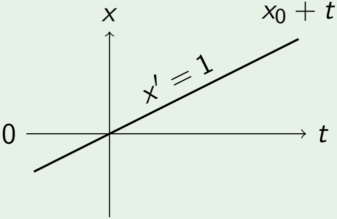
Example (Negative equations)

$$\dfrac{\dfrac{*}{\vdash \forall x\,(1 \neq 0)}}{x \neq 0 \vdash [x' = 1]x \neq 0}$$

Differential Invariance of Negative Equations

Example (Negative equations)

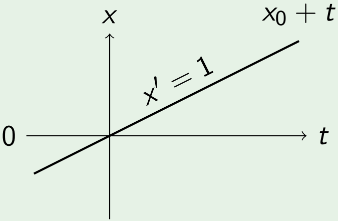
$$\cfrac{\cfrac{*}{\vdash \forall x\,(1 \neq 0)}}{x \neq 0 \vdash [x' = 1]x \neq 0}$$



Differential Invariance of Negative Equations

Example (Negative equations are unsound nonsense!)

$$\cancel{\dfrac{\dfrac{*}{\vdash \forall x\,(1 \neq 0)}}{x \neq 0 \vdash [x' = 1]\, x \neq 0}}$$



Disjunctive Differential Invariants

$$F \wedge G' \equiv$$

Disjunctive Differential Invariants

$$F \land G' \equiv F' \land G'$$

Disjunctive Differential Invariants

$$
\begin{aligned}
(F \wedge G)' &\equiv F' \wedge G' \\
(F \vee G)' &\equiv
\end{aligned}
$$

Disjunctive Differential Invariants

$$F \wedge G' \equiv F' \wedge G'$$
$$F \vee G' \equiv F' \vee G' \ ?$$

Disjunctive Differential Invariants

$$F \wedge G' \equiv F' \wedge G'$$
$$F \vee G' \equiv F' \vee G' \ ?$$

Example (Differential induction provable)

$$d_1^2 + d_2^2 = v^2 \rightarrow [\exists\omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2$$

Disjunctive Differential Invariants

$$F \wedge G' \equiv F' \wedge G'$$
$$F \vee G' \equiv F' \vee G' \text{ ?}$$

Example (Differential induction provable)

$$d_1^2 + d_2^2 = v^2 \to [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2$$

Example (Thus provable)

$$x_1 \geq 0 \vee d_1^2 + d_2^2 = v^2 \to [\exists \omega\, \mathcal{F}(\omega)](x_1 \geq 0 \vee d_1^2 + d_2^2 = v^2)$$

Disjunctive Differential Invariants

$$F \wedge G' \equiv F' \wedge G'$$
$$F \vee G' \equiv F' \vee G' \ ?$$

Example (Differential induction provable)

$$d_1^2 + d_2^2 = v^2 \rightarrow [\exists\omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2$$

Example (Nonsense!)

$$x_1 \geq 0 \vee d_1^2 + d_2^2 = v^2 \rightarrow [\exists\omega\, \mathcal{F}(\omega)](x_1 \geq 0 \vee d_1^2 + d_2^2 = v^2)$$

Disjunctive Differential Invariants

$$F \land G' \equiv F' \land G'$$

$$F \lor G' \equiv F' \land G' \;!$$

Example (Differential induction provable)

$$d_1^2 + d_2^2 = v^2 \rightarrow [\exists \omega\, \mathcal{F}(\omega)]\, d_1^2 + d_2^2 = v^2$$

Example (Nonsense!)

$$x_1 \geq 0 \lor d_1^2 + d_2^2 = v^2 \rightarrow [\exists \omega\, \mathcal{F}(\omega)](x_1 \geq 0 \lor d_1^2 + d_2^2 = v^2)$$

Closure Properties of Differential Invariants

Lemma

Differential invariants are closed under conjunction and differentiation:

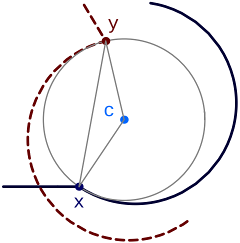
$$\begin{aligned} F \text{ diff. inv.}, G \text{ diff. inv.} \quad &\Rightarrow \quad F \land G \text{ diff. inv. (of same system)} \\ F \text{ diff. inv.} \quad &\Rightarrow \quad F' \text{ diff. inv. (of same system)} \end{aligned}$$

Outline

1. Verification Calculus for Differential-algebraic Dynamic Logic d$\mathcal{L}$
   - Motivation for Differential Induction
   - Derivations and Differentiation
   - Differential Induction
   - Motivation for Differential Saturation
   - Differential Variants
   - Compositional Verification Calculus
   - Differential Transformation
   - Differential Reduction & Differential Elimination
   - Proof Rules
2. Soundness
3. Restricting Differential Invariants
4. Deductive Power

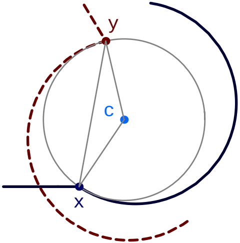
Differential Induction for Aircraft Roundabouts

$$\frac{}{\vdash [x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$



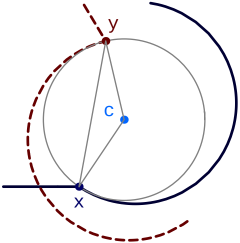
Differential Induction for Aircraft Roundabouts

$$\dfrac{\vdash \frac{\partial\|x-y\|^2}{\partial x_1}x_1' + \frac{\partial\|x-y\|^2}{\partial y_1}y_1' + \frac{\partial\|x-y\|^2}{\partial x_2}x_2' + \frac{\partial\|x-y\|^2}{\partial y_2}y_2' \geq \frac{\partial p^2}{\partial x_1}x_1' \dots}{\vdash [x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$



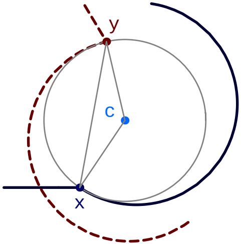
Differential Induction for Aircraft Roundabouts

$$\dfrac{\vdash \frac{\partial \|x-y\|^2}{\partial x_1} x_1' + \frac{\partial \|x-y\|^2}{\partial y_1} y_1' + \frac{\partial \|x-y\|^2}{\partial x_2} x_2' + \frac{\partial \|x-y\|^2}{\partial y_2} y_2' \geq \frac{\partial p^2}{\partial x_1} x_1' \ldots}{\vdash [x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$



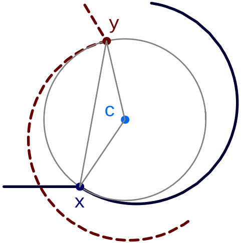
Differential Induction for Aircraft Roundabouts

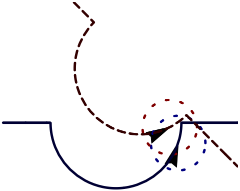
$$\dfrac{\vdash \frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2} d_2 + \frac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \ldots}{\vdash [x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1-y_1)^2 + (x_2-y_2)^2 \geq p^2}$$



Differential Induction for Aircraft Roundabouts

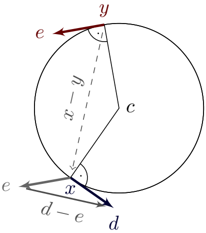
$$\begin{array}{l}
\hline
\vdash 2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0 \\
\hline
\vdash \frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2} d_2 + \frac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \dots \\
\hline
\vdash [x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2
\end{array}$$

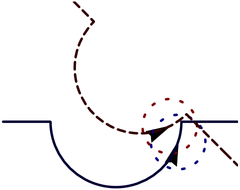




Differential Induction for Aircraft Roundabouts

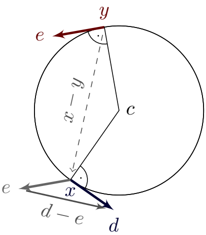
$$\begin{array}{l}
\hline
\vdash 2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0 \\
\hline
\vdash \frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2} d_2 + \frac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \dots \\
\hline
\vdash [x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2
\end{array}$$

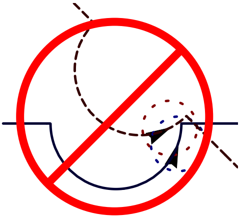




Differential Induction for Aircraft Roundabouts

$$\dfrac{\dfrac{\overline{\vdash 2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0}}{\vdash \frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial y_2}e_2\geq \frac{\partial p^2}{\partial x_1}d_1\ldots}}{\vdash [x_1'=d_1, d_1'=-\omega d_2, x_2'=d_2, d_2'=\omega d_1, ..](x_1-y_1)^2+(x_2-y_2)^2\geq p^2}$$

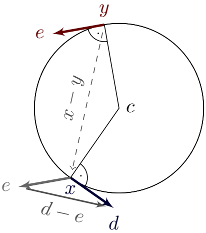




$$\overline{..\vdash [d_1'=-\omega d_2, e_1'=-\omega e_2, x_2'=d_2, d_2'=\omega d_1, ..]\,d_1-e_1=-\omega(x_2-y_2)}$$

Differential Induction for Aircraft Roundabouts

$$\begin{array}{l}
\vdash 2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0 \\
\hline
\vdash 2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0 \\
\hline
\vdash \frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2} d_2 + \frac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \ldots \\
\hline
\vdash [x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2
\end{array}$$



$$\begin{array}{l}
\hline
.. \vdash [d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1, ..] d_1 - e_1 = -\omega(x_2 - y_2)
\end{array}$$

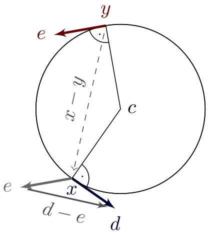
Differential Induction for Aircraft Roundabouts

$$\vdash 2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0$$

$$\vdash 2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0$$

$$\vdash \frac{\partial \|x-y\|^2}{\partial x_1} d_1 + \frac{\partial \|x-y\|^2}{\partial y_1} e_1 + \frac{\partial \|x-y\|^2}{\partial x_2} d_2 + \frac{\partial \|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \dots$$

$$\vdash [x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$

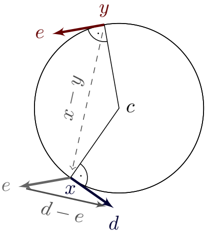


$$\vdash \frac{\partial (d_1 - e_1)}{\partial d_1} d_1' + \frac{\partial (d_1 - e_1)}{\partial e_1} e_1' = -\frac{\partial \omega (x_2 - y_2)}{\partial x_2} x_2' - \frac{\partial \omega (x_2 - y_2)}{\partial y_2} y_2'$$

$$.. \vdash [d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1, ..]d_1 - e_1 = -\omega(x_2 - y_2)$$

Differential Induction for Aircraft Roundabouts

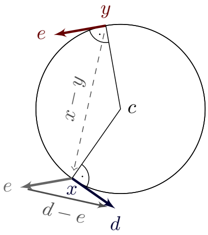
$$\begin{array}{l}
\vdash 2(x_1-y_1)(-\omega(x_2-y_2))+2(x_2-y_2)\omega(x_1-y_1)\geq 0\\
\hline
\vdash 2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0\\
\hline
\vdash \frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial y_2}e_2\geq\frac{\partial p^2}{\partial x_1}d_1\dots\\
\hline
\vdash [x_1'=d_1,d_1'=-\omega d_2,x_2'=d_2,d_2'=\omega d_1,..](x_1-y_1)^2+(x_2-y_2)^2\geq p^2
\end{array}$$



$$\begin{array}{l}
\hline
\vdash \frac{\partial(d_1-e_1)}{\partial d_1}d_1'+\frac{\partial(d_1-e_1)}{\partial e_1}e_1'=-\frac{\partial\omega(x_2-y_2)}{\partial x_2}x_2'-\frac{\partial\omega(x_2-y_2)}{\partial y_2}y_2'\\
\hline
..\vdash [d_1'=-\omega d_2,e_1'=-\omega e_2,x_2'=d_2,d_2'=\omega d_1,..]d_1-e_1=-\omega(x_2-y_2)
\end{array}$$

Differential Induction for Aircraft Roundabouts

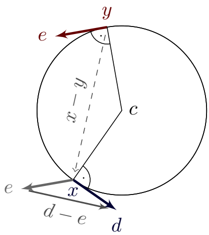
$$\begin{array}{l}
\vdash 2(x_1-y_1)(-\omega(x_2-y_2))+2(x_2-y_2)\omega(x_1-y_1)\geq 0 \\ \hline
\vdash 2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0 \\ \hline
\vdash \frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial y_2}e_2\geq\frac{\partial p^2}{\partial x_1}d_1\ldots \\ \hline
\vdash [x_1'=d_1,d_1'=-\omega d_2,x_2'=d_2,d_2'=\omega d_1,..](x_1-y_1)^2+(x_2-y_2)^2\geq p^2
\end{array}$$



$$\begin{array}{l} \hline
\vdash \frac{\partial(d_1-e_1)}{\partial d_1}(-\omega d_2)+\frac{\partial(d_1-e_1)}{\partial e_1}(-\omega e_2)=-\frac{\partial\omega(x_2-y_2)}{\partial x_2}d_2-\frac{\partial\omega(x_2-y_2)}{\partial y_2}e_2 \\ \hline
..\vdash [d_1'=-\omega d_2,e_1'=-\omega e_2,x_2'=d_2,d_2'=\omega d_1,..]d_1-e_1=-\omega(x_2-y_2)
\end{array}$$

Differential Induction for Aircraft Roundabouts

$$\dfrac{\dfrac{\dfrac{\vdash 2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0}{\vdash 2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0}}{\vdash \frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2} d_2 + \frac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \ldots}}{\vdash [x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$



$$\dfrac{\dfrac{\vdash -\omega d_2 + \omega e_2 = -\omega(d_2 - e_2)}{\vdash \frac{\partial(d_1-e_1)}{\partial d_1}(-\omega d_2) + \frac{\partial(d_1-e_1)}{\partial e_1}(-\omega e_2) = -\frac{\partial\omega(x_2-y_2)}{\partial x_2} d_2 - \frac{\partial\omega(x_2-y_2)}{\partial y_2} e_2}}{.. \vdash [d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1, ..] d_1 - e_1 = -\omega(x_2 - y_2)}$$

Differential Induction & Differential Saturation

$$
\begin{array}{l}
\vdash 2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0 \\
\hline
\vdash 2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0 \\
\hline
\vdash \frac{\partial \|x-y\|^2}{\partial x_1} d_1 + \frac{\partial \|x-y\|^2}{\partial y_1} e_1 + \frac{\partial \|x-y\|^2}{\partial x_2} d_2 + \frac{\partial \|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \dots \\
\hline
\vdash [x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2
\end{array}
$$

Proposition (Differential saturation)

F differential invariant of $[x' = \theta \land H]\phi$, then

$$[x' = \theta \land H]\phi \quad \text{iff} \quad [x' = \theta \land H \land F]\phi$$

$$
\begin{array}{l}
\quad \vdash -\omega d_2 + \omega e_2 = -\omega(d_2 - e_2) \\
\hline
\quad \vdash \frac{\partial(d_1 - e_1)}{\partial d_1}(-\omega d_2) + \frac{\partial(d_1 - e_1)}{\partial e_1}(-\omega e_2) = -\frac{\partial \omega(x_2 - y_2)}{\partial x_2} d_2 - \frac{\partial \omega(x_2 - y_2)}{\partial y_2} e_2 \\
\hline
.. \vdash [d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1, ..] d_1 - e_1 = -\omega(x_2 - y_2)
\end{array}
$$

Differential Induction & Differential Saturation

$$
\begin{array}{l}
\vdash 2(x_1-y_1)(-\omega(x_2-y_2)) + 2(x_2-y_2)\omega(x_1-y_1) \geq 0 \\
\hline
\vdash 2(x_1-y_1)(d_1-e_1) + 2(x_2-y_2)(d_2-e_2) \geq 0 \\
\hline
\vdash \frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2} d_2 + \frac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \ldots \\
\hline
\vdash [x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1-y_1)^2 + (x_2-y_2)^2 \geq p^2
\end{array}
$$

refine dynamics

by differential saturation

$$
\begin{array}{l}
\vdash -\omega d_2 + \omega e_2 = -\omega(d_2-e_2) \\
\hline
\vdash \frac{\partial(d_1-e_1)}{\partial d_1}(-\omega d_2) + \frac{\partial(d_1-e_1)}{\partial e_1}(-\omega e_2) = -\frac{\partial\omega(x_2-y_2)}{\partial x_2} d_2 - \frac{\partial\omega(x_2-y_2)}{\partial y_2} e_2 \\
\hline
.. \vdash [d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1, ..] d_1 - e_1 = -\omega(x_2-y_2)
\end{array}
$$

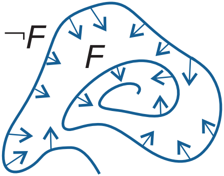
Outline

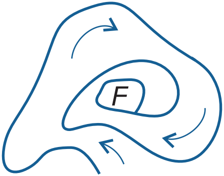
1. Verification Calculus for Differential-algebraic Dynamic Logic d$\mathcal{L}$
   - Motivation for Differential Induction
   - Derivations and Differentiation
   - Differential Induction
   - Motivation for Differential Saturation
   - Differential Variants
   - Compositional Verification Calculus
   - Differential Transformation
   - Differential Reduction & Differential Elimination
   - Proof Rules
2. Soundness
3. Restricting Differential Invariants
4. Deductive Power

Differential Induction: Local Dynamics w/o Solutions

Definition (Differential Invariant)

F closed under total differentiation with respect to differential constraints





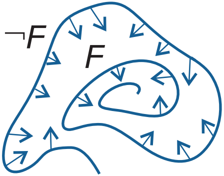
$$\frac{\vdash (\chi \to F')}{\chi \to F \vdash [x' = \theta \land \chi]F}$$

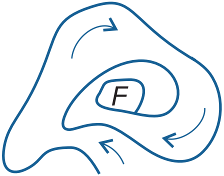
$$\frac{\vdash (\neg F \land \chi \to F'_{\gg})}{[x' = \theta \land \sim F]\chi \vdash \langle x' = \theta \land \chi\rangle F}$$

Differential Variants

Definition (Differential Variant)

F positive under total differentiation with respect to differential constraints





$$\frac{\vdash (\chi \rightarrow F')}{\chi \rightarrow F \vdash [x' = \theta \wedge \chi]F}$$

$$\frac{\vdash (\neg F \wedge \chi \rightarrow F'_{\gg})}{[x' = \theta \wedge \sim F]\chi \vdash \langle x' = \theta \wedge \chi \rangle F}$$

$$\frac{\vdash \exists \varepsilon{>}0\, \forall y_1, y_k\, (\neg F \wedge \chi \rightarrow (F' \geq \varepsilon)^{\theta_1}_{x'_1} \dots {}^{\theta_n}_{x'_n})}{[\exists y_1, y_k\, (x'_1 = \theta_1 \wedge, \wedge x'_n = \theta_n \wedge \sim F)]\chi \vdash \langle \exists y_1, y_k\, (x'_1 = \theta_1 \wedge, \wedge x'_n = \theta_n \wedge \chi) \rangle F}$$

when Lipschitz-continuous and F without equalities

Differential Variants for Flight Progress

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdash b > 0}{\vdash \mathrm{QE}(\exists d\,((\|d\|^2 \le b^2) \land (d_1 > 0 \land d_2 > 0)))}}{\vdash \|d\|^2 \le b^2 \qquad \dfrac{\dfrac{\vdash d_1 > 0 \land d_2 > 0}{\vdash \exists \epsilon{>}0\, \forall x_1, x_2\, (x_1 < p_1 \lor x_2 < p_2 \rightarrow d_1 \ge \epsilon \land d_2 \ge \epsilon)}}{\vdash \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)}}}{\vdash \|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)}}{\dfrac{\vdash \exists d\, (\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))}{\vdash \forall p\, \exists d\, (\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))}}$$

$$\begin{aligned} \mathcal{F}(0) &\equiv x_1' = d_1 \land x_2' = d_2 \\ F &\equiv x_1 \ge p_1 \land x_2 \ge p_2 \end{aligned}$$

