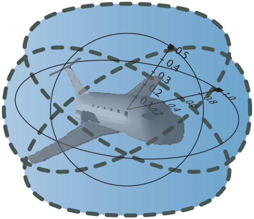
15-819/18-879: Logical Analysis of Hybrid Systems

26: Soundness of Proof Rules

André Platzer

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



Outline

1. Soundness
2. Summary

10 propositional rules

$$\frac{\vdash \phi}{\neg\phi \vdash} \qquad \frac{\phi, \psi \vdash}{\phi \wedge \psi \vdash} \qquad \frac{\phi \vdash \quad \psi \vdash}{\phi \vee \psi \vdash} \qquad \frac{\vdash \phi \quad \phi \vdash}{\vdash}$$

$$\frac{\phi \vdash}{\vdash \neg\phi} \qquad \frac{\vdash \phi \quad \vdash \psi}{\vdash \phi \wedge \psi} \qquad \frac{\vdash \phi, \psi}{\vdash \phi \vee \psi}$$

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

$$\frac{\langle\alpha\rangle\langle\beta\rangle\phi}{\langle\alpha;\beta\rangle\phi} \qquad \frac{\phi \lor \langle\alpha\rangle\langle\alpha^*\rangle\phi}{\langle\alpha^*\rangle\phi} \qquad \frac{\phi_{x_1}^{\theta_1}\dots{}_{x_n}^{\theta_n}}{\langle x_1 := \theta_1, \dots, x_n := \theta_n\rangle\phi}$$

$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi} \qquad \frac{\phi \land [\alpha][\alpha^*]\phi}{[\alpha^*]\phi} \qquad \frac{\langle x_1 := \theta_1, \dots, x_n := \theta_n\rangle\phi}{[x_1 := \theta_1, \dots, x_n := \theta_n]\phi}$$

$$\frac{\langle\alpha\rangle\phi \lor \langle\beta\rangle\phi}{\langle\alpha\cup\beta\rangle\phi} \qquad \frac{\chi \land \psi}{\langle ?\chi\rangle\psi} \qquad \frac{\exists t{\geq}0\, \big((\forall 0{\leq}\tilde{t}{\leq}t\, \langle\mathcal{S}(\tilde{t})\rangle\chi) \land \langle\mathcal{S}(t)\rangle\phi\big)}{\langle x_1' = \theta_1, \dots, x_n' = \theta_n \land \chi\rangle\phi}$$

$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha\cup\beta]\phi} \qquad \frac{\chi \to \psi}{[?\chi]\psi} \qquad \frac{\forall t{\geq}0\, \big((\forall 0{\leq}\tilde{t}{\leq}t\, \langle\mathcal{S}(\tilde{t})\rangle\chi) \to \langle\mathcal{S}(t)\rangle\phi\big)}{[x_1' = \theta_1, \dots, x_n' = \theta_n \land \chi]\phi}$$

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

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

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

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

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

QE needs to be defined in premiss

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

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

Outline

Soundness

Theorem (Soundness)

d$\mathcal{L}$ *calculus is sound, i.e.,*

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

Soundness

Theorem (Soundness)

d$\mathcal{L}$ *calculus is sound, i.e.,*

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

Challenges (Soundness Proof)

Soundness

Theorem (Soundness)

d$\mathcal{L}$ *calculus is sound, i.e.,*

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

Challenges (Soundness Proof)

- $x' = f(x)$

Soundness

Theorem (Soundness)

d$\mathcal{L}$ *calculus is sound, i.e.,*

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

Challenges (Soundness Proof)

- $x' = f(x)$
- Side deductions

Theorem (Soundness)

d$\mathcal{L}$ *calculus is sound, i.e.,*

$$\vdash \phi \quad \Rightarrow \quad \models \phi$$

Challenges (Soundness Proof)

- $x' = f(x)$
- Side deductions
- Free variables & Skolemization

Free Variables, Models, and Consequences

Definition (Tableau Model)

Formula F has model iff there is I, v such that *for all* variable assignments η we have $I, \eta, v \models \phi$.

Free Variables, Models, and Consequences

Definition (Model Consequence)

ψ *consequence* of ϕ iff, for every I, v *there is* a η such that $I, \eta, v \models \psi$, provided that, for every I, v *there is* a η such that $I, \eta, v \models \phi$.

Definition (Tableau Model)

Formula F has model iff there is I, v such that *for all* variable assignments η we have $I, \eta, v \models \phi$.

Free Variables, Models, and Consequences

Definition (Model Consequence)

ψ *consequence* of ϕ iff, for every I, v *there is* a η such that $I, \eta, v \models \psi$, provided that, for every I, v *there is* a η such that $I, \eta, v \models \phi$.

Definition (Soundness)

Calculus rule *sound* iff conclusions Ψ consequence of premisses Φ.

$$\frac{\Phi}{\Psi} \quad \text{sound iff } \Psi \text{ consequence of } \Phi$$

Free Variables, Models, and Consequences

Definition (Model Consequence)

ψ *consequence* of ϕ iff, for every I, v *there is* a η such that $I, \eta, v \models \psi$, provided that, for every I, v *there is* a η such that $I, \eta, v \models \phi$.