Differential Variants for Flight Progress

$$
\dfrac{\dfrac{\dfrac{\dfrac{\vdash b > 0}{\vdash \mathrm{QE}(\exists d\, ((\|d\|^2 \le b^2) \land (d_1 > 0 \land d_2 > 0)))}}{\vdash \|d\|^2 \le b^2 \qquad \dfrac{\dfrac{\vdash d_1 > 0 \land d_2 > 0}{\vdash \exists \epsilon{>}0\, \forall x_1, x_2\, (x_1 < p_1 \lor x_2 < p_2 \rightarrow d_1 \ge \epsilon \land d_2 \ge \epsilon)}}{\vdash \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)}}}{\vdash \|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)}}{\dfrac{\vdash \exists d\, (\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))}{\vdash \forall p\, \exists d\, (\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))}}
$$

$$
\begin{aligned}
\mathcal{F}(0) &\equiv x_1' = d_1 \land x_2' = d_2 \\
F &\equiv x_1 \ge p_1 \land x_2 \ge p_2 \\
F' &\equiv x_1' \ge 0 \land x_2' \ge 0
\end{aligned}
$$

Differential Variants for Flight Progress

$$
\dfrac{\dfrac{\dfrac{\dfrac{\vdash b > 0}{\vdash \mathrm{QE}(\exists d\,((\|d\|^2 \le b^2) \land (d_1 > 0 \land d_2 > 0)))}}{\vdash \|d\|^2 \le b^2 \qquad \dfrac{\dfrac{\vdash d_1 > 0 \land d_2 > 0}{\vdash \exists \epsilon{>}0\, \forall x_1, x_2\, (x_1 < p_1 \lor x_2 < p_2 \rightarrow d_1 \ge \epsilon \land d_2 \ge \epsilon)}}{\vdash \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)}}}{\vdash \|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)}}{\dfrac{\vdash \exists d\, (\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))}{\vdash \forall p\, \exists d\, (\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))}}
$$

$$
\begin{aligned}
\mathcal{F}(0) &\equiv x_1' = d_1 \land x_2' = d_2 \\
F &\equiv x_1 \ge p_1 \land x_2 \ge p_2 \\
F' &\equiv x_1' \ge 0 \land x_2' \ge 0 \\
F' \ge \epsilon &\equiv x_1' \ge \epsilon \land x_2' \ge \epsilon
\end{aligned}
$$

Differential Variants for Flight Progress

$$
\begin{array}{ll}
\multicolumn{2}{c}{\vdash b > 0} \\ \hline
\multicolumn{2}{c}{\vdash \mathrm{QE}(\exists d\,((\|d\|^2 \leq b^2) \land (d_1 > 0 \land d_2 > 0)))} \\ \hline
 & \vdash d_1 > 0 \land d_2 > 0 \\ \cline{2-2}
 & \vdash \exists \epsilon{>}0\, \forall x_1, x_2\, (x_1 < p_1 \lor x_2 < p_2 \rightarrow d_1 \geq \epsilon \land d_2 \geq \epsilon) \\ \cline{2-2}
\vdash \|d\|^2 \leq b^2 & \vdash \langle \mathcal{F}(0) \rangle (x_1 \geq p_1 \land x_2 \geq p_2) \\ \hline
\multicolumn{2}{c}{\vdash \|d\|^2 \leq b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \geq p_1 \land x_2 \geq p_2)} \\ \hline
\multicolumn{2}{c}{\vdash \exists d\,(\|d\|^2 \leq b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \geq p_1 \land x_2 \geq p_2))} \\ \hline
\multicolumn{2}{c}{\vdash \forall p\, \exists d\,(\|d\|^2 \leq b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \geq p_1 \land x_2 \geq p_2))}
\end{array}
$$

$$
\begin{aligned}
\mathcal{F}(0) &\equiv x_1' = d_1 \land x_2' = d_2 \\
F &\equiv x_1 \geq p_1 \land x_2 \geq p_2 \\
F' &\equiv x_1' \geq 0 \land x_2' \geq 0 \\
F' \geq \epsilon &\equiv x_1' \geq \epsilon \land x_2' \geq \epsilon
\end{aligned}
$$

Differential Variants for Flight Progress

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\vdash b > 0}{\vdash \mathrm{QE}(\exists d\,((\|d\|^2 \le b^2) \land (d_1 > 0 \land d_2 > 0)))}}{\vdash \|d\|^2 \le b^2 \qquad \cfrac{\cfrac{\vdash d_1 > 0 \land d_2 > 0}{\vdash \exists \epsilon{>}0\, \forall x_1, x_2\, (x_1 < p_1 \lor x_2 < p_2 \rightarrow d_1 \ge \epsilon \land d_2 \ge \epsilon)}}{\vdash \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)}}}{\vdash \|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)}}{\vdash \exists d\,(\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))}}{\vdash \forall p\, \exists d\,(\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))}$$

$$\begin{aligned}
\mathcal{F}(0) \;&\equiv\; x_1' = d_1 \land x_2' = d_2 \\
F \;&\equiv\; x_1 \ge p_1 \land x_2 \ge p_2 \\
F' \;&\equiv\; d_1 \ge 0 \land d_2 \ge 0 \\
F' \ge \epsilon \;&\equiv\; d_1 \ge \epsilon \land d_2 \ge \epsilon
\end{aligned}$$

Differential Variants for Progress

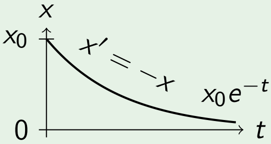
Example (Progress)

$$\frac{\vdash \forall x\,(x > 0 \rightarrow -x < 0)}{\vdash \langle x' = -x\rangle x \leq 0}$$

Differential Variants for Progress

Example (Progress)

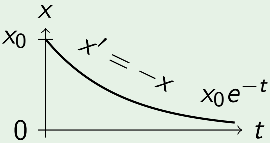
$$\frac{\vdash \forall x\,(x > 0 \rightarrow -x < 0)}{\vdash \langle x' = -x \rangle x \leq 0}$$



Differential Variants for Progress

Example (Unsound without minimal progress!)

$$\frac{\vdash \forall x\,(x > 0 \to -x < 0)}{\vdash \langle x' = -x\rangle x \le 0}$$



Differential Variants for Progress

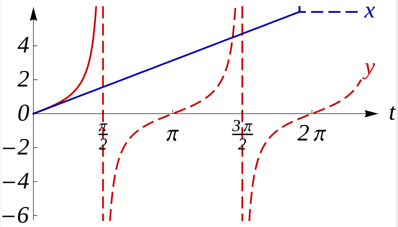
Example (Mixed dynamics)

$$\dfrac{\dfrac{*}{\vdash \exists \varepsilon{>}0\, \forall x \forall y\, (x < 6 \rightarrow 1 \geq \varepsilon)}}{\vdash \langle x' = 1 \land y' = 1 + y^2 \rangle x \geq 6}$$

Differential Variants for Progress

Example (Mixed dynamics)

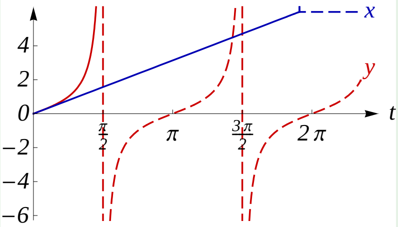
$$\cfrac{\cfrac{*}{\vdash \exists \varepsilon{>}0\, \forall x \forall y\, (x < 6 \rightarrow 1 \geq \varepsilon)}}{\vdash \langle x' = 1 \land y' = 1 + y^2 \rangle x \geq 6}$$



Differential Variants for Progress

Example (Unsound without Lipschitz-continuity!)

$$\dfrac{\dfrac{*}{\vdash \exists\varepsilon>0\,\forall x\forall y\,(x<6\to 1\geq\varepsilon)}}{\vdash \langle x'=1\wedge y'=1+y^2\rangle x\geq 6}$$

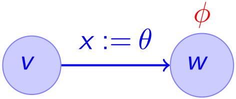


Outline

1. Verification Calculus for Differential-algebraic Dynamic Logic d$\mathcal{L}$
   - Motivation for Differential Induction
   - Derivations and Differentiation
   - Differential Induction
   - Motivation for Differential Saturation
   - Differential Variants
   - Compositional Verification Calculus
   - Differential Transformation
   - Differential Reduction & Differential Elimination
   - Proof Rules
2. Soundness
3. Restricting Differential Invariants
4. Deductive Power

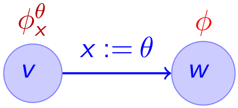
Verification of Differential-algebraic Dynamic Logic

$$\frac{}{[x := \theta]\phi}$$



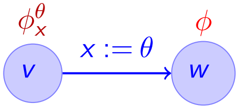
Verification of Differential-algebraic Dynamic Logic

$$\frac{}{[x := \theta]\phi}$$



Verification of Differential-algebraic Dynamic Logic

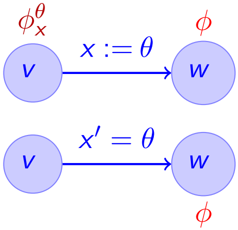
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$



Verification of Differential-algebraic Dynamic Logic

$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$

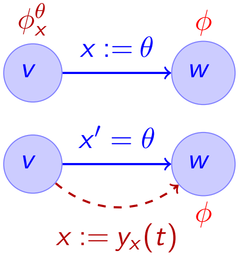
$$\frac{\quad}{\langle x' = \theta\rangle\phi}$$



Verification of Differential-algebraic Dynamic Logic

$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$

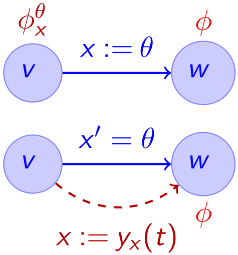
$$\frac{}{\langle x' = \theta \rangle \phi}$$



Verification of Differential-algebraic Dynamic Logic

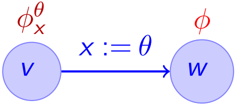
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$

$$\frac{\exists t \geq 0\, \langle x := y_x(t) \rangle \phi}{\langle x' = \theta \rangle \phi}$$

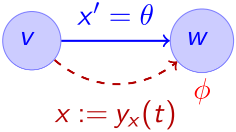


Verification of Differential-algebraic Dynamic Logic

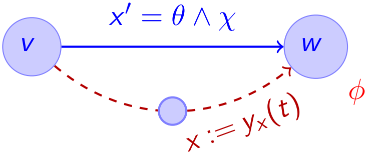
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$



$$\frac{\exists t{\geq}0\,\langle x := y_x(t)\rangle\phi}{\langle x' = \theta\rangle\phi}$$

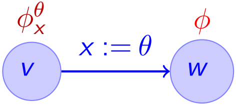


$$\frac{}{\langle x' = \theta \land \chi\rangle\phi}$$

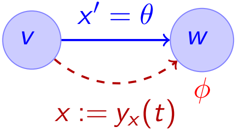


Verification of Differential-algebraic Dynamic Logic

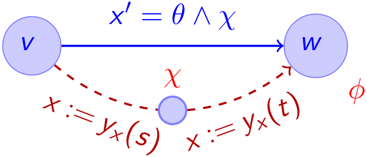
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$



$$\frac{\exists t{\geq}0\, \langle x := y_x(t)\rangle\phi}{\langle x' = \theta\rangle\phi}$$

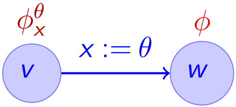


$$\frac{}{\langle x' = \theta \land \chi\rangle\phi}$$

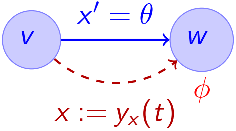


Verification of Differential-algebraic Dynamic Logic

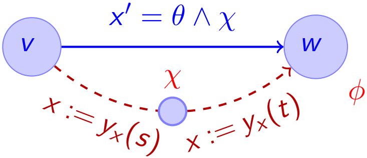
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$



$$\frac{\exists t\geq 0\, \langle x := y_x(t)\rangle\phi}{\langle x' = \theta\rangle\phi}$$

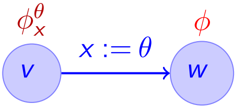


$$\frac{\exists t\geq 0\, (\bar{\chi} \wedge \langle x := y_x(t)\rangle\phi)}{\langle x' = \theta \wedge \chi\rangle\phi}$$

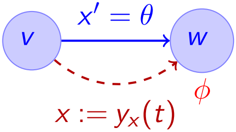


Verification of Differential-algebraic Dynamic Logic

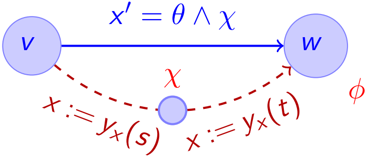
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$



$$\frac{\exists t{\geq}0\, \langle x := y_x(t)\rangle\phi}{\langle x' = \theta\rangle\phi}$$



$$\frac{\exists t{\geq}0\, (\bar\chi \land \langle x := y_x(t)\rangle\phi)}{\langle x' = \theta \land \chi\rangle\phi}$$



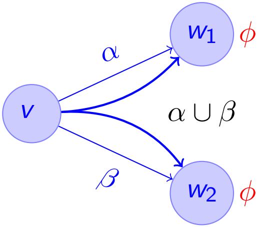
$$\bar\chi \;\equiv\; \forall 0{\leq}s{\leq}t\, \langle x := y_x(s)\rangle\chi$$

Verification of Differential-algebraic Dynamic Logic

compositional semantics ⇒ compositional rules!

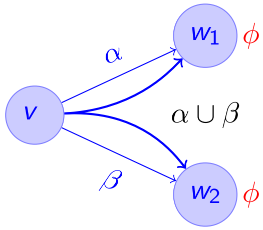
Verification of Differential-algebraic Dynamic Logic

$$\frac{}{[\alpha \cup \beta]\phi}$$



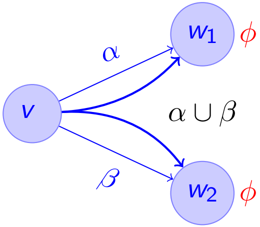
Verification of Differential-algebraic Dynamic Logic

$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$

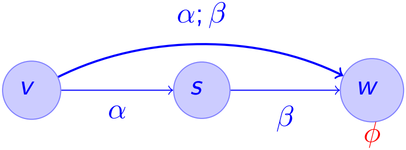


Verification of Differential-algebraic Dynamic Logic

$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$

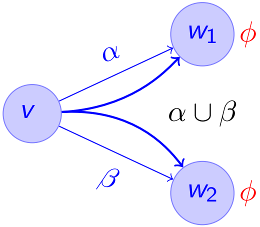


$$\frac{}{[\alpha;\beta]\phi}$$

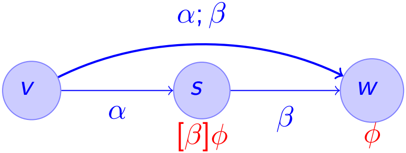


Verification of Differential-algebraic Dynamic Logic

$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$

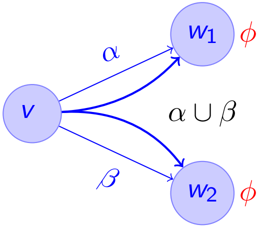


$$\frac{}{[\alpha;\beta]\phi}$$

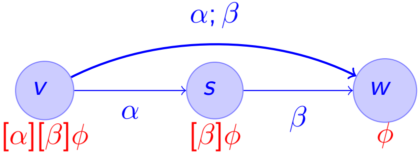


Verification of Differential-algebraic Dynamic Logic

$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$

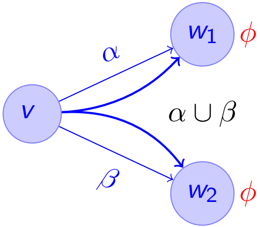


$$\frac{}{[\alpha;\beta]\phi}$$

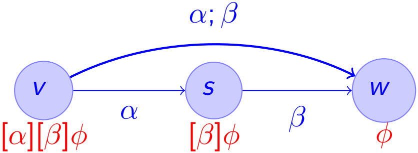


Verification of Differential-algebraic Dynamic Logic

$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$

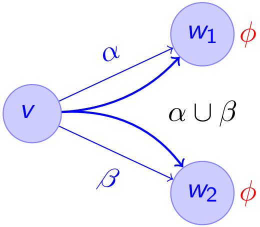


$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$

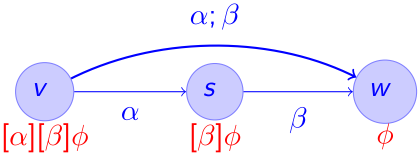


Verification of Differential-algebraic Dynamic Logic

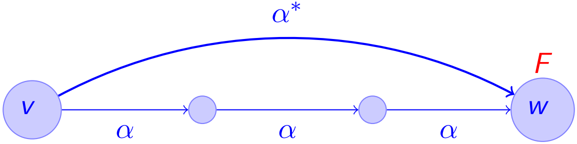
$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$



$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$

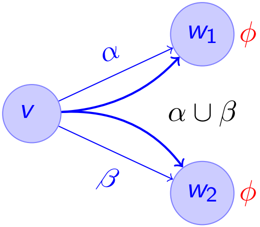


$$\frac{}{\vdash [\alpha^*]F}$$

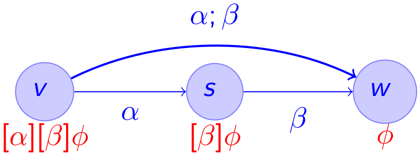


Verification of Differential-algebraic Dynamic Logic

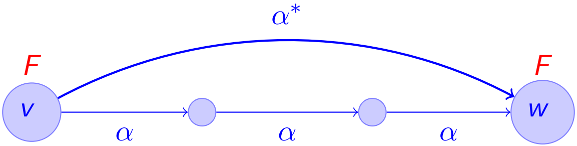
$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$



$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$

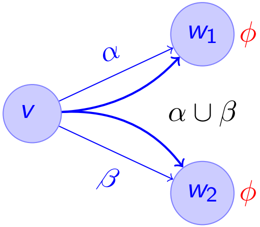


$$\frac{\vdash F}{\vdash [\alpha^*]F}$$

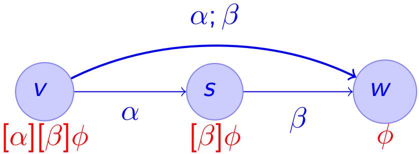


Verification of Differential-algebraic Dynamic Logic

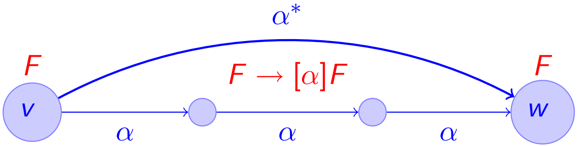
$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$



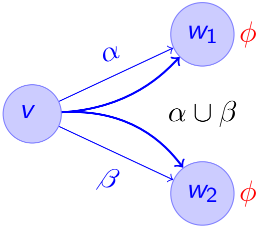
$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$



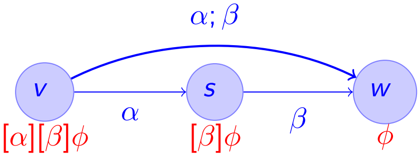
$$\frac{\vdash F}{\vdash [\alpha^*]F}$$



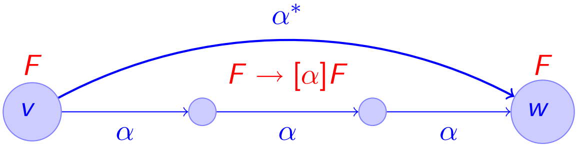
$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$



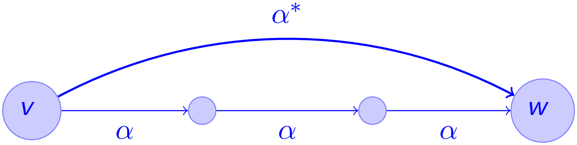
$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$



$$\frac{\vdash F \quad \vdash (F \to [\alpha]F)}{\vdash [\alpha^*]F}$$

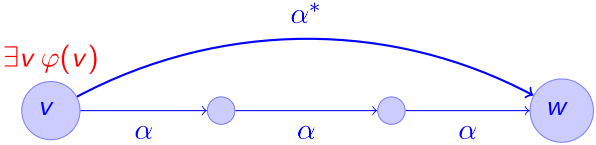


$$\frac{}{\vdash \langle \alpha^* \rangle \psi}$$



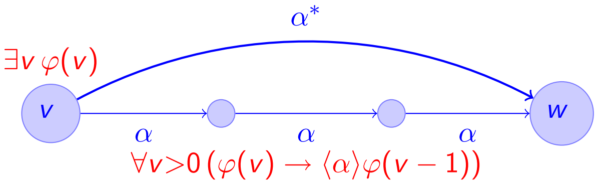
Verification of Differential-algebraic Dynamic Logic

$$\frac{\vdash \exists v\, \varphi(v)}{\vdash \langle \alpha^* \rangle \psi}$$



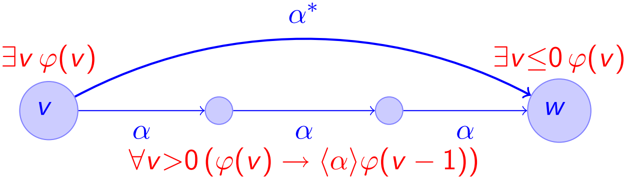
Verification of Differential-algebraic Dynamic Logic

$$\frac{\vdash \exists v\, \varphi(v) \qquad \vdash \forall v{>}0\, (\varphi(v) \rightarrow \langle\alpha\rangle\varphi(v-1))}{\vdash \langle\alpha^*\rangle\psi}$$


α^*
$\exists v\, \varphi(v)$
v
w
α
α
α
$\forall v{>}0\, (\varphi(v) \rightarrow \langle\alpha\rangle\varphi(v-1))$

Verification of Differential-algebraic Dynamic Logic

$$\frac{\vdash \exists v\, \varphi(v) \quad \vdash \forall v{>}0\, (\varphi(v) \rightarrow \langle\alpha\rangle\varphi(v-1)) \quad \vdash (\exists v{\leq}0\, \varphi(v) \rightarrow \psi)}{\vdash \langle\alpha^*\rangle\psi}$$


α^*
$\exists v\, \varphi(v)$
$\exists v{\leq}0\, \varphi(v)$
v
w
α
α
α
$\forall v{>}0\, (\varphi(v) \rightarrow \langle\alpha\rangle\varphi(v-1))$

Outline

1. Verification Calculus for Differential-algebraic Dynamic Logic d$\mathcal{L}$
   - Motivation for Differential Induction
   - Derivations and Differentiation
   - Differential Induction
   - Motivation for Differential Saturation
   - Differential Variants
   - Compositional Verification Calculus
   - Differential Transformation
   - Differential Reduction & Differential Elimination
   - Proof Rules
2. Soundness
3. Restricting Differential Invariants
4. Deductive Power

$\mathcal{R}$ Differential Transformation

Lemma (Differential transformation principle)

Let $\mathcal{D}$ and $\mathcal{E}$ be DA-constraints (same changed variables). If $\mathcal{D} \rightarrow \mathcal{E}$ is a tautology of (non-differential) first-order real arithmetic (that is, when considering $x^{(n)}$ as a new variable independent from x), then $\rho(\mathcal{D}) \subseteq \rho(\mathcal{E})$.

$\mathcal{R}$ Differential Transformation

Lemma (Differential transformation principle)

Let $\mathcal{D}$ and $\mathcal{E}$ be DA-constraints (same changed variables). If $\mathcal{D} \to \mathcal{E}$ is a tautology of (non-differential) first-order real arithmetic (that is, when considering $x^{(n)}$ as a new variable independent from x), then $\rho(\mathcal{D}) \subseteq \rho(\mathcal{E})$.

- DA-constraints $\mathcal{D}$ and $\mathcal{E}$ are *equivalent* iff $\rho(\mathcal{D}) = \rho(\mathcal{E})$.

$\mathcal{R}$ Differential Transformation

Lemma (Differential transformation principle)

Let $\mathcal{D}$ and $\mathcal{E}$ be DA-constraints (same changed variables). If $\mathcal{D} \to \mathcal{E}$ is a tautology of (non-differential) first-order real arithmetic (that is, when considering $x^{(n)}$ as a new variable independent from x), then $\rho(\mathcal{D}) \subseteq \rho(\mathcal{E})$.

- DA-constraints $\mathcal{D}$ and $\mathcal{E}$ are *equivalent* iff $\rho(\mathcal{D}) = \rho(\mathcal{E})$.
- Semantics of DA-programs is preserved when replacing DA-constraint equivalently in non-differential first-order real arithmetic.

Differential Transformation: Proof

Proof.

- $\mathcal{D} \equiv \phi_X^{x'}$ and $\mathcal{E} \equiv \psi_X^{x'}$.

□

Differential Transformation: Proof

Proof.

- $\mathcal{D} \equiv \phi_{X}^{x'}$ and $\mathcal{E} \equiv \psi_{X}^{x'}$.
- Let $\phi \rightarrow \psi$ be valid in (non-differential) real arithmetic.

□

Differential Transformation: Proof

Proof.

- $\mathcal{D} \equiv \phi_X^{x'}$ and $\mathcal{E} \equiv \psi_X^{x'}$.
- Let $\phi \rightarrow \psi$ be valid in (non-differential) real arithmetic.
- Let $(v, w) \in \rho(\mathcal{D})$ according to a state flow φ.

□

Differential Transformation: Proof

Proof.

- $\mathcal{D} \equiv \phi_X^{x'}$ and $\mathcal{E} \equiv \psi_X^{x'}$.
- Let $\phi \rightarrow \psi$ be valid in (non-differential) real arithmetic.
- Let $(v, w) \in \rho(\mathcal{D})$ according to a state flow φ.
- Then φ is a state flow for $\mathcal{E}$ that justifies $(v, w) \in \rho(\mathcal{E})$:

□

Differential Transformation: Proof

Proof.

- $\mathcal{D} \equiv \phi_X^{x'}$ and $\mathcal{E} \equiv \psi_X^{x'}$.
- Let $\phi \to \psi$ be valid in (non-differential) real arithmetic.
- Let $(v, w) \in \rho(\mathcal{D})$ according to a state flow φ.
- Then φ is a state flow for $\mathcal{E}$ that justifies $(v, w) \in \rho(\mathcal{E})$:
- For any $\zeta \in [0, r]$, we have $\bar{\varphi}(\zeta) \models \mathcal{D}$

□

Differential Transformation: Proof

Proof.

- $\mathcal{D} \equiv \phi_X^{x'}$ and $\mathcal{E} \equiv \psi_X^{x'}$.
- Let $\phi \rightarrow \psi$ be valid in (non-differential) real arithmetic.
- Let $(v, w) \in \rho(\mathcal{D})$ according to a state flow φ.
- Then φ is a state flow for $\mathcal{E}$ that justifies $(v, w) \in \rho(\mathcal{E})$:
- For any $\zeta \in [0, r]$, we have $\bar{\varphi}(\zeta) \models \mathcal{D}$
- Hence $\bar{\varphi}(\zeta) \models \mathcal{E}$,

□

Differential Transformation: Proof

Proof.

- $\mathcal{D} \equiv \phi_X^{x'}$ and $\mathcal{E} \equiv \psi_X^{x'}$.
- Let $\phi \to \psi$ be valid in (non-differential) real arithmetic.
- Let $(v, w) \in \rho(\mathcal{D})$ according to a state flow φ.
- Then φ is a state flow for $\mathcal{E}$ that justifies $(v, w) \in \rho(\mathcal{E})$:
- For any $\zeta \in [0, r]$, we have $\bar{\varphi}(\zeta) \models \mathcal{D}$
- Hence $\bar{\varphi}(\zeta) \models \mathcal{E}$,
- because $\bar{\varphi}(\zeta) \models \phi_X^{x'}$ implies $\bar{\varphi}(\zeta) \models \psi_X^{x'}$ by validity of $\phi \to \psi$.

□

Differential Transformation: Proof

Proof.

- $\mathcal{D} \equiv \phi_X^{x'}$ and $\mathcal{E} \equiv \psi_X^{x'}$.
- Let $\phi \rightarrow \psi$ be valid in (non-differential) real arithmetic.
- Let $(v, w) \in \rho(\mathcal{D})$ according to a state flow φ.
- Then φ is a state flow for $\mathcal{E}$ that justifies $(v, w) \in \rho(\mathcal{E})$:
- For any $\zeta \in [0, r]$, we have $\bar{\varphi}(\zeta) \models \mathcal{D}$
- Hence $\bar{\varphi}(\zeta) \models \mathcal{E}$,
- because $\bar{\varphi}(\zeta) \models \phi_X^{x'}$ implies $\bar{\varphi}(\zeta) \models \psi_X^{x'}$ by validity of $\phi \rightarrow \psi$.
- $\mathcal{D}$ and $\mathcal{E}$ need same set of changed variables as unchanged variables z remain constant.

□

Differential Transformation: Proof

Proof.

- $\mathcal{D} \equiv \phi_X^{x'}$ and $\mathcal{E} \equiv \psi_X^{x'}$.
- Let $\phi \rightarrow \psi$ be valid in (non-differential) real arithmetic.
- Let $(v, w) \in \rho(\mathcal{D})$ according to a state flow φ.
- Then φ is a state flow for $\mathcal{E}$ that justifies $(v, w) \in \rho(\mathcal{E})$:
- For any $\zeta \in [0, r]$, we have $\bar{\varphi}(\zeta) \models \mathcal{D}$
- Hence $\bar{\varphi}(\zeta) \models \mathcal{E}$,
- because $\bar{\varphi}(\zeta) \models \phi_X^{x'}$ implies $\bar{\varphi}(\zeta) \models \psi_X^{x'}$ by validity of $\phi \rightarrow \psi$.
- $\mathcal{D}$ and $\mathcal{E}$ need same set of changed variables as unchanged variables z remain constant.
- Add $z' = 0$ as required.

□

Outline

1. Verification Calculus for Differential-algebraic Dynamic Logic d$\mathcal{L}$
   - Motivation for Differential Induction
   - Derivations and Differentiation
   - Differential Induction
   - Motivation for Differential Saturation
   - Differential Variants
   - Compositional Verification Calculus
   - Differential Transformation
   - Differential Reduction & Differential Elimination
   - Proof Rules
2. Soundness
3. Restricting Differential Invariants
4. Deductive Power

$\mathcal{A}$ Differential Reduction

Lemma (Differential inequality elimination)

DA-constraints admit differential inequality elimination, i.e., to each DA-constraint $\mathcal{D}$, an equivalent DA-constraint without differential inequalities can be effectively associated that has no other free variables.

Proof.

□

$\mathcal{R}$ Differential Reduction

Lemma (Differential inequality elimination)

DA-constraints admit differential inequality elimination, i.e., to each DA-constraint $\mathcal{D}$, an equivalent DA-constraint without differential inequalities can be effectively associated that has no other free variables.

Proof.

- Let $\mathcal{E}$ like $\mathcal{D}$ with all differential inequalities $\theta_1 \leq \theta_2$ replaced by a quantified differential equation $\exists u\,(\theta_1 = \theta_2 - u \wedge u \geq 0)$ with a new variable u for the quantified disturbance (accordingly for $\geq, >, <$).

□

$\mathcal{R}$ Differential Reduction

Lemma (Differential inequality elimination)

DA-constraints admit differential inequality elimination, i.e., to each DA-constraint $\mathcal{D}$, an equivalent DA-constraint without differential inequalities can be effectively associated that has no other free variables.

Proof.

- Let $\mathcal{E}$ like $\mathcal{D}$ with all differential inequalities $\theta_1 \leq \theta_2$ replaced by a quantified differential equation $\exists u\,(\theta_1 = \theta_2 - u \land u \geq 0)$ with a new variable u for the quantified disturbance (accordingly for $\geq, >, <$).
- Diff. trafo: equivalence of $\mathcal{D}$ and $\mathcal{E}$ is a simple consequence of the corresponding equivalences in first-order real arithmetic.

□

Differential Equation Normalization

DA-constraint may become inhomogeneous: $\theta_1 \leq x' \leq \theta_2$ produces

$$\exists u \, \exists v \, (x' = \theta_1 + u \land x' = \theta_2 - v \land u \geq 0 \land v \geq 0)$$

$\mathcal{R}$ Differential Equation Normalization

Lemma (Differential equation normalisation)

DA-constraints admit differential equation normalisation, i.e., to each DA-constraint $\mathcal{D}$, an equivalent DA-constraint with at most one differential equation for each differential symbol can be effectively associated that has no other free variables. This differential equation is of the form $x^{(n)} = \theta$ where $\operatorname{ord}_x \theta < n$.

Differential Equation Normalization

Lemma (Differential equation normalisation)

DA-constraints admit differential equation normalisation, i.e., to each DA-constraint $\mathcal{D}$, an equivalent DA-constraint with at most one differential equation for each differential symbol can be effectively associated that has no other free variables. This differential equation is of the form $x^{(n)} = \theta$ where $\operatorname{ord}_x \theta < n$.

Proof.

□

$\mathcal{R}$ Differential Equation Normalization

Lemma (Differential equation normalisation)

DA-constraints admit differential equation normalisation, i.e., to each DA-constraint $\mathcal{D}$, an equivalent DA-constraint with at most one differential equation for each differential symbol can be effectively associated that has no other free variables. This differential equation is of the form $x^{(n)} = \theta$ where $\operatorname{ord}_x \theta < n$.

Proof.

- For each differential symbol $x^{(n)} \in \Sigma'$, introduce new non-differential variable $X_n \in \Sigma$.

□

Differential Equation Normalization

Lemma (Differential equation normalisation)

DA-constraints admit differential equation normalisation, i.e., to each DA-constraint $\mathcal{D}$, an equivalent DA-constraint with at most one differential equation for each differential symbol can be effectively associated that has no other free variables. This differential equation is of the form $x^{(n)} = \theta$ where $\operatorname{ord}_x \theta < n$.

Proof.

- For each differential symbol $x^{(n)} \in \Sigma'$, introduce new non-differential variable $X_n \in \Sigma$.
- Diff. trafo: equivalence of $\mathcal{D}$ and $\exists X_n \, (x^{(n)} = X_n \land \mathcal{D}_{x^{(n)}}^{X_n})$ is a simple consequence of the corresponding equivalence in $\mathrm{FOL}_{\mathbb{R}}$.

□

Differential Equation Normalization

Lemma (Differential equation normalisation)

DA-constraints admit differential equation normalisation, i.e., to each DA-constraint $\mathcal{D}$, an equivalent DA-constraint with at most one differential equation for each differential symbol can be effectively associated that has no other free variables. This differential equation is of the form $x^{(n)} = \theta$ where $\operatorname{ord}_x \theta < n$.

Proof.

- For each differential symbol $x^{(n)} \in \Sigma'$, introduce new non-differential variable $X_n \in \Sigma$.
- Diff. trafo: equivalence of $\mathcal{D}$ and $\exists X_n \, (x^{(n)} = X_n \wedge \mathcal{D}_{x^{(n)}}^{X_n})$ is a simple consequence of the corresponding equivalence in $\text{FOL}_{\mathbb{R}}$.
- Induction for all such $x^{(n)} \in \Sigma'$ in $\mathcal{D}$ gives desired result.

□

Differential Variants for Flight Progress

Recall aircraft progress property

$$\forall p\,\exists d\,(\|d\|^2 \le b^2 \land \langle x_1' = d_1 \land x_2' = d_2\rangle(x_1 \ge p_1 \land x_2 \ge p_2))$$

Similar proof can be found for

$$\forall p\,\exists d\,(\|d\|^2 \le b^2 \land \langle x_1' \ge d_1 \land x_2' \ge d_2\rangle(x_1 \ge p_1 \land x_2 \ge p_2))$$

$$\rightsquigarrow ..\langle \exists u\,(x_1' = d_1 + u_1 \land x_2' = d_2 + u_2 \land u_1 \ge 0 \land u_2 \ge 0)\rangle(x_1 \ge p_1 \land x_2 \ge p_2$$

The proof is identical to before, except that differential induction yields

$$\forall x\,\forall u\,((x_1 < p_1 \lor x_2 < p_2) \land u_1 \ge 0 \land u_2 \ge 0 \;\rightarrow\; d_1 + u_1 \ge \varepsilon \land d_2 + u_2 \ge \varepsilon)$$

Outline

1. Verification Calculus for Differential-algebraic Dynamic Logic d$\mathcal{L}$
   - Motivation for Differential Induction
   - Derivations and Differentiation
   - Differential Induction
   - Motivation for Differential Saturation
   - Differential Variants
   - Compositional Verification Calculus
   - Differential Transformation
   - Differential Reduction & Differential Elimination
   - Proof Rules
2. Soundness
3. Restricting Differential Invariants
4. Deductive Power

$\mathcal{R}$ Admissibility

Definition (Admissible substitution)

An application of a substitution σ is *admissible* if no variable x that σ replaces by σx occurs in the scope of a quantifier or modality binding x or a (logical or state) variable of the replacement σx. A modality *binds* variable x iff its DA-program changes x, i.e., contains a DJ-constraint with $x := \theta$ or a DA-constraint with x'.

Admissibility

Definition (Admissible substitution)

An application of a substitution σ is *admissible* if no variable x that σ replaces by σx occurs in the scope of a quantifier or modality binding x or a (logical or state) variable of the replacement σx. A modality *binds* variable x iff its DA-program changes x, i.e., contains a DJ-constraint with $x := \theta$ or a DA-constraint with x'.

All substitutions in all rules need to be admissible!