Definition (Soundness)

Calculus rule *sound* iff conclusions Ψ consequence of premisses Φ.

$$\frac{\Phi_1 \quad \dots \quad \Phi_n}{\Psi_1 \quad \dots \quad \Psi_m}$$

Free Variables, Models, and Consequences

Definition (Model Consequence)

ψ *consequence* of ϕ iff, for every I, v *there is* a η such that $I, \eta, v \models \psi$, provided that, for every I, v *there is* a η such that $I, \eta, v \models \phi$.

Definition (Soundness)

Calculus rule *sound* iff conclusions Ψ consequence of premisses Φ.

$$\frac{\Phi_1 \quad \dots \quad \Phi_n}{\Psi_1 \quad \dots \quad \Psi_m} \quad \Psi_1 \land \dots \land \Psi_m \text{ consequence of } \Phi_1 \land \dots \land \Phi_n$$

Free Variables, Models, and Consequences

Definition (Model Consequence)

ψ *consequence* of ϕ iff, for every I, v *there is* a η such that $I, \eta, v \models \psi$, provided that, for every I, v *there is* a η such that $I, \eta, v \models \phi$.

Definition (Soundness)

Calculus rule *sound* iff conclusions Ψ consequence of premisses Φ.

$$\frac{\Phi_1 \quad \dots \quad \Phi_n}{\Psi_1 \quad \dots \quad \Psi_m} \quad \Psi_1 \land \dots \land \Psi_m \text{ consequence of } \Phi_1 \land \dots \land \Phi_n$$

Definition (Local Soundness)

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

Free Variables, Models, and Consequences

Definition (Model Consequence)

ψ *consequence* of ϕ iff, for every I, v *there is* a η such that $I, \eta, v \models \psi$, provided that, for every I, v *there is* a η such that $I, \eta, v \models \phi$.

Definition (Soundness)

Calculus rule *sound* iff conclusions Ψ consequence of premisses Φ.

$$\frac{\Phi_1 \quad \dots \quad \Phi_n}{\Psi_1 \quad \dots \quad \Psi_m} \quad \Psi_1 \wedge \dots \wedge \Psi_m \text{ consequence of } \Phi_1 \wedge \dots \wedge \Phi_n$$

$$\Uparrow / \Downarrow ?$$

Definition (Local Soundness)

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

Free Variables, Models, and Consequences

Definition (Model Consequence)

ψ *consequence* of ϕ iff, for every I, v *there is* a η such that $I, \eta, v \models \psi$, provided that, for every I, v *there is* a η such that $I, \eta, v \models \phi$.

Definition (Soundness)

Calculus rule *sound* iff conclusions Ψ consequence of premisses Φ.

$$\frac{\Phi_1 \quad \dots \quad \Phi_n}{\Psi_1 \quad \dots \quad \Psi_m} \quad \Psi_1 \wedge \dots \wedge \Psi_m \text{ consequence of } \Phi_1 \wedge \dots \wedge \Phi_n$$

$$\Uparrow$$

Definition (Local Soundness)

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

Local Application of Local Soundness in Context

Definition (Local Soundness)

$$\frac{\Phi' \vdash \Psi'}{\Phi \vdash \Psi} \quad \text{locally sound iff}$$

$$\text{for each } \; I, \eta, v \; \big(I, \eta, v \models \Phi' \vdash \Psi' \;\; \Rightarrow \;\; I, \eta, v \models \Phi \vdash \Psi \big)$$

Local Application of Local Soundness in Context

Definition (Local Soundness)

$$\frac{\Phi' \vdash \Psi'}{\Phi \vdash \Psi} \quad \text{locally sound iff}$$

$$\text{for each } I,\eta,v \ \left(I,\eta,v \models \Phi' \vdash \Psi' \ \Rightarrow \ I,\eta,v \models \Phi \vdash \Psi\right)$$

$$\Downarrow$$

Lemma (Local application context lifting)

If α is a deterministic HP, then

$$\frac{\Phi' \vdash \Psi'}{\Phi \vdash \Psi} \ \textit{locally sound} \ \Rightarrow \ \frac{\Gamma, \langle\alpha\rangle\Phi' \vdash \langle\alpha\rangle\Psi', \Delta}{\Gamma, \langle\alpha\rangle\Phi \vdash \langle\alpha\rangle\Psi, \Delta} \ \textit{locally sound}$$

Soundness Proof

$$\frac{\phi_{x_1}^{\theta_1} \dots {}_{x_n}^{\theta_n}}{\langle x_1 := \theta_1, \dots, x_n := \theta_n \rangle \phi}$$

Proof ($\langle := \rangle$ locally sound).

- Assume premiss holds in I, η, v, i.e., $I, \eta, v \models \phi_{x_1}^{\theta_1} \dots {}_{x_n}^{\theta_n}$.

□

Soundness Proof

$$\frac{\phi_{x_1}^{\theta_1} \dots {}_{x_n}^{\theta_n}}{\langle x_1 := \theta_1, \dots, x_n := \theta_n \rangle \phi}$$

Proof ($\langle := \rangle$ locally sound).

- Assume premiss holds in I, η, v, i.e., $I, \eta, v \models \phi_{x_1}^{\theta_1} \dots {}_{x_n}^{\theta_n}$.
- Show $I, \eta, v \models \langle x_1 := \theta_1, \dots, x_n := \theta_n \rangle \phi$,

$\square$

Soundness Proof

$$\frac{\phi_{x_1}^{\theta_1} \dots {}_{x_n}^{\theta_n}}{\langle x_1 := \theta_1, \dots, x_n := \theta_n \rangle \phi}$$

Proof ($\langle := \rangle$ locally sound).