Rule Schema Applications

Definition (Rules)

Any instance

$$\frac{\Phi_1 \vdash \Psi_1 \quad \dots \quad \Phi_n \vdash \Psi_n}{\Phi_0 \vdash \Psi_0}$$

of a rule can be applied as a proof rule in context:

$$\frac{\Gamma, \Phi_1 \vdash \Psi_1, \Delta \quad \dots \quad \Gamma, \Phi_n \vdash \Psi_n, \Delta}{\Gamma, \Phi_0 \vdash \Psi_0, \Delta}$$

Γ, Δ are arbitrary finite sets of additional context formulas (including empty sets)

Rule Schema Applications

Definition (Rules)

Symmetric schemata can be applied on either side of the sequent: If

$$\frac{\phi_1}{\phi_0}$$

is an instance, then

$$\frac{\Gamma \vdash \phi_1, \Delta}{\Gamma \vdash \phi_0, \Delta} \qquad \text{and} \qquad \frac{\Gamma, \phi_1 \vdash \Delta}{\Gamma, \phi_0 \vdash \Delta}$$

can both be applied as proof rules of the d$\mathcal{L}$ calculus, where Γ, Δ are arbitrary finite sets of context formulas

Verification of Differential-algebraic Dynamic Logic

Propositional Rules

10 propositional rules

$$\frac{\vdash \phi}{\neg\phi \vdash} \qquad \frac{\phi, \psi \vdash}{\phi \land \psi \vdash} \qquad \frac{\phi \vdash \quad \psi \vdash}{\phi \lor \psi \vdash} \qquad \frac{\vdash \phi \quad \phi \vdash}{\vdash}$$

$$\frac{\phi \vdash}{\vdash \neg\phi} \qquad \frac{\vdash \phi \quad \vdash \psi}{\vdash \phi \land \psi} \qquad \frac{\vdash \phi, \psi}{\vdash \phi \lor \psi}$$

$$\frac{\phi \vdash \psi}{\vdash \phi \rightarrow \psi} \qquad \frac{\vdash \phi \quad \psi \vdash}{\phi \rightarrow \psi \vdash} \qquad \frac{}{\phi \vdash \phi}$$

Verification of Differential-algebraic Dynamic Logic

Dynamic Rules

$$\frac{\langle\alpha\rangle\langle\beta\rangle\phi}{\langle\alpha;\beta\rangle\phi} \qquad \frac{\exists x\,\langle\mathcal{J}\rangle\phi}{\langle\exists x\,\mathcal{J}\rangle\phi} \qquad \frac{\chi \wedge \phi_{x_1}^{\theta_1}\dots{}_{x_n}^{\theta_n}}{\langle x_1 := \theta_1 \wedge \dots \wedge x_n := \theta_n \wedge \chi\rangle\phi}$$

$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi} \qquad \frac{\forall x\,[\mathcal{J}]\phi}{[\exists x\,\mathcal{J}]\phi} \qquad \frac{\chi \rightarrow \phi_{x_1}^{\theta_1}\dots{}_{x_n}^{\theta_n}}{[x_1 := \theta_1 \wedge \dots \wedge x_n := \theta_n \wedge \chi]\phi}$$

$$\frac{\langle\alpha\rangle\phi \vee \langle\beta\rangle\phi}{\langle\alpha\cup\beta\rangle\phi} \qquad \frac{\langle\mathcal{J}_1 \cup \ldots \cup \mathcal{J}_n\rangle\phi}{\langle\mathcal{J}\rangle\phi} \qquad \frac{\langle(\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*\rangle\phi}{\langle\mathcal{D}\rangle\phi}$$

$$\frac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha\cup\beta]\phi} \qquad \frac{[\mathcal{J}_1 \cup \ldots \cup \mathcal{J}_n]\phi}{[\mathcal{J}]\phi} \qquad \frac{[(\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*]\phi}{[\mathcal{D}]\phi}$$

Dynamic Rules

$$\frac{\vdash [\mathcal{E}]\phi}{\vdash [\mathcal{D}]\phi} \qquad \frac{\vdash \langle\mathcal{D}\rangle\phi}{\vdash \langle\mathcal{E}\rangle\phi} \qquad \frac{\vdash [\mathcal{D}]\chi \quad \vdash [\mathcal{D} \land \chi]\phi}{\vdash [\mathcal{D}]\phi} \text{ where "}\mathcal{D} \rightarrow \mathcal{E}\text{"}$$

in $\mathrm{FOL}_{\mathbb{R}}$

Verification of Differential-algebraic Dynamic Logic

Global Rules

$$\frac{\vdash \forall^\alpha(\phi \to \psi)}{[\alpha]\phi \vdash [\alpha]\psi} \qquad \frac{\vdash \forall^\alpha(\phi \to \psi)}{\langle\alpha\rangle\phi \vdash \langle\alpha\rangle\psi} \qquad \frac{\vdash \forall^\alpha(F \to [\alpha]F)}{F \vdash [\alpha^*]F}$$

$$\frac{\vdash \forall^\alpha(\varphi(x) \to \langle\alpha\rangle\varphi(x-1))}{\exists v\, \varphi(v) \vdash \langle\alpha^*\rangle \exists v{\leq}0\, \varphi(v)}$$

$$\frac{\vdash \forall^\alpha \forall y_1 \ldots \forall y_k\, (\chi \to F'{}^{\theta_1}_{x_1'} \ldots {}^{\theta_n}_{x_n'})}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k\, (x_1' = \theta_1 \land \ldots \land x_n' = \theta_n \land \chi)]F}$$

$$\frac{\vdash \exists \varepsilon{>}0\, \forall^\alpha \forall y_1, y_k\, (\neg F \land \chi \to (F' \geq \varepsilon)^{\theta_1}_{x_1'} \ldots {}^{\theta_n}_{x_n'})}{[\exists y_1, y_k\, (x_1' = \theta_1 \land, \land x_n' = \theta_n \land \sim F)]\chi \vdash \langle \exists y_1, y_k\, (x_1' = \theta_1 \land, \land x_n' = \theta_n \land \chi)\rangle F}$$

$$\frac{\vdash \phi(s(X_1,\dots,X_n))}{\vdash \forall x\, \phi(x)} \qquad \frac{\vdash \phi(X)}{\vdash \exists x\, \phi(x)}$$

$$\frac{\phi(s(X_1,\dots,X_n)) \vdash}{\exists x\, \phi(x) \vdash} \qquad \frac{\phi(X) \vdash}{\forall x\, \phi(x) \vdash}$$

s new, $\{X_1,\dots,X_n\} = FV(\exists x\, \phi(x))$ $\qquad$ X new variable

$$\frac{\vdash \mathrm{QE}(\forall X\, (\Phi(X) \vdash \Psi(X)))}{\Phi(s(X_1,\dots,X_n)) \vdash \Psi(s(X_1,\dots,X_n))} \qquad \frac{\vdash \mathrm{QE}(\exists X\, \bigwedge_i(\Phi_i \vdash \Psi_i))}{\Phi_1 \vdash \Psi_1 \quad \dots \quad \Phi_n \vdash \Psi_n}$$

X new variable $\qquad$ X only in branches $\Phi_i \vdash \Psi_i$

QE needs to be defined in premiss

Outline

1. Verification Calculus for Differential-algebraic Dynamic Logic d$\mathcal{L}$
   - Motivation for Differential Induction
   - Derivations and Differentiation
   - Differential Induction
   - Motivation for Differential Saturation
   - Differential Variants
   - Compositional Verification Calculus
   - Differential Transformation
   - Differential Reduction & Differential Elimination
   - Proof Rules
2. Soundness
3. Restricting Differential Invariants
4. Deductive Power

Soundness

Theorem (Soundness)

DAL *calculus is sound, i.e.,*

$$\vdash \phi \quad \Rightarrow \quad \vDash \phi$$

Definition (Local Soundness)

$$\frac{\Phi}{\Psi} \text{ locally sound iff for each } v \ (v \models \Phi \quad \Rightarrow \quad v \models \Psi)$$

Soundness

Theorem (Soundness)

DAL *calculus is sound, i.e.,*

$$\vdash \phi \quad \Rightarrow \quad \vDash \phi$$

Challenges (Soundness Proof)

Definition (Local Soundness)

$$\frac{\Phi}{\Psi} \quad \text{locally sound iff for each } v \ (v \vDash \Phi \quad \Rightarrow \quad v \vDash \Psi)$$

Soundness

Theorem (Soundness)

DAL *calculus is sound, i.e.,*

$$\vdash \phi \quad \Rightarrow \quad \vDash \phi$$

Challenges (Soundness Proof)

- Differential induction

Definition (Local Soundness)

$$\frac{\Phi}{\Psi} \quad \text{locally sound iff for each } v \ (v \vDash \Phi \quad \Rightarrow \quad v \vDash \Psi)$$

Soundness

Theorem (Soundness)

DAL *calculus is sound, i.e.,*

$$\vdash \phi \quad \Rightarrow \quad \vDash \phi$$

Challenges (Soundness Proof)

- Differential induction
- Side deductions

Definition (Local Soundness)

$$\frac{\Phi}{\Psi} \quad \text{locally sound iff} \;\; \text{for each} \;\; v \;\; (v \vDash \Phi \quad \Rightarrow \quad v \vDash \Psi)$$

Soundness Proof

$$\frac{[(\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*]\phi}{[\mathcal{D}]\phi}$$

Proof (locally sound).

- diff.trafo. $\Rightarrow$ there is an equivalent DNF $\mathcal{D}_1 \vee \cdots \vee \mathcal{D}_n$ of $\mathcal{D}$.

Soundness Proof

$$\frac{[(\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*]\phi}{[\mathcal{D}]\phi}$$

Proof (locally sound).

- diff.trafo. ⇒ there is an equivalent DNF $\mathcal{D}_1 \vee \cdots \vee \mathcal{D}_n$ of $\mathcal{D}$.
- $\rho(\mathcal{D}) \supseteq \rho((\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*)$ obvious

□

Soundness Proof

$$\frac{[(\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*]\phi}{[\mathcal{D}]\phi}$$

Proof (locally sound).

- diff.trafo. $\Rightarrow$ there is an equivalent DNF $\mathcal{D}_1 \vee \cdots \vee \mathcal{D}_n$ of $\mathcal{D}$.
- $\rho(\mathcal{D}) \supseteq \rho((\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*)$ obvious
- $\rho(\mathcal{D}) \subseteq \rho((\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*)$ to show.

□

Soundness Proof

$$\frac{[(\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*]\phi}{[\mathcal{D}]\phi}$$

Proof (locally sound).

- diff.trafo. $\Rightarrow$ there is an equivalent DNF $\mathcal{D}_1 \vee \cdots \vee \mathcal{D}_n$ of $\mathcal{D}$.
- $\rho(\mathcal{D}) \supseteq \rho((\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*)$ obvious
- $\rho(\mathcal{D}) \subseteq \rho((\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*)$ to show.
- Let φ state flow for a transition $(v, \omega) \in \rho(\mathcal{D})$.

□

Soundness Proof

$$\frac{[(\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*]\phi}{[\mathcal{D}]\phi}$$

Proof (locally sound).

- diff.trafo. $\Rightarrow$ there is an equivalent DNF $\mathcal{D}_1 \vee \cdots \vee \mathcal{D}_n$ of $\mathcal{D}$.
- $\rho(\mathcal{D}) \supseteq \rho((\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*)$ obvious
- $\rho(\mathcal{D}) \subseteq \rho((\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*)$ to show.
- Let φ state flow for a transition $(v, \omega) \in \rho(\mathcal{D})$.
- Assume φ non-Zeno.

Soundness Proof

$$\frac{[(\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*]\phi}{[\mathcal{D}]\phi}$$

Proof (locally sound).

- diff.trafo. $\Rightarrow$ there is an equivalent DNF $\mathcal{D}_1 \vee \cdots \vee \mathcal{D}_n$ of $\mathcal{D}$.
- $\rho(\mathcal{D}) \supseteq \rho((\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*)$ obvious
- $\rho(\mathcal{D}) \subseteq \rho((\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*)$ to show.
- Let φ state flow for a transition $(v, \omega) \in \rho(\mathcal{D})$.
- Assume φ non-Zeno.
- Finite number, m, of switches between $\mathcal{D}_i$, say $\mathcal{D}_{i_1}, \mathcal{D}_{i_2}, \ldots, \mathcal{D}_{i_m}$.

Soundness Proof

$$\frac{[(\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*]\phi}{[\mathcal{D}]\phi}$$

Proof (locally sound).

- diff.trafo. $\Rightarrow$ there is an equivalent DNF $\mathcal{D}_1 \vee \cdots \vee \mathcal{D}_n$ of $\mathcal{D}$.
- $\rho(\mathcal{D}) \supseteq \rho((\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*)$ obvious
- $\rho(\mathcal{D}) \subseteq \rho((\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*)$ to show.
- Let φ state flow for a transition $(v, \omega) \in \rho(\mathcal{D})$.
- Assume φ non-Zeno.
- Finite number, m, of switches between $\mathcal{D}_i$, say $\mathcal{D}_{i_1}, \mathcal{D}_{i_2}, \ldots, \mathcal{D}_{i_m}$.
- Transition (v, ω) belonging to φ can be simulated piecewise by m repetitions of $\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n$:

□

Soundness Proof

$$\frac{[(\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*]\phi}{[\mathcal{D}]\phi}$$

Proof (locally sound).

- diff.trafo. $\Rightarrow$ there is an equivalent DNF $\mathcal{D}_1 \vee \cdots \vee \mathcal{D}_n$ of $\mathcal{D}$.
- $\rho(\mathcal{D}) \supseteq \rho((\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*)$ obvious
- $\rho(\mathcal{D}) \subseteq \rho((\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n)^*)$ to show.
- Let φ state flow for a transition $(v, \omega) \in \rho(\mathcal{D})$.
- Assume φ non-Zeno.
- Finite number, m, of switches between $\mathcal{D}_i$, say $\mathcal{D}_{i_1}, \mathcal{D}_{i_2}, \ldots, \mathcal{D}_{i_m}$.
- Transition (v, ω) belonging to φ can be simulated piecewise by m repetitions of $\mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n$:
- Each piece selects the respective part $\mathcal{D}_{i_j}$.

□

Soundness Proof

$$\frac{\vdash [\mathcal{E}]\phi}{\vdash [\mathcal{D}]\phi} \quad \text{where "}\mathcal{D} \rightarrow \mathcal{E}\text{" in } \mathrm{FOL}_{\mathbb{R}}$$

$$\frac{\vdash \langle\mathcal{D}\rangle\phi}{\vdash \langle\mathcal{E}\rangle\phi}$$

Proof (locally sound).

- Immediate consequence of diff.trafo. and semantics of modalities. ▸

□

Soundness Proof

$$\frac{\vdash [\mathcal{D}]\chi \quad \vdash [\mathcal{D} \land \chi]\phi}{\vdash [\mathcal{D}]\phi}$$

Proof (locally sound).

- Left premiss $\Rightarrow$ every flow φ that satisfies $\mathcal{D}$ also satisfies χ *all along* the flow, i.e., $\varphi \models \chi$.

□

Soundness Proof

$$\frac{\vdash [\mathcal{D}]\chi \quad \vdash [\mathcal{D} \land \chi]\phi}{\vdash [\mathcal{D}]\phi}$$

Proof (locally sound).

- Left premiss $\Rightarrow$ every flow φ that satisfies $\mathcal{D}$ also satisfies χ *all along* the flow, i.e., $\varphi \models \chi$.
- Thus, $\varphi \models \mathcal{D}$ implies $\varphi \models \mathcal{D} \land \chi$

□

Soundness Proof

$$\frac{\vdash [\mathcal{D}]\chi \quad \vdash [\mathcal{D} \land \chi]\phi}{\vdash [\mathcal{D}]\phi}$$

Proof (locally sound).

- Left premiss $\Rightarrow$ every flow φ that satisfies $\mathcal{D}$ also satisfies χ *all along* the flow, i.e., $\varphi \models \chi$.
- Thus, $\varphi \models \mathcal{D}$ implies $\varphi \models \mathcal{D} \land \chi$
- Right premiss entails the conclusion.

□

Soundness Proof

$$\frac{\vdash \forall^{\alpha}\forall y_1 \ldots \forall y_k\,(\chi \to {F'}^{\theta_1}_{x_1'} \ldots {}^{\theta_n}_{x_n'})}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k\,(x_1' = \theta_1 \land \ldots \land x_n' = \theta_n \land \chi)]F}$$

Proof (locally sound).

- Let v satisfy premiss and antecedent of conclusion.

Soundness Proof

$$\frac{\vdash \forall^{\alpha} \forall y_1 \ldots \forall y_k \, (\chi \rightarrow F'^{\theta_1}_{x'_1} \ldots {}^{\theta_n}_{x'_n})}{[\exists y_1 \ldots \exists y_k \, \chi] F \vdash [\exists y_1 \ldots \exists y_k \, (x'_1 = \theta_1 \land \ldots \land x'_n = \theta_n \land \chi)] F}$$

Proof (locally sound).

- Let v satisfy premiss and antecedent of conclusion.
- Diff.trafo. $\Rightarrow$ assume F in DNF. Consider disjunct G of F with $v \models G$.

Soundness Proof

$$\frac{\vdash \forall^\alpha \forall y_1 \ldots \forall y_k\, (\chi \to F'^{\theta_1}_{x'_1} \cdots ^{\theta_n}_{x'_n})}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k\, (x'_1 = \theta_1 \land \ldots \land x'_n = \theta_n \land \chi)]F}$$

Proof (locally sound).

- Let v satisfy premiss and antecedent of conclusion.
- Diff.trafo. $\Rightarrow$ assume F in DNF. Consider disjunct G of F with $v \models G$.
- F continuous invariant if, say, each conjunct of G is.

Soundness Proof

$$\frac{\vdash \forall^{\alpha}\forall y_1 \ldots \forall y_k \left(\chi \to {F'}^{\theta_1}_{x'_1} \ldots {}^{\theta_n}_{x'_n}\right)}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k\, (x'_1 = \theta_1 \land \ldots \land x'_n = \theta_n \land \chi)]F}$$

Proof (locally sound).

- Let v satisfy premiss and antecedent of conclusion.
- Diff.trafo. $\Rightarrow$ assume F in DNF. Consider disjunct G of F with $v \models G$.
- F continuous invariant if, say, each conjunct of G is.
- Assume conjunct is $c \geq 0$ (accordingly for $c > 0$).

Soundness Proof

$$\frac{\vdash \forall^{\alpha}\forall y_1 \ldots \forall y_k\,(\chi \to F'^{\theta_1}_{x_1'}\ldots^{\theta_n}_{x_n'})}{[\exists y_1 \ldots \exists y_k\,\chi]F \vdash [\exists y_1 \ldots \exists y_k\,(x_1' = \theta_1 \land \ldots \land x_n' = \theta_n \land \chi)]F}$$

Proof (locally sound).

- Let v satisfy premiss and antecedent of conclusion.
- Diff.trafo. $\Rightarrow$ assume F in DNF. Consider disjunct G of F with $v \models G$.
- F continuous invariant if, say, each conjunct of G is.
- Assume conjunct is $c \geq 0$ (accordingly for $c > 0$).
- Let $\varphi : [0, r] \to$ States flow with $\varphi \models \exists y\,(x' = \theta \land \chi)$ and $\varphi(0) = v$.

Soundness Proof

$$\frac{\vdash \forall^{\alpha} \forall y_1 \ldots \forall y_k \, (\chi \rightarrow F'^{\theta_1}_{x'_1} \cdots {}^{\theta_n}_{x'_n})}{[\exists y_1 \ldots \exists y_k \, \chi]F \vdash [\exists y_1 \ldots \exists y_k \, (x'_1 = \theta_1 \wedge \ldots \wedge x'_n = \theta_n \wedge \chi)]F}$$

Proof (locally sound).

- Let v satisfy premiss and antecedent of conclusion.
- Diff.trafo. $\Rightarrow$ assume F in DNF. Consider disjunct G of F with $v \models G$.
- F continuous invariant if, say, each conjunct of G is.
- Assume conjunct is $c \geq 0$ (accordingly for $c > 0$).
- Let $\varphi : [0, r] \rightarrow$ States flow with $\varphi \models \exists y \, (x' = \theta \wedge \chi)$ and $\varphi(0) = v$.

$\Rightarrow$ $\varphi \models \exists y \, \chi$, thus $v \models F$, i.e., $c \geq 0$ holds at v.

Soundness Proof

$$\frac{\vdash \forall^{\alpha}\forall y_1 \ldots \forall y_k \, (\chi \to F'^{\theta_1}_{x'_1} \ldots {}^{\theta_n}_{x'_n})}{[\exists y_1 \ldots \exists y_k \, \chi]F \vdash [\exists y_1 \ldots \exists y_k \, (x'_1 = \theta_1 \land \ldots \land x'_n = \theta_n \land \chi)]F}$$

Proof (locally sound).

- Let v satisfy premiss and antecedent of conclusion.
- Diff.trafo. $\Rightarrow$ assume F in DNF. Consider disjunct G of F with $v \models G$.
- F continuous invariant if, say, each conjunct of G is.
- Assume conjunct is $c \geq 0$ (accordingly for $c > 0$).
- Let $\varphi : [0, r] \to$ States flow with $\varphi \models \exists y \, (x' = \theta \land \chi)$ and $\varphi(0) = v$.

$\Rightarrow$ $\varphi \models \exists y \, \chi$, thus $v \models F$, i.e., $c \geq 0$ holds at v.

- Assume duration $r > 0$ (otherwise $v \models c \geq 0$ already holds).

Soundness Proof

$$\frac{\vdash \forall^{\alpha}\forall y_1 \ldots \forall y_k \, (\chi \rightarrow F'^{\theta_1}_{x'_1} \cdots ^{\theta_n}_{x'_n})}{[\exists y_1 \ldots \exists y_k \, \chi]F \vdash [\exists y_1 \ldots \exists y_k \, (x'_1 = \theta_1 \land \ldots \land x'_n = \theta_n \land \chi)]F}$$

Proof (locally sound).