- Assume premiss holds in I, η, v, i.e., $I, \eta, v \models \phi_{x_1}^{\theta_1} \dots {}_{x_n}^{\theta_n}$.
- Show $I, \eta, v \models \langle x_1 := \theta_1, \dots, x_n := \theta_n \rangle \phi$,
- i.e., $I, \eta, \omega \models \phi$ for a state ω with $(v, \omega) \in \rho_{I,\eta}(x_1 := \theta_1, \dots, x_n := \theta_n)$.

□

Soundness Proof

$$\frac{\phi_{x_1}^{\theta_1} \ldots {}_{x_n}^{\theta_n}}{\langle x_1 := \theta_1, \ldots, x_n := \theta_n \rangle \phi}$$

Proof ($\langle := \rangle$ locally sound).

- Assume premiss holds in I, η, v, i.e., $I, \eta, v \models \phi_{x_1}^{\theta_1} \ldots {}_{x_n}^{\theta_n}$.
- Show $I, \eta, v \models \langle x_1 := \theta_1, \ldots, x_n := \theta_n \rangle \phi$,
- i.e., $I, \eta, \omega \models \phi$ for a state ω with $(v, \omega) \in \rho_{I,\eta}(x_1 := \theta_1, \ldots, x_n := \theta_n)$.
- Follows from substitution lemma, which generalises to dynamic logic for admissible substitutions.

$\square$

Soundness Proof

$$\frac{\exists t{\geq}0\,\big((\forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi)\wedge\langle\mathcal{S}(t)\rangle\phi\big)}{\langle x_1'=\theta_1,\ldots,x_n'=\theta_n\wedge\chi\rangle\phi}\quad\text{where}\quad \begin{array}{l}\bar{\chi}\equiv\forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi\\ \mathcal{D}\equiv x_1'=\theta_1,\ldots,x_n'=\theta_n\wedge\chi\end{array}$$

Proof ($\langle x'\rangle$ locally sound).

- Let $y_1,\ldots,y_n$ solve ODE $x_1'=\theta_1,\ldots,x_n'=\theta_n$ with IV $x_1,\ldots,x_n$.

Soundness Proof

$$\frac{\exists t{\geq}0\,\big((\forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi) \wedge \langle\mathcal{S}(t)\rangle\phi\big)}{\langle x_1' = \theta_1,..,x_n' = \theta_n \wedge \chi\rangle\phi} \quad \text{where} \quad \begin{array}{l}\bar{\chi} \equiv \forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi \\ \mathcal{D} \equiv x_1' = \theta_1,..,x_n' = \theta_n \wedge \chi\end{array}$$

Proof ($\langle x'\rangle$ locally sound).

- Let $y_1,\dots,y_n$ solve ODE $x_1' = \theta_1,\dots,x_n' = \theta_n$ with IV $x_1,\dots,x_n$.
- Let $\langle\mathcal{S}(t)\rangle$ be $\langle x_1 := y_1(t),\dots,x_n := y_n(t)\rangle$.

Soundness Proof

$$\frac{\exists t{\geq}0\,\big((\forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi) \land \langle\mathcal{S}(t)\rangle\phi\big)}{\langle x_1' = \theta_1, .., x_n' = \theta_n \land \chi\rangle\phi} \quad \text{where} \quad \begin{array}{l}\bar{\chi} \equiv \forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi \\ \mathcal{D} \equiv x_1' = \theta_1, .., x_n' = \theta_n \land \chi\end{array}$$

Proof ($\langle x'\rangle$ locally sound).

- Let $y_1, \dots, y_n$ solve ODE $x_1' = \theta_1, \dots, x_n' = \theta_n$ with IV $x_1, \dots, x_n$.
- Let $\langle\mathcal{S}(t)\rangle$ be $\langle x_1 := y_1(t), \dots, x_n := y_n(t)\rangle$.
- Assume premiss holds: $I, \eta, v \models \exists t{\geq}0\,(\bar{\chi} \land \langle\mathcal{S}(t)\rangle\phi)$

Soundness Proof

$$\frac{\exists t{\geq}0\,((\forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi) \land \langle\mathcal{S}(t)\rangle\phi)}{\langle x_1' = \theta_1, .., x_n' = \theta_n \land \chi\rangle\phi} \quad \text{where} \quad \begin{array}{l}\bar{\chi} \equiv \forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi \\ \mathcal{D} \equiv x_1' = \theta_1, .., x_n' = \theta_n \land \chi\end{array}$$

Proof ($\langle x' \rangle$ locally sound).

- Let $y_1, \dots, y_n$ solve ODE $x_1' = \theta_1, \dots, x_n' = \theta_n$ with IV $x_1, \dots, x_n$.
- Let $\langle\mathcal{S}(t)\rangle$ be $\langle x_1 := y_1(t), \dots, x_n := y_n(t)\rangle$.
- Assume premiss holds: $I, \eta, v \models \exists t{\geq}0\,(\bar{\chi} \land \langle\mathcal{S}(t)\rangle\phi)$
- By assumption, there is a $r \geq 0$ such that $I, \eta_t^r, v \models \bar{\chi} \land \langle\mathcal{S}(t)\rangle\phi$.