- Let v satisfy premiss and antecedent of conclusion.
- Diff.trafo. $\Rightarrow$ assume F in DNF. Consider disjunct G of F with $v \models G$.
- F continuous invariant if, say, each conjunct of G is.
- Assume conjunct is $c \geq 0$ (accordingly for $c > 0$).
- Let $\varphi : [0, r] \rightarrow$ States flow with $\varphi \models \exists y \, (x' = \theta \land \chi)$ and $\varphi(0) = v$.

$\Rightarrow$ $\varphi \models \exists y \, \chi$, thus $v \models F$, i.e., $c \geq 0$ holds at v.

- Assume duration $r > 0$ (otherwise $v \models c \geq 0$ already holds).
- Show $\varphi \models c \geq 0$.

Soundness Proof

$$\frac{\vdash \forall^{\alpha}\forall y_1 \ldots \forall y_k \, (\chi \to F'^{\theta_1}_{x_1'} \cdots {}^{\theta_n}_{x_n'})}{[\exists y_1 \ldots \exists y_k \, \chi]F \vdash [\exists y_1 \ldots \exists y_k \, (x_1' = \theta_1 \land \ldots \land x_n' = \theta_n \land \chi)]F}$$

Proof (locally sound).

- By contradiction suppose there was a $\zeta \in [0, r]$ where $\varphi(\zeta) \models c < 0$.

□

Soundness Proof

$$\frac{\vdash \forall^\alpha \forall y_1 \ldots \forall y_k\, (\chi \to F'{}^{\theta_1}_{x_1'} \cdots {}^{\theta_n}_{x_n'})}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k\, (x_1' = \theta_1 \land \ldots \land x_n' = \theta_n \land \chi)]F}$$

Proof (locally sound).

- By contradiction suppose there was a $\zeta \in [0, r]$ where $\varphi(\zeta) \models c < 0$.

$\Rightarrow$ $h : [0, r] \to \mathbb{R}; h(t) = [\![c]\!]_{\varphi(t)}$ satisfies $h(0) \geq 0 > h(\zeta)$, because $v \models c \geq 0$ by antecedent.

□

Soundness Proof

$$\frac{\vdash \forall^{\alpha}\forall y_1 \ldots \forall y_k \, (\chi \rightarrow F'^{\theta_1}_{x_1'} \ldots {}^{\theta_n}_{x_n'})}{[\exists y_1 \ldots \exists y_k \, \chi]F \vdash [\exists y_1 \ldots \exists y_k \, (x_1' = \theta_1 \wedge \ldots \wedge x_n' = \theta_n \wedge \chi)]F}$$

Proof (locally sound).

- By contradiction suppose there was a $\zeta \in [0, r]$ where $\varphi(\zeta) \models c < 0$.

$\Rightarrow$ $h : [0, r] \rightarrow \mathbb{R}; h(t) = [\![c]\!]_{\varphi(t)}$ satisfies $h(0) \geq 0 > h(\zeta)$, because $v \models c \geq 0$ by antecedent.

- φ is of order of c': $\operatorname{ord}_x \varphi \geq 1$, $\operatorname{ord}_z \varphi = \infty$ for unchanged z.

□

Soundness Proof

$$\frac{\vdash \forall^\alpha \forall y_1 \ldots \forall y_k\, (\chi \rightarrow {F'}_{x_1'}^{\theta_1} \cdots {}_{x_n'}^{\theta_n})}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k\, (x_1' = \theta_1 \land \ldots \land x_n' = \theta_n \land \chi)]F}$$

Proof (locally sound).

- By contradiction suppose there was a $\zeta \in [0, r]$ where $\varphi(\zeta) \models c < 0$.

$\Rightarrow$ $h : [0, r] \rightarrow \mathbb{R}; h(t) = [\![c]\!]_{\varphi(t)}$ satisfies $h(0) \geq 0 > h(\zeta)$, because $v \models c \geq 0$ by antecedent.

- φ is of order of c': $\operatorname{ord}_x \varphi \geq 1$, $\operatorname{ord}_z \varphi = \infty$ for unchanged z.
- By α-renaming, c' cannot contain quantified variables y, hence, φ is not required to be of any order in y.

□

Soundness Proof

$$\frac{\vdash \forall^{\alpha}\forall y_1 \ldots \forall y_k \left(\chi \to F'^{\theta_1}_{x'_1} \ldots ^{\theta_n}_{x'_n}\right)}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k\, (x'_1 = \theta_1 \land \ldots \land x'_n = \theta_n \land \chi)]F}$$

Proof (locally sound).

- By contradiction suppose there was a $\zeta \in [0, r]$ where $\varphi(\zeta) \models c < 0$.

$\Rightarrow$ $h : [0, r] \to \mathbb{R}; h(t) = [\![c]\!]_{\varphi(t)}$ satisfies $h(0) \geq 0 > h(\zeta)$, because $v \models c \geq 0$ by antecedent.

- φ is of order of c': $\operatorname{ord}_x \varphi \geq 1$, $\operatorname{ord}_z \varphi = \infty$ for unchanged z.
- By α-renaming, c' cannot contain quantified variables y, hence, φ is not required to be of any order in y.
- Value of c defined along φ, as χ guards against zeros division.

□

Soundness Proof

$$\frac{\vdash \forall^\alpha \forall y_1 \ldots \forall y_k\, (\chi \rightarrow F'^{\theta_1}_{x_1'} \ldots {}^{\theta_n}_{x_n'})}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k\, (x_1' = \theta_1 \wedge \ldots \wedge x_n' = \theta_n \wedge \chi)]F}$$

Proof (locally sound).

- By contradiction suppose there was a $\zeta \in [0, r]$ where $\varphi(\zeta) \models c < 0$.

$\Rightarrow$ $h : [0, r] \rightarrow \mathbb{R}; h(t) = [\![c]\!]_{\varphi(t)}$ satisfies $h(0) \geq 0 > h(\zeta)$, because $v \models c \geq 0$ by antecedent.

- φ is of order of c': $\operatorname{ord}_x \varphi \geq 1$, $\operatorname{ord}_z \varphi = \infty$ for unchanged z.
- By α-renaming, c' cannot contain quantified variables y, hence, φ is not required to be of any order in y.
- Value of c defined along φ, as χ guards against zeros division.
- Thus, by derivation lemma, h is continuous on $[0, r]$ and differentiable at every $\xi \in (0, r)$.

□

Soundness Proof

$$\frac{\vdash \forall^{\alpha} \forall y_1 \ldots \forall y_k \, (\chi \rightarrow {F'}^{\theta_1}_{x_1'} \ldots {}^{\theta_n}_{x_n'})}{[\exists y_1 \ldots \exists y_k \, \chi]F \vdash [\exists y_1 \ldots \exists y_k \, (x_1' = \theta_1 \land \ldots \land x_n' = \theta_n \land \chi)]F}$$

Proof (locally sound).

- Mean value theorem $\Rightarrow$ there is $\xi \in (0, \zeta)$ such that

$$\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) \cdot (\underbrace{\zeta - 0}_{}) = h(\zeta) - h(0) < 0$$

Soundness Proof

$$\frac{\vdash \forall^{\alpha}\forall y_1 \ldots \forall y_k \, (\chi \rightarrow {F'}^{\theta_1}_{x_1'} \ldots {}^{\theta_n}_{x_n'})}{[\exists y_1 \ldots \exists y_k \, \chi]F \vdash [\exists y_1 \ldots \exists y_k \, (x_1' = \theta_1 \land \ldots \land x_n' = \theta_n \land \chi)]F}$$

Proof (locally sound).

- Mean value theorem $\Rightarrow$ there is $\xi \in (0, \zeta)$ such that

$$\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) \cdot (\underbrace{\zeta - 0}_{\geq 0}) = h(\zeta) - h(0) < 0$$

Soundness Proof

$$\frac{\vdash \forall^\alpha \forall y_1 \ldots \forall y_k\, (\chi \to {F'}^{\theta_1}_{x'_1} \cdots {}^{\theta_n}_{x'_n})}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k\, (x'_1 = \theta_1 \land \ldots \land x'_n = \theta_n \land \chi)]F}$$

Proof (locally sound).

- Mean value theorem $\Rightarrow$ there is $\xi \in (0, \zeta)$ such that

$$\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) \cdot (\underbrace{\zeta - 0}_{\geq 0}) = h(\zeta) - h(0) < 0$$

$$0 > \frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) \overset{deriv.lem}{=} [\![c']\!]_{\bar{\varphi}(\xi)}$$

Soundness Proof

$$\frac{\vdash \forall^{\alpha} \forall y_1 \ldots \forall y_k\, (\chi \to F'^{\theta_1}_{x'_1} \ldots {}^{\theta_n}_{x'_n})}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k\, (x'_1 = \theta_1 \land \ldots \land x'_n = \theta_n \land \chi)]F}$$

Proof (locally sound).

- Mean value theorem $\Rightarrow$ there is $\xi \in (0, \zeta)$ such that

$$\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) \cdot (\underbrace{\zeta - 0}_{\geq 0}) = h(\zeta) - h(0) < 0$$

$$0 > \frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) \overset{deriv.lem}{=} [\![c']\!]_{\bar{\varphi}(\xi)} \overset{diff.subst}{=} [\![c'^{\theta}_{x'}]\!]_{\bar{\varphi}(\xi)^{u}_{y}}$$

because $\varphi \models \exists y\, (x' = \theta \land \chi)$ so that $\bar{\varphi}(\xi)^{u}_{y} \models x' = \theta \land \chi$ for some $u \in \mathbb{R}$ and because y' does not occur and $y \notin c$.

Soundness Proof

$$\frac{\vdash \forall^\alpha \forall y_1 \ldots \forall y_k \left(\chi \to F'{}^{\theta_1}_{x'_1} \ldots {}^{\theta_n}_{x'_n}\right)}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k\, (x'_1 = \theta_1 \land \ldots \land x'_n = \theta_n \land \chi)]F}$$

Proof (locally sound).

- Mean value theorem $\Rightarrow$ there is $\xi \in (0, \zeta)$ such that

$$\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) \cdot (\underbrace{\zeta - 0}_{\geq 0}) = h(\zeta) - h(0) < 0$$

$$0 > \frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) \overset{deriv.lem}{=} [\![c']\!]_{\bar\varphi(\xi)} \overset{diff.subst}{=} [\![c'{}^{\theta}_{x'}]\!]_{\bar\varphi(\xi)^u_y}$$

because $\varphi \models \exists y\, (x' = \theta \land \chi)$ so that $\bar\varphi(\xi)^u_y \models x' = \theta \land \chi$ for some $u \in \mathbb{R}$ and because y' does not occur and $y \notin c$.

- Contradiction: by premiss $\varphi \models \forall y\, (\chi \to c'{}^{\theta}_{x'} \geq 0)$ as $\forall^\alpha$ comprises all changed variables.

Soundness Proof

$$\frac{\vdash \forall^\alpha \forall y_1 \ldots \forall y_k\, (\chi \rightarrow F'^{\theta_1}_{x'_1} \ldots {}^{\theta_n}_{x'_n})}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k\, (x'_1 = \theta_1 \land \ldots \land x'_n = \theta_n \land \chi)]F}$$

Proof (locally sound).

- Mean value theorem $\Rightarrow$ there is $\xi \in (0, \zeta)$ such that

$$\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) \cdot (\underbrace{\zeta - 0}_{\geq 0}) = h(\zeta) - h(0) < 0$$

$$0 > \frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) \overset{deriv.lem}{=} [\![c']\!]_{\bar{\varphi}(\xi)} \overset{diff.subst}{=} [\![c'^{\theta}_{x'}]\!]_{\bar{\varphi}(\xi)^u_y}$$

because $\varphi \models \exists y\, (x' = \theta \land \chi)$ so that $\bar{\varphi}(\xi)^u_y \models x' = \theta \land \chi$ for some $u \in \mathbb{R}$ and because y' does not occur and $y \notin c$.

- Contradiction: by premiss $\varphi \models \forall y\, (\chi \rightarrow c'^{\theta}_{x'} \geq 0)$ as $\forall^\alpha$ comprises all changed variables. For $\bar{\varphi}(\xi)^u_y \models \chi$, we have $\bar{\varphi}(\xi)^u_y \models c'^{\theta}_{x'} \geq 0$.

Soundness Proof

$$\frac{\vdash \exists \varepsilon{>}0\, \forall^{\alpha} \forall y_1, y_k\, (\neg F \land \chi \rightarrow (F' \geq \varepsilon)_{x_1'}^{\theta_1} \dots {}_{x_n'}^{\theta_n})}{[\exists y_1, y_k\, (x_1' = \theta_1 \land, \land x_n' = \theta_n \land {\sim} F)]\chi \vdash \langle \exists y_1, y_k\, (x_1' = \theta_1 \land, \land x_n' = \theta_n \land \chi)\rangle F}$$

Proof (locally sound, quantifier free case).

- Let v satisfy premiss and antecedent of conclusion.

□

Soundness Proof

$$\frac{\vdash \exists \varepsilon{>}0\, \forall^{\alpha} \forall y_1, y_k\, (\neg F \land \chi \rightarrow (F' \geq \varepsilon)^{\theta_1}_{x'_1} \cdots ^{\theta_n}_{x'_n})}{[\exists y_1, y_k\, (x'_1 = \theta_1 \land, \land x'_n = \theta_n \land {\sim} F)]\chi \vdash \langle \exists y_1, y_k\, (x'_1 = \theta_1 \land, \land x'_n = \theta_n \land \chi)\rangle F}$$

Proof (locally sound, quantifier free case).

- Let v satisfy premiss and antecedent of conclusion.
- After α-renaming, ε fresh, thus $v \models \forall^{\alpha}(\neg F \land \chi \rightarrow (F' \geq \varepsilon)^{\theta}_{x'})$.

□

Soundness Proof

$$\frac{\vdash \exists\varepsilon{>}0\,\forall^{\alpha}\forall y_1, y_k\,(\neg F \wedge \chi \rightarrow (F' \geq \varepsilon)^{\theta_1}_{x_1'}\cdots^{\theta_n}_{x_n'})}{[\exists y_1, y_k\,(x_1' = \theta_1 \wedge, \wedge x_n' = \theta_n \wedge \sim\! F)]\chi \vdash \langle\exists y_1, y_k\,(x_1' = \theta_1 \wedge, \wedge x_n' = \theta_n \wedge \chi)\rangle F}$$

Proof (locally sound, quantifier free case).

- Let v satisfy premiss and antecedent of conclusion.
- After α-renaming, ε fresh, thus $v \models \forall^{\alpha}(\neg F \wedge \chi \rightarrow (F' \geq \varepsilon)^{\theta}_{x'})$.
- We required Lipschitz-continuity. Global Picard-Lindelöf theorem $\Rightarrow$ there is a global solution of arbitrary duration $r \geq 0$.

□

Soundness Proof

$$\frac{\vdash \exists \varepsilon{>}0\, \forall^{\alpha} \forall y_1, y_k \, (\neg F \land \chi \to (F' \geq \varepsilon)^{\theta_1}_{x'_1} \cdots^{\theta_n}_{x'_n})}{[\exists y_1, y_k \, (x'_1 = \theta_1 \land, \land x'_n = \theta_n \land \sim F)]\chi \vdash \langle \exists y_1, y_k \, (x'_1 = \theta_1 \land, \land x'_n = \theta_n \land \chi)\rangle F}$$

Proof (locally sound, quantifier free case).

- Let v satisfy premiss and antecedent of conclusion.
- After α-renaming, ε fresh, thus $v \models \forall^{\alpha}(\neg F \land \chi \to (F' \geq \varepsilon)^{\theta}_{x'})$.
- We required Lipschitz-continuity. Global Picard-Lindelöf theorem $\Rightarrow$ there is a global solution of arbitrary duration $r \geq 0$.
- Let $\varphi \models x' = \theta$ start in v of some duration $r \geq 0$.

□

Soundness Proof

$$\frac{\vdash \exists \varepsilon{>}0\, \forall^{\alpha} \forall y_1, y_k\, (\neg F \wedge \chi \rightarrow (F' \geq \varepsilon)^{\theta_1}_{x_1'} \cdots {}^{\theta_n}_{x_n'})}{[\exists y_1, y_k\, (x_1' = \theta_1 \wedge, \wedge x_n' = \theta_n \wedge \sim F)]\chi \vdash \langle \exists y_1, y_k\, (x_1' = \theta_1 \wedge, \wedge x_n' = \theta_n \wedge \chi)\rangle F}$$

Proof (locally sound, quantifier free case).

- Let v satisfy premiss and antecedent of conclusion.
- After α-renaming, ε fresh, thus $v \models \forall^{\alpha}(\neg F \wedge \chi \rightarrow (F' \geq \varepsilon)^{\theta}_{x'})$.
- We required Lipschitz-continuity. Global Picard-Lindelöf theorem $\Rightarrow$ there is a global solution of arbitrary duration $r \geq 0$.
- Let $\varphi \models x' = \theta$ start in v of some duration $r \geq 0$.
- If there is ζ with $\varphi(\zeta) \models F$, then by antecedent, until (including, as $\sim F$ contains closure of $\neg F$) "first" ζ, χ holds during φ.

□

Soundness Proof

$$\frac{\vdash \exists \varepsilon{>}0\, \forall^{\alpha} \forall y_1, y_k\, (\neg F \land \chi \to (F' \geq \varepsilon)^{\theta_1}_{x_1'} \cdots {}^{\theta_n}_{x_n'})}{[\exists y_1, y_k\, (x_1' = \theta_1 \land, \land x_n' = \theta_n \land \sim F)]\chi \vdash \langle \exists y_1, y_k\, (x_1' = \theta_1 \land, \land x_n' = \theta_n \land \chi)\rangle F}$$

Proof (locally sound, quantifier free case).

- Let v satisfy premiss and antecedent of conclusion.
- After α-renaming, ε fresh, thus $v \models \forall^{\alpha}(\neg F \land \chi \to (F' \geq \varepsilon)^{\theta}_{x'})$.
- We required Lipschitz-continuity. Global Picard-Lindelöf theorem $\Rightarrow$ there is a global solution of arbitrary duration $r \geq 0$.
- Let $\varphi \models x' = \theta$ start in v of some duration $r \geq 0$.
- If there is ζ with $\varphi(\zeta) \models F$, then by antecedent, until (including, as $\sim F$ contains closure of $\neg F$) “first” ζ, χ holds during φ.
- Hence, restriction of φ to $[0, \zeta]$ is flow for $v \models \langle x' = \theta \land \chi \rangle F$.

□

Soundness Proof

$$\frac{\vdash \exists \varepsilon{>}0\, \forall^{\alpha} \forall y_1, y_k\, (\neg F \wedge \chi \rightarrow (F' \geq \varepsilon)^{\theta_1}_{x_1'} \dots {}^{\theta_n}_{x_n'})}{[\exists y_1, y_k\, (x_1' = \theta_1 \wedge, \wedge x_n' = \theta_n \wedge {\sim}F)]\chi \vdash \langle \exists y_1, y_k\, (x_1' = \theta_1 \wedge, \wedge x_n' = \theta_n \wedge \chi)\rangle F}$$

Proof (locally sound, quantified case).

- If there is no such ζ, extending φ by larger r will make F true:

□

Soundness Proof

$$\frac{\vdash \exists\varepsilon{>}0\,\forall^\alpha\forall y_1, y_k\,(\neg F \wedge \chi \rightarrow (F' \geq \varepsilon)_{x_1'}^{\theta_1}\dots{}_{x_n'}^{\theta_n})}{[\exists y_1, y_k\,(x_1' = \theta_1 \wedge, \wedge x_n' = \theta_n \wedge \sim F)]\chi \vdash \langle \exists y_1, y_k\,(x_1' = \theta_1 \wedge, \wedge x_n' = \theta_n \wedge \chi)\rangle F}$$

Proof (locally sound, quantified case).

- If there is no such ζ, extending φ by larger r will make F true:
- Thus $\varphi \models \neg F \wedge \chi$ and, by premiss, $\varphi \models {F'}_{x'}^{\theta} \geq \varepsilon$, because $\forall^\alpha$ comprises all changed variables.

$\square$

Soundness Proof

$$\frac{\vdash \exists\varepsilon{>}0\,\forall^\alpha\forall y_1, y_k\,(\neg F \land \chi \rightarrow (F' \geq \varepsilon)^{\theta_1}_{x_1'}\dots^{\theta_n}_{x_n'})}{[\exists y_1, y_k\,(x_1' = \theta_1 \land, \land x_n' = \theta_n \land {\sim}F)]\chi \vdash \langle\exists y_1, y_k\,(x_1' = \theta_1 \land, \land x_n' = \theta_n \land \chi)\rangle F}$$

Proof (locally sound, quantified case).

- If there is no such ζ, extending φ by larger r will make F true:
- Thus $\varphi \models \neg F \land \chi$ and, by premiss, $\varphi \models F'^{\theta}_{x'} \geq \varepsilon$, because $\forall^\alpha$ comprises all changed variables.
- $F'^{\theta}_{x'} \geq \varepsilon$ is a conjunction.

□

Soundness Proof

$$\frac{\vdash \exists\varepsilon{>}0\,\forall^{\alpha}\forall y_1, y_k\,(\neg F \wedge \chi \to (F' \geq \varepsilon)^{\theta_1}_{x'_1}\dots{}^{\theta_n}_{x'_n})}{[\exists y_1, y_k\,(x'_1 = \theta_1 \wedge, \wedge x'_n = \theta_n \wedge \sim F)]\chi \vdash \langle \exists y_1, y_k\,(x'_1 = \theta_1 \wedge, \wedge x'_n = \theta_n \wedge \chi)\rangle F}$$

Proof (locally sound, quantified case).

- If there is no such ζ, extending φ by larger r will make F true:
- Thus $\varphi \models \neg F \wedge \chi$ and, by premiss, $\varphi \models F'^{\theta}_{x'} \geq \varepsilon$, because $\forall^{\alpha}$ comprises all changed variables.
- $F'^{\theta}_{x'} \geq \varepsilon$ is a conjunction.
- Consider one of its conjuncts $c'^{\theta}_{x'} \geq \varepsilon$ belonging to $c \geq 0$ (others similar).

□

Soundness Proof

$$\frac{\vdash \exists\varepsilon{>}0\,\forall^\alpha\forall y_1,y_k\,(\neg F\land\chi\to(F'\geq\varepsilon)^{\theta_1}_{x'_1}\dots{}^{\theta_n}_{x'_n})}{[\exists y_1,y_k\,(x'_1=\theta_1\land,\land x'_n=\theta_n\land{\sim}F)]\chi\vdash\langle\exists y_1,y_k\,(x'_1=\theta_1\land,\land x'_n=\theta_n\land\chi)\rangle F}$$

Proof (locally sound, quantified case).

- If there is no such ζ, extending φ by larger r will make F true:
- Thus $\varphi\models\neg F\land\chi$ and, by premiss, $\varphi\models {F'}^{\theta}_{x'}\geq\varepsilon$, because $\forall^\alpha$ comprises all changed variables.
- ${F'}^{\theta}_{x'}\geq\varepsilon$ is a conjunction.
- Consider one of its conjuncts ${c'}^{\theta}_{x'}\geq\varepsilon$ belonging to $c\geq 0$ (others similar).
- Again, φ of the order of c' and value of c defined along φ, because $\varphi\models\chi$ and χ guards against zeros.

□

Soundness Proof

$$\frac{\vdash \exists \varepsilon{>}0\, \forall^{\alpha} \forall y_1, y_k\, (\neg F \land \chi \to (F' \geq \varepsilon)_{x_1'}^{\theta_1} \dots {}_{x_n'}^{\theta_n})}{[\exists y_1, y_k\, (x_1' = \theta_1 \land, \land x_n' = \theta_n \land {\sim}F)]\chi \vdash \langle \exists y_1, y_k\, (x_1' = \theta_1 \land, \land x_n' = \theta_n \land \chi)\rangle F}$$

Proof (locally sound, quantified case).

- By mean-value theorem, derivation lemma & diff.subst., we conclude for each $\zeta \in [0, r]$ that for some $\xi \in (0, \zeta)$

$$[\![c]\!]_{\varphi(\zeta)} - [\![c]\!]_{\varphi(0)} = [\![{c'}_{x'}^{\theta}]\!]_{\bar{\varphi}(\xi)}(\zeta - 0)$$

Soundness Proof

$$\frac{\vdash \exists \varepsilon{>}0\, \forall^{\alpha} \forall y_1, y_k\, (\neg F \wedge \chi \rightarrow (F' \geq \varepsilon)_{x_1'}^{\theta_1} \dots_{x_n'}^{\theta_n})}{[\exists y_1, y_k\, (x_1' = \theta_1 \wedge, \wedge x_n' = \theta_n \wedge {\sim}F)]\chi \vdash \langle \exists y_1, y_k\, (x_1' = \theta_1 \wedge, \wedge x_n' = \theta_n \wedge \chi)\rangle F}$$

Proof (locally sound, quantified case).

- By mean-value theorem, derivation lemma & diff.subst., we conclude for each $\zeta \in [0, r]$ that for some $\xi \in (0, \zeta)$

$$[\![c]\!]_{\varphi(\zeta)} - [\![c]\!]_{\varphi(0)} = [\![{c'}_{x'}^{\theta}]\!]_{\bar{\varphi}(\xi)}(\zeta - 0) \geq \zeta [\![\varepsilon]\!]_{\varphi(0)}$$

Soundness Proof

$$\frac{\vdash \exists\varepsilon{>}0\,\forall^{\alpha}\forall y_1, y_k\,(\neg F \wedge \chi \to (F' \geq \varepsilon)_{x_1'}^{\theta_1}\dots{}_{x_n'}^{\theta_n})}{[\exists y_1, y_k\,(x_1' = \theta_1\wedge, \wedge x_n' = \theta_n \wedge \sim F)]\chi \vdash \langle\exists y_1, y_k\,(x_1' = \theta_1\wedge, \wedge x_n' = \theta_n \wedge \chi)\rangle F}$$

Proof (locally sound, quantified case).

- By mean-value theorem, derivation lemma & diff.subst., we conclude for each $\zeta \in [0, r]$ that for some $\xi \in (0, \zeta)$

$$[\![c]\!]_{\varphi(\zeta)} - [\![c]\!]_{\varphi(0)} = [\![{c'}^{\theta}_{x'}]\!]_{\bar{\varphi}(\xi)}(\zeta - 0) \geq \zeta[\![\varepsilon]\!]_{\varphi(0)}$$

- As $[\![\varepsilon]\!]_{\varphi(0)} > 0$ we have for all $\zeta > -\frac{[\![c]\!]_{\varphi(0)}}{[\![\varepsilon]\!]_{\varphi(0)}}$ that $\varphi(\zeta) \models c \geq 0$ and $\varphi(r) \models c \geq 0$, even $\varphi(r) \models c > 0$.

Soundness Proof

$$\frac{\vdash \exists \varepsilon{>}0\, \forall^{\alpha} \forall y_1, y_k\, (\neg F \land \chi \to (F' \geq \varepsilon)^{\theta_1}_{x_1'} \dots {}^{\theta_n}_{x_n'})}{[\exists y_1, y_k\, (x_1' = \theta_1 \land, \land x_n' = \theta_n \land {\sim}F)]\chi \vdash \langle \exists y_1, y_k\, (x_1' = \theta_1 \land, \land x_n' = \theta_n \land \chi)\rangle F}$$

Proof (locally sound, quantified case).

- By mean-value theorem, derivation lemma & diff.subst., we conclude for each $\zeta \in [0, r]$ that for some $\xi \in (0, \zeta)$

$$[\![c]\!]_{\varphi(\zeta)} - [\![c]\!]_{\varphi(0)} = [\![{c'}^{\theta}_{x'}]\!]_{\bar{\varphi}(\xi)}(\zeta - 0) \geq \zeta [\![\varepsilon]\!]_{\varphi(0)}$$

- As $[\![\varepsilon]\!]_{\varphi(0)} > 0$ we have for all $\zeta > -\frac{[\![c]\!]_{\varphi(0)}}{[\![\varepsilon]\!]_{\varphi(0)}}$ that $\varphi(\zeta) \models c \geq 0$ and $\varphi(r) \models c \geq 0$, even $\varphi(r) \models c > 0$.
- By extending r, all literals $c \geq 0$ of one conjunct of F are true, which concludes the proof, because, until F finally holds, $\varphi \models \chi$ is implied by antecedent (above).

Soundness Proof

$$\frac{\vdash \exists \varepsilon{>}0\, \forall^{\alpha} \forall y_1 \ldots y_k\, (\neg F \land \chi \to (F' \geq \varepsilon)_{x_1'}^{\theta_1} \ldots {}_{x_n'}^{\theta_n})}{[\exists y_1 \ldots y_k\, (x_1' = \theta_1 \land \ldots \land x_n' = \theta_n \land {\sim}F)]\chi \vdash \langle \exists y_1 \ldots y_k\, (x_1' = \theta_1 \land \ldots \land x_n' = \theta_n}$$

Proof (locally sound, quantified case).

- With quantifiers $\exists y$ we prove slightly stronger statement, because y is quantified universally in the premiss (and antecedent):

□

Soundness Proof

$$\frac{\vdash \exists\varepsilon{>}0\, \forall^{\alpha}\forall y_1\,..\,y_k\,(\neg F \land \chi \rightarrow (F' \geq \varepsilon)^{\theta_1}_{x_1'}\cdots{}^{\theta_n}_{x_n'})}{[\exists y_1\,..\,y_k\,(x_1' = \theta_1 \land\,..\,\land x_n' = \theta_n \land {\sim}F)]\chi \vdash \langle\exists y_1\,..\,y_k\,(x_1' = \theta_1 \land\,..\,\land x_n' = \theta_n}$$

Proof (locally sound, quantified case).

- With quantifiers $\exists y$ we prove slightly stronger statement, because y is quantified universally in the premiss (and antecedent):
- F reachable for *all* choices of y that respect χ (not only one).

□

Soundness Proof

$$\frac{\vdash \exists \varepsilon > 0 \, \forall^{\alpha} \forall y_1 \ldots y_k \, (\neg F \wedge \chi \rightarrow (F' \geq \varepsilon)^{\theta_1}_{x_1'} \ldots {}^{\theta_n}_{x_n'})}{[\exists y_1 \ldots y_k \, (x_1' = \theta_1 \wedge \ldots \wedge x_n' = \theta_n \wedge \sim F)]\chi \vdash \langle \exists y_1 \ldots y_k \, (x_1' = \theta_1 \wedge \ldots \wedge x_n' = \theta_n}$$

Proof (locally sound, quantified case).

- With quantifiers $\exists y$ we prove slightly stronger statement, because y is quantified universally in the premiss (and antecedent):
- F reachable for *all* choices of y that respect χ (not only one).
- By antecedent, there is a $u \in \mathbb{R}$ such that $v_y^u \models \chi$.

□

Soundness Proof

$$\frac{\vdash \exists \varepsilon{>}0\, \forall^{\alpha} \forall y_1 \ldotp\ldotp y_k\, (\neg F \land \chi \to (F' \geq \varepsilon)^{\theta_1}_{x'_1} \cdots ^{\theta_n}_{x'_n})}{[\exists y_1 \ldotp\ldotp y_k\, (x'_1 = \theta_1 \land \ldotp\ldotp \land x'_n = \theta_n \land {\sim}F)]\chi \vdash \langle \exists y_1 \ldotp\ldotp y_k\, (x'_1 = \theta_1 \land \ldotp\ldotp \land x'_n = \theta_n}$$

Proof (locally sound, quantified case).

- With quantifiers $\exists y$ we prove slightly stronger statement, because y is quantified universally in the premiss (and antecedent):
- F reachable for *all* choices of y that respect χ (not only one).
- By antecedent, there is a $u \in \mathbb{R}$ such that $v_y^u \models \chi$.
- Hence, v_y^u satisfies assumptions of quantifier-free case.

□

Soundness Proof

$$\frac{\vdash \exists \varepsilon{>}0\, \forall^{\alpha} \forall y_1 \,..\, y_k\, (\neg F \land \chi \rightarrow (F' \geq \varepsilon)^{\theta_1}_{x'_1} \cdots ^{\theta_n}_{x'_n})}{[\exists y_1 \,..\, y_k\, (x'_1 = \theta_1 \land \,..\, \land x'_n = \theta_n \land \sim F)]\chi \vdash \langle \exists y_1 \,..\, y_k\, (x'_1 = \theta_1 \land \,..\, \land x'_n = \theta_n}$$

Proof (locally sound, quantified case).

- With quantifiers $\exists y$ we prove slightly stronger statement, because y is quantified universally in the premiss (and antecedent):
- F reachable for *all* choices of y that respect χ (not only one).
- By antecedent, there is a $u \in \mathbb{R}$ such that $v_y^u \models \chi$.
- Hence, v_y^u satisfies assumptions of quantifier-free case.
- Thus, $v_y^u \models \langle x' = \theta \land \chi \rangle F$,

□

Soundness Proof

$$\frac{\vdash \exists \varepsilon{>}0\, \forall^{\alpha} \forall y_1 \,..\, y_k\, (\neg F \land \chi \to (F' \geq \varepsilon)^{\theta_1}_{x_1'} \cdots ^{\theta_n}_{x_n'})}{[\exists y_1 \,..\, y_k\, (x_1' = \theta_1 \land \,..\, \land x_n' = \theta_n \land \sim F)]\chi \vdash \langle \exists y_1 \,..\, y_k\, (x_1' = \theta_1 \land \,..\, \land x_n' = \theta_n}$$

Proof (locally sound, quantified case).

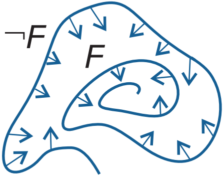
- With quantifiers $\exists y$ we prove slightly stronger statement, because y is quantified universally in the premiss (and antecedent):
- F reachable for *all* choices of y that respect χ (not only one).
- By antecedent, there is a $u \in \mathbb{R}$ such that $v_y^u \models \chi$.
- Hence, v_y^u satisfies assumptions of quantifier-free case.
- Thus, $v_y^u \models \langle x' = \theta \land \chi \rangle F$,
- Hence $v \models \langle \exists y\, (x' = \theta \land \chi) \rangle F$ using u constantly as the value for the quantified variable y during the evolution.

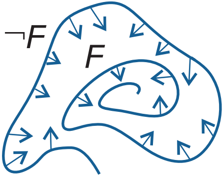
□

Outline

1. Verification Calculus for Differential-algebraic Dynamic Logic d$\mathcal{L}$
   - Motivation for Differential Induction
   - Derivations and Differentiation
   - Differential Induction
   - Motivation for Differential Saturation
   - Differential Variants
   - Compositional Verification Calculus
   - Differential Transformation
   - Differential Reduction & Differential Elimination
   - Proof Rules
2. Soundness
3. Restricting Differential Invariants
4. Deductive Power

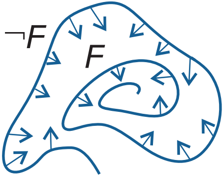
Restricting Differential Invariance



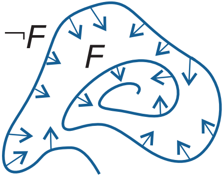


$$\frac{\vdash (\chi \rightarrow F')}{\chi \rightarrow F \vdash [x' = \theta \land \chi]F}$$

Restricting Differential Invariance

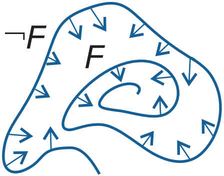


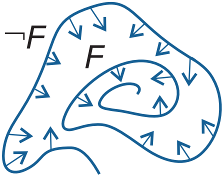
$$\frac{\vdash (\chi \rightarrow F')}{\chi \rightarrow F \vdash [x' = \theta \land \chi]F}$$



$$\frac{\vdash (F \land \chi \rightarrow F')}{\chi \rightarrow F \vdash [x' = \theta \land \chi]F}$$

Restricting Differential Invariance





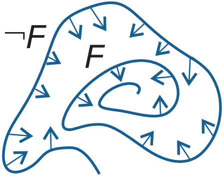
$$\frac{\vdash (\chi \rightarrow F')}{\chi \rightarrow F \vdash [x' = \theta \land \chi]F}$$

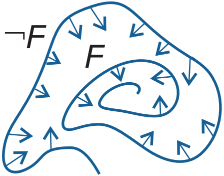
$$\frac{\vdash (F \land \chi \rightarrow F')}{\chi \rightarrow F \vdash [x' = \theta \land \chi]F}$$

Example (Restrictions)

$$\frac{\vdash \forall x\,(x^2 \leq 0 \rightarrow 2x \cdot 1 \leq 0)}{x^2 \leq 0 \vdash [x' = 1]x^2 \leq 0}$$

Restricting Differential Invariance



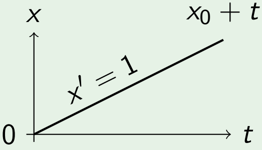


$$\frac{\vdash (\chi \to F')}{\chi \to F \vdash [x' = \theta \land \chi]F}$$

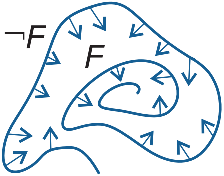
$$\frac{\vdash (F \land \chi \to F')}{\chi \to F \vdash [x' = \theta \land \chi]F}$$

Example (Restrictions)

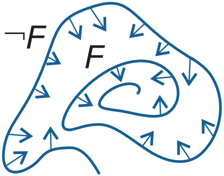
$$\frac{\vdash \forall x\,(x^2 \leq 0 \to 2x \cdot 1 \leq 0)}{x^2 \leq 0 \vdash [x' = 1]x^2 \leq 0}$$



Restricting Differential Invariance



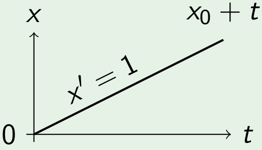
$$\frac{\vdash (\chi \to F')}{\chi \to F \vdash [x' = \theta \land \chi]F}$$



$$\cancel{\frac{\vdash (F \land \chi \to F')}{\chi \to F \vdash [x' = \theta \land \chi]F}}$$

Example (Restrictions are unsound nonsense!)

$$\frac{\vdash \forall x\, (x^2 \leq 0 \to 2x \cdot 1 \leq 0)}{x^2 \leq 0 \vdash [x' = 1]x^2 \leq 0}$$



Restricting Differential Invariants (Soundly!)

$$\frac{\vdash \forall y_1 \ldots \forall y_k \, (F \land \chi \rightarrow F'^{\theta_1}_{x_1'} \cdots ^{\theta_n}_{x_n'})}{[\exists y_1 \ldots \exists y_k \, \chi]F \vdash [\exists y_1 \ldots \exists y_k \, (x_1' = \theta_1 \land \cdots \land x_n' = \theta_n \land \chi)]F} \; F \text{ open}$$

locally sound if F open.

- Proof similar to diff.inv.

□

Restricting Differential Invariants (Soundly!)

$$\frac{\vdash \forall y_1 \ldots \forall y_k\,(F \land \chi \rightarrow F'^{\theta_1}_{x'_1}\cdots^{\theta_n}_{x'_n})}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k\,(x'_1 = \theta_1 \land \cdots \land x'_n = \theta_n \land \chi)]F} \quad F \text{ open}$$

locally sound if F open.

- Proof similar to diff.inv.
- Except that assuming $\varphi(\zeta) \models \neg F$ only yields $h(0) \geq 0 \geq h(\zeta)$,

□

Restricting Differential Invariants (Soundly!)

$$\frac{\vdash \forall y_1 \ldots \forall y_k\,(F \land \chi \rightarrow F'^{\theta_1}_{x'_1}\cdots^{\theta_n}_{x'_n})}{[\exists y_1 \ldots \exists y_k\,\chi]F \vdash [\exists y_1 \ldots \exists y_k\,(x'_1 = \theta_1 \land \cdots \land x'_n = \theta_n \land \chi)]F} \quad F \text{ open}$$

locally sound if F open.