Soundness Proof

$$\frac{\exists t{\geq}0\,\big((\forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi) \land \langle\mathcal{S}(t)\rangle\phi\big)}{\langle x_1' = \theta_1, \ldots, x_n' = \theta_n \land \chi\rangle\phi} \quad \text{where} \quad \begin{array}{l}\bar{\chi} \equiv \forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi \\ \mathcal{D} \equiv x_1' = \theta_1, \ldots, x_n' = \theta_n \land \chi\end{array}$$

Proof ($\langle x' \rangle$ locally sound).

- Let $y_1, \ldots, y_n$ solve ODE $x_1' = \theta_1, \ldots, x_n' = \theta_n$ with IV $x_1, \ldots, x_n$.
- Let $\langle\mathcal{S}(t)\rangle$ be $\langle x_1 := y_1(t), \ldots, x_n := y_n(t)\rangle$.
- Assume premiss holds: $I, \eta, v \models \exists t{\geq}0\,(\bar{\chi} \land \langle\mathcal{S}(t)\rangle\phi)$
- By assumption, there is a $r \geq 0$ such that $I, \eta_t^r, v \models \bar{\chi} \land \langle\mathcal{S}(t)\rangle\phi$.
- We have to show $I, \eta, v \models \langle\mathcal{D}\rangle\phi$.

Soundness Proof

$$\frac{\exists t \geq 0\, \big((\forall 0 \leq \tilde{t} \leq t\, \langle \mathcal{S}(\tilde{t}) \rangle \chi) \land \langle \mathcal{S}(t) \rangle \phi\big)}{\langle x_1' = \theta_1, \ldots, x_n' = \theta_n \land \chi \rangle \phi} \quad \text{where} \quad \begin{array}{l} \bar{\chi} \equiv \forall 0 \leq \tilde{t} \leq t\, \langle \mathcal{S}(\tilde{t}) \rangle \chi \\ \mathcal{D} \equiv x_1' = \theta_1, \ldots, x_n' = \theta_n \land \chi \end{array}$$

Proof ($\langle x' \rangle$ locally sound).

- Let $y_1, \ldots, y_n$ solve ODE $x_1' = \theta_1, \ldots, x_n' = \theta_n$ with IV $x_1, \ldots, x_n$.
- Let $\langle \mathcal{S}(t) \rangle$ be $\langle x_1 := y_1(t), \ldots, x_n := y_n(t) \rangle$.
- Assume premiss holds: $I, \eta, v \models \exists t \geq 0\, (\bar{\chi} \land \langle \mathcal{S}(t) \rangle \phi)$
- By assumption, there is a $r \geq 0$ such that $I, \eta_t^r, v \models \bar{\chi} \land \langle \mathcal{S}(t) \rangle \phi$.
- We have to show $I, \eta, v \models \langle \mathcal{D} \rangle \phi$.
- Equivalently, by coincidence lemma, $I, \eta_t^r, v \models \langle \mathcal{D} \rangle \phi$, because t fresh.

Soundness Proof

$$\frac{\exists t{\geq}0\,\big((\forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi) \land \langle\mathcal{S}(t)\rangle\phi\big)}{\langle x_1' = \theta_1, \ldots, x_n' = \theta_n \land \chi\rangle\phi} \quad \text{where} \quad \begin{array}{l}\bar{\chi} \equiv \forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi \\ \mathcal{D} \equiv x_1' = \theta_1, \ldots, x_n' = \theta_n \land \chi\end{array}$$

Proof ($\langle x'\rangle$ locally sound).

- Let $y_1, \ldots, y_n$ solve ODE $x_1' = \theta_1, \ldots, x_n' = \theta_n$ with IV $x_1, \ldots, x_n$.
- Let $\langle\mathcal{S}(t)\rangle$ be $\langle x_1 := y_1(t), \ldots, x_n := y_n(t)\rangle$.
- Assume premiss holds: $I, \eta, v \models \exists t{\geq}0\,(\bar{\chi} \land \langle\mathcal{S}(t)\rangle\phi)$
- By assumption, there is a $r \geq 0$ such that $I, \eta_t^r, v \models \bar{\chi} \land \langle\mathcal{S}(t)\rangle\phi$.
- We have to show $I, \eta, v \models \langle\mathcal{D}\rangle\phi$.
- Equivalently, by coincidence lemma, $I, \eta_t^r, v \models \langle\mathcal{D}\rangle\phi$, because t fresh.
- Let $f : [0, r] \to \text{States}$ such that $(v, f(\zeta)) \in \rho_{I,\eta_t^\zeta}(\mathcal{S}(t))$ for all $\zeta \in [0, r]$. By premiss, $f(0) = v$ and ϕ holds at $f(r)$.

Soundness Proof

$$\frac{\exists t{\geq}0\, \left((\forall 0{\leq}\tilde{t}{\leq}t\, \langle \mathcal{S}(\tilde{t})\rangle\chi) \wedge \langle \mathcal{S}(t)\rangle\phi\right)}{\langle x_1' = \theta_1, \ldots, x_n' = \theta_n \wedge \chi\rangle\phi} \quad \text{where} \quad \begin{array}{l}\bar{\chi} \equiv \forall 0{\leq}\tilde{t}{\leq}t\, \langle \mathcal{S}(\tilde{t})\rangle\chi \\ \mathcal{D} \equiv x_1' = \theta_1, \ldots, x_n' = \theta_n \wedge \chi\end{array}$$

Proof ($\langle x' \rangle$ locally sound).

- Let $y_1, \ldots, y_n$ solve ODE $x_1' = \theta_1, \ldots, x_n' = \theta_n$ with IV $x_1, \ldots, x_n$.
- Let $\langle \mathcal{S}(t)\rangle$ be $\langle x_1 := y_1(t), \ldots, x_n := y_n(t)\rangle$.
- Assume premiss holds: $I, \eta, v \models \exists t{\geq}0\, (\bar{\chi} \wedge \langle \mathcal{S}(t)\rangle\phi)$
- By assumption, there is a $r \geq 0$ such that $I, \eta_t^r, v \models \bar{\chi} \wedge \langle \mathcal{S}(t)\rangle\phi$.
- We have to show $I, \eta, v \models \langle \mathcal{D}\rangle\phi$.
- Equivalently, by coincidence lemma, $I, \eta_t^r, v \models \langle \mathcal{D}\rangle\phi$, because t fresh.
- Let $f : [0, r] \to \text{States}$ such that $(v, f(\zeta)) \in \rho_{I,\eta_t^\zeta}(\mathcal{S}(t))$ for all $\zeta \in [0, r]$. By premiss, $f(0) = v$ and ϕ holds at $f(r)$.
- It only remains to show that f is a flow for $\rho_{I,\eta}(\mathcal{D})$.

Soundness Proof

$$\frac{\exists t{\geq}0\,((\forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi)\wedge\langle\mathcal{S}(t)\rangle\phi)}{\langle x_1'=\theta_1,\ldots,x_n'=\theta_n\wedge\chi\rangle\phi}\quad\text{where}\quad\begin{array}{l}\bar{\chi}\equiv\forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi\\ \mathcal{D}\equiv x_1'=\theta_1,\ldots,x_n'=\theta_n\wedge\chi\end{array}$$

Proof ($\langle x'\rangle$ locally sound).

- Let $y_1,\ldots,y_n$ solve ODE $x_1'=\theta_1,\ldots,x_n'=\theta_n$ with IV $x_1,\ldots,x_n$.
- Let $\langle\mathcal{S}(t)\rangle$ be $\langle x_1:=y_1(t),\ldots,x_n:=y_n(t)\rangle$.
- Assume premiss holds: $I,\eta,v\models\exists t{\geq}0\,(\bar{\chi}\wedge\langle\mathcal{S}(t)\rangle\phi)$
- By assumption, there is a $r\geq 0$ such that $I,\eta_t^r,v\models\bar{\chi}\wedge\langle\mathcal{S}(t)\rangle\phi$.
- We have to show $I,\eta,v\models\langle\mathcal{D}\rangle\phi$.
- Equivalently, by coincidence lemma, $I,\eta_t^r,v\models\langle\mathcal{D}\rangle\phi$, because t fresh.
- Let $f:[0,r]\to$ States such that $(v,f(\zeta))\in\rho_{I,\eta_t^\zeta}(\mathcal{S}(t))$ for all $\zeta\in[0,r]$. By premiss, $f(0)=v$ and ϕ holds at $f(r)$.
- It only remains to show that f is a flow for $\rho_{I,\eta}(\mathcal{D})$.
- f continuous and differentiable according to y_i.

Soundness Proof

$$\frac{\exists t{\ge}0\,\big((\forall 0{\le}\tilde{t}{\le}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi) \land \langle\mathcal{S}(t)\rangle\phi\big)}{\langle x_1' = \theta_1, \ldots, x_n' = \theta_n \land \chi\rangle\phi} \quad \text{where} \quad \begin{array}{l}\bar{\chi} \equiv \forall 0{\le}\tilde{t}{\le}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi \\ \mathcal{D} \equiv x_1' = \theta_1, \ldots, x_n' = \theta_n \land \chi\end{array}$$

Proof ($\langle x' \rangle$ locally sound).

- Moreover, $[\![x_i]\!]_{I,f(\zeta),\eta_t^r} = [\![y_i(t)]\!]_{I,v,\eta_t^r}$ has a derivative of value $[\![\theta_i]\!]_{I,f(\zeta),\eta_t^r}$, because y_i is a solution of the differential equation $x_i' = \theta_i$ with corresponding initial value $v(x_i)$.

$\square$

$$\frac{\exists t{\geq}0\, \big((\forall 0{\leq}\tilde{t}{\leq}t\, \langle \mathcal{S}(\tilde{t})\rangle\chi) \land \langle \mathcal{S}(t)\rangle\phi\big)}{\langle x_1' = \theta_1, .., x_n' = \theta_n \land \chi\rangle\phi} \quad \text{where} \quad \begin{array}{l}\bar{\chi} \equiv \forall 0{\leq}\tilde{t}{\leq}t\, \langle \mathcal{S}(\tilde{t})\rangle\chi \\ \mathcal{D} \equiv x_1' = \theta_1, .., x_n' = \theta_n \land \chi\end{array}$$

Proof ($\langle x'\rangle$ locally sound).

- Moreover, $[\![x_i]\!]_{I,f(\zeta),\eta_t^r} = [\![y_i(t)]\!]_{I,v,\eta_t^r}$ has a derivative of value $[\![\theta_i]\!]_{I,f(\zeta),\eta_t^r}$, because y_i is a solution of the differential equation $x_i' = \theta_i$ with corresponding initial value $v(x_i)$.
- Further, evolution invariant region χ is respected along f:

$\square$

Soundness Proof

$$\frac{\exists t{\geq}0\,\big((\forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi) \wedge \langle\mathcal{S}(t)\rangle\phi\big)}{\langle x_1' = \theta_1, .., x_n' = \theta_n \wedge \chi\rangle\phi} \quad \text{where} \quad \begin{array}{l}\bar{\chi} \equiv \forall 0{\leq}\tilde{t}{\leq}t\,\langle\mathcal{S}(\tilde{t})\rangle\chi \\ \mathcal{D} \equiv x_1' = \theta_1, .., x_n' = \theta_n \wedge \chi\end{array}$$

Proof ($\langle x'\rangle$ locally sound).