- Proof similar to diff.inv.
- Except that assuming $\varphi(\zeta) \models \neg F$ only yields $h(0) \geq 0 \geq h(\zeta)$,
- which does not lead to a contradiction.

□

Restricting Differential Invariants (Soundly!)

$$\frac{\vdash \forall y_1 \ldots \forall y_k\, (F \land \chi \rightarrow F'^{\theta_1}_{x'_1} \cdots ^{\theta_n}_{x'_n})}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k\, (x'_1 = \theta_1 \land \cdots \land x'_n = \theta_n \land \chi)]F} \quad F \text{ open}$$

locally sound if F open.

- Proof similar to diff.inv.
- Except that assuming $\varphi(\zeta) \models \neg F$ only yields $h(0) \geq 0 \geq h(\zeta)$,
- which does not lead to a contradiction.
- F open $\Rightarrow$ distance to ∂F is positive in $\varphi(0)$

□

Restricting Differential Invariants (Soundly!)

$$\frac{\vdash \forall y_1 \dots \forall y_k\, (F \land \chi \to F'^{\theta_1}_{x'_1} \cdots ^{\theta_n}_{x'_n})}{[\exists y_1 \dots \exists y_k\, \chi]F \vdash [\exists y_1 \dots \exists y_k\, (x'_1 = \theta_1 \land \dots \land x'_n = \theta_n \land \chi)]F} \quad F \text{ open}$$

locally sound if F open.

- Proof similar to diff.inv.
- Except that assuming $\varphi(\zeta) \models \neg F$ only yields $h(0) \geq 0 \geq h(\zeta)$,
- which does not lead to a contradiction.
- F open $\Rightarrow$ distance to ∂F is positive in $\varphi(0)$
- Thus $h(0) > 0 \geq h(\zeta)$, and the contradiction arises accordingly.

□

Restricting Differential Invariants (Soundly!)

$$\frac{\vdash \forall y_1 \ldots \forall y_k\,(F \land \chi \rightarrow (F' > 0)^{\theta_1}_{x_1'} \cdots {}^{\theta_n}_{x_n'})}{[\exists y_1 \ldots \exists y_k\,\chi]F \vdash [\exists y_1 \ldots \exists y_k\,(x_1' = \theta_1 \land \cdots \land x_n' = \theta_n \land \chi)]F}$$

locally sound.

- Repeating argument for diff.inv., assume $F \equiv c \geq 0$.

□

Restricting Differential Invariants (Soundly!)

$$\frac{\vdash \forall y_1 \ldots \forall y_k\,(F \land \chi \to (F' > 0)_{x_1'}^{\theta_1} \ldots {}_{x_n'}^{\theta_n})}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k\,(x_1' = \theta_1 \land \cdots \land x_n' = \theta_n \land \chi)]F}$$

locally sound.

- Repeating argument for diff.inv., assume $F \equiv c \geq 0$.
- By contradiction suppose there was a $\iota \in [0, r]$ where $\varphi(\iota) \models c < 0$.

□

Restricting Differential Invariants (Soundly!)

$$\frac{\vdash \forall y_1 \dots \forall y_k \, (F \land \chi \to (F' > 0)^{\theta_1}_{x'_1} \dots ^{\theta_n}_{x'_n})}{[\exists y_1 \dots \exists y_k \, \chi]F \vdash [\exists y_1 \dots \exists y_k \, (x'_1 = \theta_1 \land \dots \land x'_n = \theta_n \land \chi)]F}$$

locally sound.

- Repeating argument for diff.inv., assume $F \equiv c \geq 0$.
- By contradiction suppose there was a $\iota \in [0, r]$ where $\varphi(\iota) \models c < 0$.
- Let $\zeta \in [0, r]$ infimum of these ι,

□

Restricting Differential Invariants (Soundly!)

$$\frac{\vdash \forall y_1 \dots \forall y_k\, (F \land \chi \to (F' > 0)_{x_1'}^{\theta_1} \dots {}_{x_n'}^{\theta_n})}{[\exists y_1 \dots \exists y_k\, \chi]F \vdash [\exists y_1 \dots \exists y_k\, (x_1' = \theta_1 \land \dots \land x_n' = \theta_n \land \chi)]F}$$

locally sound.

- Repeating argument for diff.inv., assume $F \equiv c \geq 0$.
- By contradiction suppose there was a $\iota \in [0, r]$ where $\varphi(\iota) \models c < 0$.
- Let $\zeta \in [0, r]$ infimum of these ι,
- Hence, $\varphi(\zeta) \models c = 0$ by continuity.

□

Restricting Differential Invariants (Soundly!)

$$\frac{\vdash \forall y_1 \dots \forall y_k\,(F \land \chi \to (F' > 0)_{x_1'}^{\theta_1}\dots{}_{x_n'}^{\theta_n})}{[\exists y_1 \dots \exists y_k\,\chi]F \vdash [\exists y_1 \dots \exists y_k\,(x_1' = \theta_1 \land \dots \land x_n' = \theta_n \land \chi)]F}$$

locally sound.

- Repeating argument for diff.inv., assume $F \equiv c \geq 0$.
- By contradiction suppose there was a $\iota \in [0, r]$ where $\varphi(\iota) \models c < 0$.
- Let $\zeta \in [0, r]$ infimum of these ι,
- Hence, $\varphi(\zeta) \models c = 0$ by continuity.

$\Rightarrow$ $h : [0, r] \to \mathbb{R}; h(t) = [\![c]\!]_{\varphi(t)}$ satisfies $h(0) \geq 0 \geq h(\zeta)$, because $v \models c \geq 0$ by antecedent.

□

Restricting Differential Invariants (Soundly!)

$$\frac{\vdash \forall y_1 \dots \forall y_k \, (F \land \chi \to (F' > 0)^{\theta_1}_{x'_1} \dots ^{\theta_n}_{x'_n})}{[\exists y_1 \dots \exists y_k \, \chi]F \vdash [\exists y_1 \dots \exists y_k \, (x'_1 = \theta_1 \land \dots \land x'_n = \theta_n \land \chi)]F}$$

locally sound.

- Repeating argument for diff.inv., assume $F \equiv c \geq 0$.
- By contradiction suppose there was a $\iota \in [0, r]$ where $\varphi(\iota) \models c < 0$.
- Let $\zeta \in [0, r]$ infimum of these ι,
- Hence, $\varphi(\zeta) \models c = 0$ by continuity.

$\Rightarrow$ $h : [0, r] \to \mathbb{R}; h(t) = [\![c]\!]_{\varphi(t)}$ satisfies $h(0) \geq 0 \geq h(\zeta)$, because $v \models c \geq 0$ by antecedent.

- Repeating argument with derivation lemma, h continuous on $[0, r]$ and differentiable at every $\xi \in (0, r)$ with a derivative of $\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) = [\![c']\!]_{\bar{\varphi}(\xi)} \overset{diff.subst.}{=} [\![c'^{\theta}_{x'}]\!]_{\bar{\varphi}(\xi)}$, as $\varphi \models x' = \theta$.

□

Restricting Differential Invariants (Soundly!)

$$\frac{\vdash \forall y_1 \ldots \forall y_k \left(F \land \chi \to (F' > 0)_{x_1'}^{\theta_1} \cdots {}_{x_n'}^{\theta_n}\right)}{[\exists y_1 \ldots \exists y_k\, \chi]F \vdash [\exists y_1 \ldots \exists y_k \left(x_1' = \theta_1 \land \cdots \land x_n' = \theta_n \land \chi\right)]F}$$

locally sound.

- Mean value theorem $\Rightarrow$ there is $\xi \in (0, \zeta)$ such that

$$\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) \cdot (\underbrace{\zeta - 0}_{\geq 0}) = h(\zeta) - h(0)$$

□

Restricting Differential Invariants (Soundly!)

$$\frac{\vdash \forall y_1 \dots \forall y_k\, (F \land \chi \to (F' > 0)_{x_1'}^{\theta_1} \dots {}_{x_n'}^{\theta_n})}{[\exists y_1 \dots \exists y_k\, \chi]F \vdash [\exists y_1 \dots \exists y_k\, (x_1' = \theta_1 \land \dots \land x_n' = \theta_n \land \chi)]F}$$

locally sound.

- Mean value theorem ⇒ there is $\xi \in (0, \zeta)$ such that

$$\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) \cdot (\underbrace{\zeta - 0}_{\geq 0}) = h(\zeta) - h(0) \leq 0$$

□

Restricting Differential Invariants (Soundly!)

$$\frac{\vdash \forall y_1 \ldots \forall y_k \, (F \land \chi \rightarrow (F' > 0)_{x'_1}^{\theta_1} \cdots {}_{x'_n}^{\theta_n})}{[\exists y_1 \ldots \exists y_k \, \chi]F \vdash [\exists y_1 \ldots \exists y_k \, (x'_1 = \theta_1 \land \cdots \land x'_n = \theta_n \land \chi)]F}$$

locally sound.

- Mean value theorem ⇒ there is $\xi \in (0, \zeta)$ such that

$$\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) \cdot (\underbrace{\zeta - 0}_{\geq 0}) = h(\zeta) - h(0) \leq 0$$

$$\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) = [\![{c'}_{x'}^{\theta}]\!]_{\bar{\varphi}(\xi)} \leq 0$$

□

Restricting Differential Invariants (Soundly!)

$$\frac{\vdash \forall y_1 \ldots \forall y_k \, (F \land \chi \rightarrow (F' > 0)^{\theta_1}_{x_1'} \cdots {}^{\theta_n}_{x_n'})}{[\exists y_1 \ldots \exists y_k \, \chi]F \vdash [\exists y_1 \ldots \exists y_k \, (x_1' = \theta_1 \land \cdots \land x_n' = \theta_n \land \chi)]F}$$

locally sound.

- Mean value theorem $\Rightarrow$ there is $\xi \in (0, \zeta)$ such that

$$\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) \cdot \underbrace{(\zeta - 0)}_{\geq 0} = h(\zeta) - h(0) \leq 0$$

$$\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) = [\![c'^{\theta}_{x'}]\!]_{\bar{\varphi}(\xi)} \leq 0$$

- Contradiction: by premiss $\bar{\varphi}(\xi) \models c'^{\theta}_{x'} > 0$, as the flow satisfies $\varphi \models \chi$ and $\varphi(\xi) \models c \geq 0$, because $\zeta > \xi$ is the infimum of the counterexamples ι with $\varphi(\iota) \models c < 0$.

□

Restricting Differential Invariants

Example (Any differential invariant restriction rule)

$$\frac{}{x > \frac{1}{4} \vdash [x' = x^3]x > \frac{1}{4}}$$

Restricting Differential Invariants

Example (Any differential invariant restriction rule)

$$\dfrac{\dfrac{}{\vdash \forall x\,(x > \frac{1}{4} \to x^3 > 0)}}{x > \frac{1}{4} \vdash [x' = x^3]x > \frac{1}{4}}$$

Restricting Differential Invariants

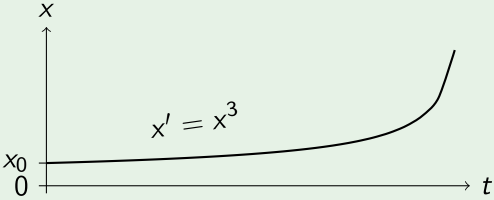
Example (Any differential invariant restriction rule)

$$\dfrac{\dfrac{*}{\vdash \forall x\,(x > \frac{1}{4} \rightarrow x^3 > 0)}}{x > \frac{1}{4} \vdash [x' = x^3]x > \frac{1}{4}}$$

Restricting Differential Invariants

Example (Any differential invariant restriction rule)

$$\dfrac{\dfrac{*}{\vdash \forall x\,(x > \frac{1}{4} \rightarrow x^3 > 0)}}{x > \frac{1}{4} \vdash [x' = x^3]x > \frac{1}{4}}$$



Outline

1. Verification Calculus for Differential-algebraic Dynamic Logic d$\mathcal{L}$
   - Motivation for Differential Induction
   - Derivations and Differentiation
   - Differential Induction
   - Motivation for Differential Saturation
   - Differential Variants
   - Compositional Verification Calculus
   - Differential Transformation
   - Differential Reduction & Differential Elimination
   - Proof Rules
2. Soundness
3. Restricting Differential Invariants
4. Deductive Power

Which formulas are best as differential invariants?

Equational Deductive Power

Does it make a difference if we have propositional operators?

Equational Deductive Power

Does it make a difference if we have propositional operators?

Proposition (Equational deductive power)

The deductive power of differential induction with atomic equations is identical to the deductive power of differential induction with propositional combinations of polynomial equations: Formulas are provable with propositional combinations of equations as differential invariants iff they are provable with only atomic equations as differential invariants.

"differential induction for '$=$' $\equiv$ differential induction for logic of '$=$' "

Equational Deductive Power: Proof

Proof.

- Assume differential invariant F is in NNF.

□

Equational Deductive Power: Proof

Proof.

- Assume differential invariant F is in NNF.
- $F \equiv p_1 = p_2 \lor q_1 = q_2$ equivalent to

□

Equational Deductive Power: Proof

Proof.

- Assume differential invariant F is in NNF.
- $F \equiv p_1 = p_2 \lor q_1 = q_2$ equivalent to
- $(p_1 - p_2)(q_1 - q_2) = 0$.

□

Equational Deductive Power: Proof

Proof.

- Assume differential invariant F is in NNF.
- $F \equiv p_1 = p_2 \lor q_1 = q_2$ equivalent to
- $(p_1 - p_2)(q_1 - q_2) = 0$.
- $F' \equiv p_1' = p_2' \land q_1' = q_2'$ implies
  $((p_1 - p_2)(q_1 - q_2))' = (p_1' - p_2')(q_1 - q_2) + (p_1 - p_2)(q_1' - q_2')$

□

Equational Deductive Power: Proof

Proof.

- Assume differential invariant F is in NNF.
- $F \equiv p_1 = p_2 \lor q_1 = q_2$ equivalent to
- $(p_1 - p_2)(q_1 - q_2) = 0$.
- $F' \equiv p_1' = p_2' \land q_1' = q_2'$ implies
  $((p_1 - p_2)(q_1 - q_2))' = (p_1' - p_2')(q_1 - q_2) + (p_1 - p_2)(q_1' - q_2')$

□

Equational Deductive Power: Proof

Proof.

- Assume differential invariant F is in NNF.
- $F \equiv p_1 = p_2 \lor q_1 = q_2$ equivalent to
- $(p_1 - p_2)(q_1 - q_2) = 0$.
- $F' \equiv p_1' = p_2' \land q_1' = q_2'$ implies
  $((p_1 - p_2)(q_1 - q_2))' = (p_1' - p_2')(q_1 - q_2) + (p_1 - p_2)(q_1' - q_2')$

□

Equational Deductive Power: Proof

Proof.

- Assume differential invariant F is in NNF.
- $F \equiv p_1 = p_2 \vee q_1 = q_2$ equivalent to
- $(p_1 - p_2)(q_1 - q_2) = 0$.
- $F' \equiv p_1' = p_2' \wedge q_1' = q_2'$ implies
  $((p_1 - p_2)(q_1 - q_2))' = (p_1' - p_2')(q_1 - q_2) + (p_1 - p_2)(q_1' - q_2') = 0$

□

Equational Deductive Power: Proof

Proof.

- Assume differential invariant F is in NNF.
- $F \equiv p_1 = p_2 \vee q_1 = q_2$ equivalent to
- $(p_1 - p_2)(q_1 - q_2) = 0$.
- $F' \equiv p_1' = p_2' \wedge q_1' = q_2'$ implies
  $((p_1 - p_2)(q_1 - q_2))' = (p_1' - p_2')(q_1 - q_2) + (p_1 - p_2)(q_1' - q_2') = 0$
- $F \equiv p_1 = p_2 \wedge q_1 = q_2$ equivalent to $(p_1 - p_2)^2 + (q_1 - q_2)^2 = 0$.

□

Equational Deductive Power: Proof

Proof.

- Assume differential invariant F is in NNF.
- $F \equiv p_1 = p_2 \lor q_1 = q_2$ equivalent to
- $(p_1 - p_2)(q_1 - q_2) = 0$.
- $F' \equiv p_1' = p_2' \land q_1' = q_2'$ implies $((p_1 - p_2)(q_1 - q_2))' = (p_1' - p_2')(q_1 - q_2) + (p_1 - p_2)(q_1' - q_2') = 0$
- $F \equiv p_1 = p_2 \land q_1 = q_2$ equivalent to $(p_1 - p_2)^2 + (q_1 - q_2)^2 = 0$.
- $F' \equiv p_1' = p_2' \land q_1' = q_2'$ implies $2(p_1 - p_2)(p_1' - p_2') + 2(q_1 - q_2)(q_1' - q_2')$

□

Equational Deductive Power: Proof

Proof.

- Assume differential invariant F is in NNF.
- $F \equiv p_1 = p_2 \lor q_1 = q_2$ equivalent to
- $(p_1 - p_2)(q_1 - q_2) = 0$.
- $F' \equiv p_1' = p_2' \land q_1' = q_2'$ implies
  $((p_1 - p_2)(q_1 - q_2))' = (p_1' - p_2')(q_1 - q_2) + (p_1 - p_2)(q_1' - q_2') = 0$
- $F \equiv p_1 = p_2 \land q_1 = q_2$ equivalent to $(p_1 - p_2)^2 + (q_1 - q_2)^2 = 0$.
- $F' \equiv p_1' = p_2' \land q_1' = q_2'$ implies
  $2(p_1 - p_2)(p_1' - p_2') + 2(q_1 - q_2)(q_1' - q_2')$

□

Equational Deductive Power: Proof

Proof.

- Assume differential invariant F is in NNF.
- $F \equiv p_1 = p_2 \lor q_1 = q_2$ equivalent to
- $(p_1 - p_2)(q_1 - q_2) = 0$.
- $F' \equiv p_1' = p_2' \land q_1' = q_2'$ implies
  $((p_1 - p_2)(q_1 - q_2))' = (p_1' - p_2')(q_1 - q_2) + (p_1 - p_2)(q_1' - q_2') = 0$
- $F \equiv p_1 = p_2 \land q_1 = q_2$ equivalent to $(p_1 - p_2)^2 + (q_1 - q_2)^2 = 0$.
- $F' \equiv p_1' = p_2' \land {\color{red} q_1' = q_2'}$ implies
  $2(p_1 - p_2)(p_1' - p_2') + 2(q_1 - q_2)({\color{red} q_1' - q_2'})$

□

Equational Deductive Power: Proof

Proof.

- Assume differential invariant F is in NNF.
- $F \equiv p_1 = p_2 \lor q_1 = q_2$ equivalent to
- $(p_1 - p_2)(q_1 - q_2) = 0$.
- $F' \equiv p_1' = p_2' \land q_1' = q_2'$ implies
  $((p_1 - p_2)(q_1 - q_2))' = (p_1' - p_2')(q_1 - q_2) + (p_1 - p_2)(q_1' - q_2') = 0$
- $F \equiv p_1 = p_2 \land q_1 = q_2$ equivalent to $(p_1 - p_2)^2 + (q_1 - q_2)^2 = 0$.
- $F' \equiv p_1' = p_2' \land q_1' = q_2'$ implies
  $2(p_1 - p_2)(p_1' - p_2') + 2(q_1 - q_2)(q_1' - q_2') = 0$

□

Equational Deductive Power: Proof

Proof.