- Moreover, $[\![x_i]\!]_{I,f(\zeta),\eta_t^r} = [\![y_i(t)]\!]_{I,v,\eta_t^r}$ has a derivative of value $[\![\theta_i]\!]_{I,f(\zeta),\eta_t^r}$, because y_i is a solution of the differential equation $x_i' = \theta_i$ with corresponding initial value $v(x_i)$.
- Further, evolution invariant region χ is respected along f:
- By premiss, $I, \eta_t^r, v \models \bar{\chi}$ holds for the initial state v, thus $[\![\chi]\!]_{I,f(\zeta),\eta_t^r} = \mathit{true}$ for all $\zeta \in [0, r]$.

□

Soundness Proof

$$\frac{\exists t{\geq}0\ \big((\forall 0{\leq}\tilde{t}{\leq}t\ \langle \mathcal{S}(\tilde{t})\rangle\chi) \land \langle \mathcal{S}(t)\rangle\phi\big)}{\langle x_1' = \theta_1, \ldots, x_n' = \theta_n \land \chi\rangle\phi} \quad \text{where} \quad \begin{array}{l}\bar{\chi} \equiv \forall 0{\leq}\tilde{t}{\leq}t\ \langle \mathcal{S}(\tilde{t})\rangle\chi \\ \mathcal{D} \equiv x_1' = \theta_1, \ldots, x_n' = \theta_n \land \chi\end{array}$$

Proof ($\langle x'\rangle$ locally sound).

- Moreover, $[\![x_i]\!]_{I,f(\zeta),\eta_t^r} = [\![y_i(t)]\!]_{I,v,\eta_t^r}$ has a derivative of value $[\![\theta_i]\!]_{I,f(\zeta),\eta_t^r}$, because y_i is a solution of the differential equation $x_i' = \theta_i$ with corresponding initial value $v(x_i)$.
- Further, evolution invariant region χ is respected along f:
- By premiss, $I, \eta_t^r, v \models \bar{\chi}$ holds for the initial state v, thus $[\![\chi]\!]_{I,f(\zeta),\eta_t^r} = \mathit{true}$ for all $\zeta \in [0, r]$.
- In short, f is a witness for $I, \eta, v \models \langle \mathcal{D}\rangle\phi$.

$\square$

Soundness Proof

$$\frac{\exists t{\geq}0\, \big((\forall 0{\leq}\tilde{t}{\leq}t\, \langle \mathcal{S}(\tilde{t})\rangle \chi) \land \langle \mathcal{S}(t)\rangle \phi\big)}{\langle x_1' = \theta_1, \ldots, x_n' = \theta_n \land \chi\rangle \phi} \quad \text{where} \quad \begin{array}{l} \bar{\chi} \equiv \forall 0{\leq}\tilde{t}{\leq}t\, \langle \mathcal{S}(\tilde{t})\rangle \chi \\ \mathcal{D} \equiv x_1' = \theta_1, \ldots, x_n' = \theta_n \land \chi \end{array}$$

Proof ($\langle x' \rangle$ locally sound).

- Moreover, $[\![x_i]\!]_{I,f(\zeta),\eta_t^r} = [\![y_i(t)]\!]_{I,v,\eta_t^r}$ has a derivative of value $[\![\theta_i]\!]_{I,f(\zeta),\eta_t^r}$, because y_i is a solution of the differential equation $x_i' = \theta_i$ with corresponding initial value $v(x_i)$.
- Further, evolution invariant region χ is respected along f:
- By premiss, $I, \eta_t^r, v \models \bar{\chi}$ holds for the initial state v, thus $[\![\chi]\!]_{I,f(\zeta),\eta_t^r} = \mathit{true}$ for all $\zeta \in [0, r]$.
- In short, f is a witness for $I, \eta, v \models \langle \mathcal{D}\rangle \phi$.
- Converse direction can be shown to prove the dual rule $[x']$ using that flows are unique.

□

Soundness Proof

$$\frac{\vdash \phi(s(X_1, .., X_n))}{\vdash \forall x\, \phi(x)}$$

Proof ($\forall$r sound).

- Contrapositively, assume there are I, v such that for all η, $I, \eta, v \not\models \forall x\, \phi(x)$, hence $I, \eta, v \models \exists x\, \neg\phi(x)$.

Soundness Proof

$$\frac{\vdash \phi(s(X_1, .., X_n))}{\vdash \forall x\, \phi(x)}$$

Proof (∀r sound).

- Contrapositively, assume there are I, v such that for all η, $I, \eta, v \not\models \forall x\, \phi(x)$, hence $I, \eta, v \models \exists x\, \neg\phi(x)$.
- Construct I' that agrees with I except for new function symbol s.

Soundness Proof

$$\frac{\vdash \phi(s(X_1,..,X_n))}{\vdash \forall x\, \phi(x)}$$

Proof (∀r sound).

- Contrapositively, assume there are I, v such that for all η, $I, \eta, v \not\models \forall x\, \phi(x)$, hence $I, \eta, v \models \exists x\, \neg\phi(x)$.
- Construct I' that agrees with I except for new function symbol s.
- For any $b_1, \ldots, b_n \in \mathbb{R}$ let η^b assign b_i to X_i for $1 \leq i \leq n$.

Soundness Proof

$$\frac{\vdash \phi(s(X_1,..,X_n))}{\vdash \forall x\, \phi(x)}$$

Proof ($\forall$r sound).

- Contrapositively, assume there are I, v such that for all η, $I, \eta, v \not\models \forall x\, \phi(x)$, hence $I, \eta, v \models \exists x\, \neg\phi(x)$.
- Construct I' that agrees with I except for new function symbol s.
- For any $b_1, \ldots, b_n \in \mathbb{R}$ let η^b assign b_i to X_i for $1 \leq i \leq n$.
- As $I, \eta, v \models \exists x\, \neg\phi(x)$ holds for all η, we pick a witness d for $I, \eta^b, v \models \exists x\, \neg\phi(x)$ and choose $I'(s)(b_1, \ldots, b_n) = d$.

$$\frac{\vdash \phi(s(X_1, \ldots, X_n))}{\vdash \forall x\, \phi(x)}$$

Proof ($\forall$r sound).

- Contrapositively, assume there are I, v such that for all η, $I, \eta, v \not\models \forall x\, \phi(x)$, hence $I, \eta, v \models \exists x\, \neg\phi(x)$.
- Construct I' that agrees with I except for new function symbol s.
- For any $b_1, \ldots, b_n \in \mathbb{R}$ let η^b assign b_i to X_i for $1 \leq i \leq n$.
- As $I, \eta, v \models \exists x\, \neg\phi(x)$ holds for all η, we pick a witness d for $I, \eta^b, v \models \exists x\, \neg\phi(x)$ and choose $I'(s)(b_1, \ldots, b_n) = d$.
- We have $I', \eta, v \not\models \phi(s(X_1, \ldots, X_n))$ for all η by coincidence lemma, as $X_1, \ldots, X_n$ are all FV determining truth value of $\phi(s(X_1, \ldots, X_n))$.

Soundness Proof

$$\frac{\vdash \phi(s(X_1,..,X_n))}{\vdash \forall x\, \phi(x)}$$

Proof ($\forall$r sound).

- Contrapositively, assume there are I, v such that for all η, $I, \eta, v \not\models \forall x\, \phi(x)$, hence $I, \eta, v \models \exists x\, \neg\phi(x)$.
- Construct I' that agrees with I except for new function symbol s.
- For any $b_1, \ldots, b_n \in \mathbb{R}$ let η^b assign b_i to X_i for $1 \le i \le n$.
- As $I, \eta, v \models \exists x\, \neg\phi(x)$ holds for all η, we pick a witness d for $I, \eta^b, v \models \exists x\, \neg\phi(x)$ and choose $I'(s)(b_1, \ldots, b_n) = d$.
- We have $I', \eta, v \not\models \phi(s(X_1, \ldots, X_n))$ for all η by coincidence lemma, as $X_1, \ldots, X_n$ are all FV determining truth value of $\phi(s(X_1, \ldots, X_n))$.
- $\Gamma, \Delta, \langle \mathcal{J} \rangle$ can be added: Since s is new, Γ, Δ do not change truth value by passing from I to I'. Further s is rigid and does not change value by adding jump prefix $\langle \mathcal{J} \rangle$.

Soundness Proof

$$\frac{\vdash \mathrm{QE}(\forall X\,(\Phi(X) \vdash \Psi(X)))}{\Phi(s(X_1,\ldots,X_n)) \vdash \Psi(s(X_1,\ldots,X_n))}$$

X new variable

Proof (i$\forall$ locally sound).

- Assume $I, \eta, v \models \mathrm{QE}(\forall X\,(\Phi(X) \vdash \Psi(X)))$.

$\square$

Soundness Proof

$$\frac{\vdash \mathrm{QE}(\forall X\,(\Phi(X) \vdash \Psi(X)))}{\Phi(s(X_1,\ldots,X_n)) \vdash \Psi(s(X_1,\ldots,X_n))}$$

X new variable

Proof (i$\forall$ locally sound).

- Assume $I, \eta, v \models \mathrm{QE}(\forall X\,(\Phi(X) \vdash \Psi(X)))$.
- QE yields an equivalence, thus $I, \eta, v \models \forall X\,(\Phi(X) \vdash \Psi(X))$.

$\square$

Soundness Proof

$$\frac{\vdash \mathrm{QE}(\forall X\,(\Phi(X) \vdash \Psi(X)))}{\Phi(s(X_1,..,X_n)) \vdash \Psi(s(X_1,..,X_n))}$$

X new variable

Proof ($\mathrm{i}\forall$ locally sound).

- Assume $I, \eta, v \models \mathrm{QE}(\forall X\,(\Phi(X) \vdash \Psi(X)))$.
- QE yields an equivalence, thus $I, \eta, v \models \forall X\,(\Phi(X) \vdash \Psi(X))$.
- If $I, \eta, v \models \Phi(s(X_1, \dots, X_n))$, we conclude $I, \eta, v \models \Psi(s(X_1, \dots, X_n))$ by choosing $[\![s(X_1, \dots, X_n)]\!]_{I,v,\eta}$ for X in premiss.