- Assume differential invariant F is in NNF.
- $F \equiv p_1 = p_2 \vee q_1 = q_2$ equivalent to
- $(p_1 - p_2)(q_1 - q_2) = 0$.
- $F' \equiv p_1' = p_2' \wedge q_1' = q_2'$ implies
  $((p_1 - p_2)(q_1 - q_2))' = (p_1' - p_2')(q_1 - q_2) + (p_1 - p_2)(q_1' - q_2') = 0$
- $F \equiv p_1 = p_2 \wedge q_1 = q_2$ equivalent to $(p_1 - p_2)^2 + (q_1 - q_2)^2 = 0$.
- $F' \equiv p_1' = p_2' \wedge q_1' = q_2'$ implies
  $2(p_1 - p_2)(p_1' - p_2') + 2(q_1 - q_2)(q_1' - q_2') = 0$
- $F \equiv \neg(p_1 = p_2)$ does not qualify as differential invariant.

□

Deductive Power

Does it make a difference if we have propositional operators?

$\mathcal{R}$ Deductive Power

Does it make a difference if we have propositional operators?

Theorem (Deductive power)

The deductive power of differential induction with arbitrary formulas exceeds the deductive power of differential induction with atomic formulas: All DAL *formulas that are provable using atomic differential invariants are provable using general differential invariants, but not vice versa!*

"differential induction for atomic formulas $<$ general differential induction"

Deductive Power: Proof

Proof (Single differential induction step).

$$\frac{}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

Deductive Power: Proof

Proof (Single differential induction step).

$$\cfrac{\cfrac{}{\vdash \forall x\,\forall y\,(x > 0 \land y > 0 \to xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

Deductive Power: Proof

Proof (Single differential induction step).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

Deductive Power: Proof

Proof (Single differential induction step).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- Suppose single polynomial $p(x, y)$ such that $p(x, y) > 0$ is a differential invariant. The we have valid formulas:

Deductive Power: Proof

Proof (Single differential induction step).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x>0 \land y>0 \rightarrow xy>0 \land xy>0)}}{x>0 \land y>0 \vdash [x' = xy \land y' = xy](x>0 \land y>0)}$$

- Suppose single polynomial $p(x,y)$ such that $p(x,y)>0$ is a differential invariant. The we have valid formulas:
  1. $x>0 \land y>0 \rightarrow p(x,y)>0$, as differential invariants hold in prestate

Deductive Power: Proof

Proof (Single differential induction step).

$$\dfrac{\dfrac{*}{\vdash \forall x\, \forall y\, (x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- Suppose single polynomial $p(x, y)$ such that $p(x, y) > 0$ is a differential invariant. The we have valid formulas:
    1. $x > 0 \land y > 0 \rightarrow p(x, y) > 0$, as differential invariants hold in prestate
    2. $p(x, y) > 0 \rightarrow x > 0 \land y > 0$, as differential invariant implies postcondition

Deductive Power: Proof

Proof (Single differential induction step).

$$\cfrac{\cfrac{*}{\vdash \forall x\,\forall y\,(x>0\land y>0\to xy>0\land xy>0)}}{x>0\land y>0\vdash [x'=xy\land y'=xy](x>0\land y>0)}$$

- Suppose single polynomial $p(x,y)$ such that $p(x,y)>0$ is a differential invariant. The we have valid formulas:
  1. $x>0\land y>0\to p(x,y)>0$, as differential invariants hold in prestate
  2. $p(x,y)>0\to x>0\land y>0$, as differential invariant implies postcondition
- Hence $x>0\land y>0\leftrightarrow p(x,y)>0$ valid.

Deductive Power: Proof

Proof (Single differential induction step).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x>0 \land y>0 \rightarrow xy>0 \land xy>0)}}{x>0 \land y>0 \vdash [x'=xy \land y'=xy](x>0 \land y>0)}$$

- Suppose single polynomial $p(x,y)$ such that $p(x,y)>0$ is a differential invariant. The we have valid formulas:
  1. $x>0 \land y>0 \rightarrow p(x,y)>0$, as differential invariants hold in prestate
  2. $p(x,y)>0 \rightarrow x>0 \land y>0$, as differential invariant implies postcondition
- Hence $x>0 \land y>0 \leftrightarrow p(x,y)>0$ valid.
- Thus, p satisfies:

$$p(x,y) \geq 0 \text{ for } x \geq 0, y \geq 0, \text{ and, otherwise, } p(x,y) \leq 0 \qquad \text{(QS)}$$

Deductive Power: Proof

Proof (Single differential induction step).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x>0\land y>0 \rightarrow xy>0\land xy>0)}}{x>0\land y>0 \vdash [x'=xy\land y'=xy](x>0\land y>0)}$$

- Assume p minimal total degree with property

$$p(x,y)\geq 0 \text{ for } x\geq 0, y\geq 0, \text{ and, otherwise, } p(x,y)\leq 0 \qquad \text{(QS)}$$

- $p(x,0)$ is univariate polynomial in x with zeros at all $x>0$

$\Rightarrow$ $p(x,0)=0$ is the zero polynomial

$\Rightarrow$ y divides $p(x,y)$.

- Accordingly, $p(0,y)=0$ for all y, hence x divides $p(x,y)$.
- Thus, xy divides p.

Deductive Power: Proof

Proof (Single differential induction step).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- Assume p minimal total degree with property

$$p(x,y) \geq 0 \text{ for } x \geq 0, y \geq 0, \text{ and, otherwise, } p(x,y) \leq 0 \qquad \text{(QS)}$$

- $p(x,0)$ is univariate polynomial in x with zeros at all $x > 0$

$\Rightarrow$ $p(x,0) = 0$ is the zero polynomial

$\Rightarrow$ y divides $p(x,y)$.

- Accordingly, $p(0,y) = 0$ for all y, hence x divides $p(x,y)$.
- Thus, xy divides p.
- $\frac{-p(-x,-y)}{xy}$ satisfies (QS) with smaller total degree than p, contradiction!

Deductive Power: Proof

Proof (Single differential induction step).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

□

Deductive Power: Proof

Proof (Single differential induction step).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x>0\land y>0 \to xy>0\land xy>0)}}{x>0\land y>0 \vdash [x'=xy\land y'=xy](x>0\land y>0)}$$

- There is no polynomial p such that $x>0\land y>0 \leftrightarrow p(x,y)=0$,

□

Deductive Power: Proof

Proof (Single differential induction step).

$$\dfrac{\dfrac{*}{\vdash \forall x\, \forall y\, (x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- There is no polynomial p such that $x > 0 \land y > 0 \leftrightarrow p(x, y) = 0$,
- because only zero polynomial is zero on the full quadrant $(0, \infty)^2$.

□

Deductive Power: Proof

Proof (Single differential induction step).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- There is no polynomial p such that $x > 0 \land y > 0 \leftrightarrow p(x, y) = 0$,
- because only zero polynomial is zero on the full quadrant $(0, \infty)^2$.
- $x > 0 \land y > 0 \leftrightarrow p(x, y) \geq 0$ is impossible for continuity reasons that imply $p(0, 0) = 0$, which is a contradiction.

□

Deductive Power: Proof

Proof (Single differential induction step).

$$\dfrac{\dfrac{*}{\vdash \forall x\, \forall y\, (x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- There is no polynomial p such that $x > 0 \land y > 0 \leftrightarrow p(x, y) = 0$,
- because only zero polynomial is zero on the full quadrant $(0, \infty)^2$.
- $x > 0 \land y > 0 \leftrightarrow p(x, y) \geq 0$ is impossible for continuity reasons that imply $p(0, 0) = 0$, which is a contradiction.
- Same argument for any other sign condition that characterizes one quadrant of $\mathbb{R}^2$ uniquely.

□

Deductive Power: Proof

Proof (Single differential induction step).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- There is no polynomial p such that $x > 0 \land y > 0 \leftrightarrow p(x, y) = 0$,
- because only zero polynomial is zero on the full quadrant $(0, \infty)^2$.
- $x > 0 \land y > 0 \leftrightarrow p(x, y) \geq 0$ is impossible for continuity reasons that imply $p(0, 0) = 0$, which is a contradiction.
- Same argument for any other sign condition that characterizes one quadrant of $\mathbb{R}^2$ uniquely.
- So far, argument independent of actual dynamics

□

Deductive Power: Proof

Proof (Single differential induction step).

$$\cfrac{\cfrac{*}{\vdash \forall x\,\forall y\,(x>0\land y>0 \to xy>0\land xy>0)}}{x>0\land y>0 \vdash [x'=xy\land y'=xy](x>0\land y>0)}$$

- There is no polynomial p such that $x>0\land y>0 \leftrightarrow p(x,y)=0$,
- because only zero polynomial is zero on the full quadrant $(0,\infty)^2$.
- $x>0\land y>0 \leftrightarrow p(x,y)\geq 0$ is impossible for continuity reasons that imply $p(0,0)=0$, which is a contradiction.
- Same argument for any other sign condition that characterizes one quadrant of $\mathbb{R}^2$ uniquely.
- So far, argument independent of actual dynamics
- Thus, still valid in the presence of arbitrary differential weakening.

□

Deductive Power: Proof

Proof (Nested differential induction + strengthening).

$$\dfrac{\dfrac{*}{\vdash \forall x\, \forall y\, (x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

Deductive Power: Proof

Proof (Nested differential induction + strengthening).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x>0 \land y>0 \to xy>0 \land xy>0)}}{x>0 \land y>0 \vdash [x'=xy \land y'=xy](x>0 \land y>0)}$$

- Inductively, strengthening χ needs to be a differential invariant:

Proof (Nested differential induction + strengthening).

$$\dfrac{\dfrac{*}{\vdash \forall x\, \forall y\, (x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- Inductively, strengthening χ needs to be a differential invariant:

$$xy > 0$$

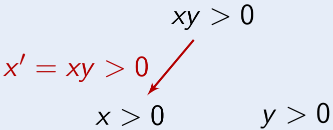
$$x > 0 \qquad y > 0$$

Deductive Power: Proof

Proof (Nested differential induction + strengthening).

$$\cfrac{\cfrac{*}{\vdash \forall x \, \forall y \, (x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- Inductively, strengthening χ needs to be a differential invariant:



$xy > 0$

$x' = xy > 0$

$x > 0$

$y > 0$

Deductive Power: Proof

Proof (Nested differential induction + strengthening).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x > 0 \land y > 0 \to xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- Inductively, strengthening χ needs to be a differential invariant:

$$\begin{tikzcd}
 & xy > 0 \arrow[dl, "x' = xy > 0"'] \arrow[dr, "y' = xy > 0"] & \\
x > 0 & & y > 0
\end{tikzcd}$$

Deductive Power: Proof

Proof (Nested differential induction + strengthening).

$$\dfrac{\dfrac{*}{\vdash \forall x\, \forall y\, (x > 0 \land y > 0 \to xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- Inductively, strengthening χ needs to be a differential invariant:

$$\begin{tikzcd} & xy > 0 \arrow[dl, "x' = xy > 0"'] \arrow[dr, "y' = xy > 0"] & \\ x > 0 & & y > 0 \end{tikzcd}$$

- Differential invariance of $xy > 0$ needs $xy > 0 \to (xy)'{}^{xy}_{x'}{}^{xy}_{y'}$

Deductive Power: Proof

Proof (Nested differential induction + strengthening).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x>0\land y>0\to xy>0\land xy>0)}}{x>0\land y>0\vdash[x'=xy\land y'=xy](x>0\land y>0)}$$

- Inductively, strengthening χ needs to be a differential invariant:

$$\begin{tikzcd} & xy>0 \arrow[dl, "x'=xy>0"'] \arrow[dr, "y'=xy>0"] & \\ x>0 & & y>0 \end{tikzcd}$$

- Differential invariance of $xy>0$ needs $xy>0\to {(xy)'}_{x'}^{xy}{}_{y'}^{xy}=(x'y+yx')_{x'}^{xy}{}_{y'}^{xy}$

Deductive Power: Proof

Proof (Nested differential induction + strengthening).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- Inductively, strengthening χ needs to be a differential invariant:

$$\begin{tikzcd} & xy > 0 \arrow[dl, "x' = xy > 0"'] \arrow[dr, "y' = xy > 0"] & \\ x > 0 & & y > 0 \end{tikzcd}$$

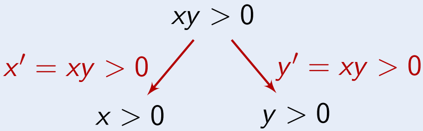
- Differential invariance of $xy > 0$ needs
  $xy > 0 \rightarrow (xy)'{}^{xy}_{x'}{}^{xy}_{y'} = (x'y + yx')^{xy}_{x'}{}^{xy}_{y'} = xyy + yxy$

Deductive Power: Proof

Proof (Nested differential induction + strengthening).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x>0 \land y>0 \to xy>0 \land xy>0)}}{x>0 \land y>0 \vdash [x'=xy \land y'=xy](x>0 \land y>0)}$$

- Inductively, strengthening χ needs to be a differential invariant:



$xy > 0$

$x' = xy > 0$

$y' = xy > 0$

$x > 0$

$y > 0$

- Differential invariance of $xy > 0$ needs
$xy > 0 \to (xy)'^{xy}_{x'}{}^{xy}_{y'} = (x'y + yx')^{xy}_{x'}{}^{xy}_{y'} = xyy + yxy = (y + x)xy$

Deductive Power: Proof

Proof (Nested differential induction + strengthening).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x>0\land y>0\to xy>0\land xy>0)}}{x>0\land y>0\vdash [x'=xy\land y'=xy](x>0\land y>0)}$$

- Inductively, strengthening χ needs to be a differential invariant:

$$\begin{tikzcd}
 & xy>0 \arrow[dl, "x'=xy>0"'] \arrow[dr, "y'=xy>0"] & \\
x>0 & & y>0
\end{tikzcd}$$

- Differential invariance of $xy>0$ needs
$xy>0\to (xy)'^{xy}_{x'}{}^{xy}_{y'} = (x'y+yx')^{xy}_{x'}{}^{xy}_{y'} = xyy+yxy=(y+x)xy>0$

Deductive Power: Proof

Proof (Nested differential induction + strengthening).

$$\cfrac{\cfrac{*}{\vdash \forall x\, \forall y\, (x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- Inductively, strengthening χ needs to be a differential invariant:

$$\begin{tikzcd} & xy > 0 \arrow[dl, "x' = xy > 0"'] \arrow[dr, "y' = xy > 0"] & \\ x > 0 & & y > 0 \end{tikzcd}$$

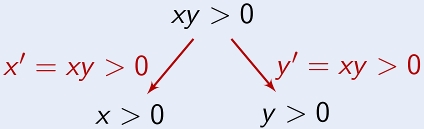
- Differential invariance of $xy > 0$ needs
  $xy > 0 \rightarrow (xy)'^{xy\ xy}_{x'\ y'} = (x'y + yx')^{xy\ xy}_{x'\ y'} = xyy + yxy = (y + x)xy > 0$
- $xy > 0 \rightarrow (y + x)xy > 0$

Deductive Power: Proof

Proof (Nested differential induction + strengthening).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x>0\land y>0\rightarrow xy>0\land xy>0)}}{x>0\land y>0\vdash[x'=xy\land y'=xy](x>0\land y>0)}$$

- Inductively, strengthening χ needs to be a differential invariant:



- Differential invariance of $xy>0$ needs
  $xy>0\rightarrow(xy)'^{xy}_{x'}{}^{xy}_{y'}=(x'y+yx')^{xy}_{x'}{}^{xy}_{y'}=xyy+yxy=(y+x)xy>0$
- $xy>0\rightarrow(y+x)xy>0\equiv x\geq0\lor y\geq0$

Deductive Power: Proof

Proof (Nested differential induction + strengthening).

$$\dfrac{\dfrac{*}{\vdash \forall x\,\forall y\,(x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- Inductively, strengthening χ needs to be a differential invariant:

$$\begin{tikzcd} & xy > 0 & \\ x > 0 \arrow[ur, leftrightarrow, "x' = xy > 0"] & & y > 0 \arrow[ul, leftrightarrow, "y' = xy > 0"'] \end{tikzcd}$$

- Differential invariance of $xy > 0$ needs
  $xy > 0 \rightarrow (xy)'^{xy}_{x'}{}^{xy}_{y'} = (x'y + yx')^{xy}_{x'}{}^{xy}_{y'} = xyy + yxy = (y + x)xy > 0$
- $xy > 0 \rightarrow (y + x)xy > 0 \equiv x \geq 0 \lor y \geq 0 \equiv \neg(-x > 0 \land -y > 0)$

Deductive Power: Proof

Proof (Nested differential induction + strengthening).

$$\dfrac{\dfrac{*}{\vdash \forall x\, \forall y\, (x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- Inductively, strengthening χ needs to be a differential invariant:

$$\begin{tikzcd}
 & xy > 0 \arrow[dl, leftrightarrow, "x' = xy > 0"'] \arrow[dr, leftrightarrow, "y' = xy > 0"] & \\
x > 0 & & y > 0
\end{tikzcd}$$

- Differential invariance of $xy > 0$ needs
  $xy > 0 \rightarrow (xy)'{}^{xy}_{x'}{}^{xy}_{y'} = (x'y + yx')^{xy}_{x'}{}^{xy}_{y'} = xyy + yxy = (y + x)xy > 0$
- $xy > 0 \rightarrow (y + x)xy > 0 \equiv x \geq 0 \lor y \geq 0 \equiv \neg(-x > 0 \land -y > 0)$
- not provable by atomic differential induction/weakening (see above).

Deductive Power: Proof

Proof (Nested differential induction + strengthening).

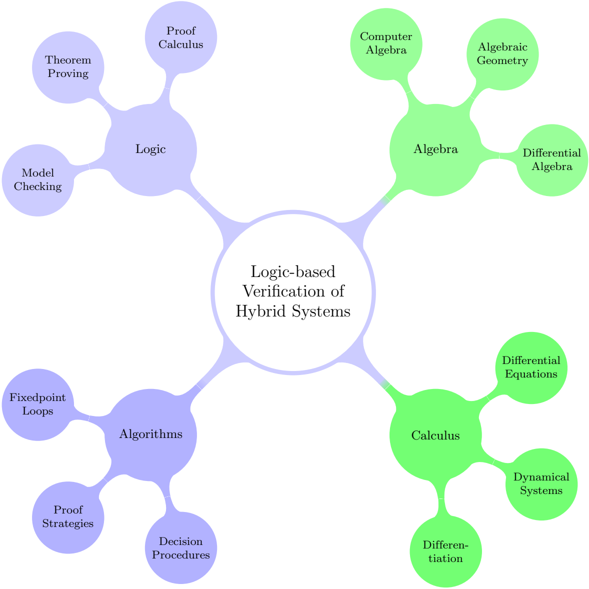
$$\dfrac{\dfrac{*}{\vdash \forall x\, \forall y\, (x > 0 \land y > 0 \rightarrow xy > 0 \land xy > 0)}}{x > 0 \land y > 0 \vdash [x' = xy \land y' = xy](x > 0 \land y > 0)}$$

- Inductively, strengthening χ needs to be a differential invariant:

$$\begin{tikzcd}
& xy > 0 & \\
x > 0 \arrow[ur, leftrightarrow, "x' = xy > 0"] & & y > 0 \arrow[ul, leftrightarrow, "y' = xy > 0"']
\end{tikzcd}$$

- Differential invariance of $xy > 0$ needs
$xy > 0 \rightarrow (xy)'^{xy}_{x'}{}^{xy}_{y'} = (x'y + yx')^{xy}_{x'}{}^{xy}_{y'} = xyy + yxy = (y + x)xy > 0$
- $xy > 0 \rightarrow (y + x)xy > 0 \equiv x \geq 0 \lor y \geq 0 \equiv \neg(-x > 0 \land -y > 0)$
- not provable by atomic differential induction/weakening (see above).
- Circular dependencies for strengthening by $x > 0$, $y > 0$, $xy > 0$,

Landscape


Logic-based Verification of Hybrid Systems
Logic
Proof Calculus
Theorem Proving
Model Checking
Algebra
Computer Algebra
Algebraic Geometry
Differential Algebra
Algorithms
Fixedpoint Loops
Proof Strategies
Decision Procedures
Calculus
Differential Equations
Dynamical Systems
Differentiation