$\square$

$$\frac{\vdash \mathrm{QE}(\forall X\,(\Phi(X) \vdash \Psi(X)))}{\Phi(s(X_1,..,X_n)) \vdash \Psi(s(X_1,..,X_n))}$$

X new variable

Proof ($i\forall$ locally sound).

- Assume $I, \eta, v \models \mathrm{QE}(\forall X\,(\Phi(X) \vdash \Psi(X)))$.
- QE yields an equivalence, thus $I, \eta, v \models \forall X\,(\Phi(X) \vdash \Psi(X))$.
- If $I, \eta, v \models \Phi(s(X_1, \dots, X_n))$, we conclude $I, \eta, v \models \Psi(s(X_1, \dots, X_n))$ by choosing $[\![s(X_1, \dots, X_n)]\!]_{I,v,\eta}$ for X in premiss.
- By admissibility of substitutions, variables $X_1, \dots, X_n$ are free at all occurrences of $s(X_1, \dots, X_n)$, hence their value is the same in all occurrences.

$\square$

Soundness Proof

$$\frac{\vdash \phi(X)}{\vdash \exists x\, \phi(x)}$$

Proof ($\exists$r locally sound).

- For any I, η, v with $I, \eta, v \models \phi(X)$ we conclude $I, \eta, v \models \exists x\, \phi(x)$ according to the witness $\eta(X)$.

$\square$

$$\frac{\vdash \mathrm{QE}(\exists X \bigwedge_i (\Phi_i \vdash \Psi_i))}{\Phi_1 \vdash \Psi_1 \quad \dots \quad \Phi_n \vdash \Psi_n}$$

X only in branches $\Phi_i \vdash \Psi_i$

Proof (i$\exists$ sound).

- For any I, v let η be such that $I, \eta, v \models \mathrm{QE}(\exists X \bigwedge_i (\Phi_i \vdash \Psi_i))$.

Soundness Proof

$$\frac{\vdash \mathrm{QE}(\exists X \bigwedge_i (\Phi_i \vdash \Psi_i))}{\Phi_1 \vdash \Psi_1 \quad \ldots \quad \Phi_n \vdash \Psi_n}$$

X only in branches $\Phi_i \vdash \Psi_i$

Proof (i$\exists$ sound).

- For any I, v let η be such that $I, \eta, v \models \mathrm{QE}(\exists X \bigwedge_i (\Phi_i \vdash \Psi_i))$.
- QE yields equivalence, thus $I, \eta, v \models \exists X \bigwedge_i (\Phi_i \vdash \Psi_i)$.

Soundness Proof

$$\frac{\vdash \mathrm{QE}(\exists X\ \bigwedge_i(\Phi_i \vdash \Psi_i))}{\Phi_1 \vdash \Psi_1 \quad \dots \quad \Phi_n \vdash \Psi_n}$$

X only in branches $\Phi_i \vdash \Psi_i$

Proof (i$\exists$ sound).

- For any I, v let η be such that $I, \eta, v \models \mathrm{QE}(\exists X\ \bigwedge_i(\Phi_i \vdash \Psi_i))$.
- QE yields equivalence, thus $I, \eta, v \models \exists X\ \bigwedge_i(\Phi_i \vdash \Psi_i)$.
- Pick witness $d \in \mathbb{R}$ for this existential quantifier.

Soundness Proof

$$\frac{\vdash \mathrm{QE}(\exists X \bigwedge_i (\Phi_i \vdash \Psi_i))}{\Phi_1 \vdash \Psi_1 \quad \dots \quad \Phi_n \vdash \Psi_n}$$

X only in branches $\Phi_i \vdash \Psi_i$

Proof (i∃ sound).

- For any I, v let η be such that $I, \eta, v \models \mathrm{QE}(\exists X \bigwedge_i (\Phi_i \vdash \Psi_i))$.
- QE yields equivalence, thus $I, \eta, v \models \exists X \bigwedge_i (\Phi_i \vdash \Psi_i)$.
- Pick witness $d \in \mathbb{R}$ for this existential quantifier.
- As X does not occur anywhere else in the proof, it disappears from all open premisses of the proof by applying i∃. Hence, by coincidence lemma, value of X does not change truth value of premise.

Soundness Proof

$$\frac{\vdash \mathrm{QE}(\exists X \bigwedge_i (\Phi_i \vdash \Psi_i))}{\Phi_1 \vdash \Psi_1 \quad \ldots \quad \Phi_n \vdash \Psi_n}$$

X only in branches $\Phi_i \vdash \Psi_i$

Proof (i$\exists$ sound).

- For any I, v let η be such that $I, \eta, v \models \mathrm{QE}(\exists X \bigwedge_i (\Phi_i \vdash \Psi_i))$.
- QE yields equivalence, thus $I, \eta, v \models \exists X \bigwedge_i (\Phi_i \vdash \Psi_i)$.
- Pick witness $d \in \mathbb{R}$ for this existential quantifier.
- As X does not occur anywhere else in the proof, it disappears from all open premisses of the proof by applying i$\exists$. Hence, by coincidence lemma, value of X does not change truth value of premise.
- Consequently, η can be extended to η' by changing the interpretation of X to the witness d such that $I, \eta', v \models \bigwedge_i (\Phi_i \vdash \Psi_i)$.

Soundness Proof

$$\frac{\vdash \mathrm{QE}(\exists X \bigwedge_i (\Phi_i \vdash \Psi_i))}{\Phi_1 \vdash \Psi_1 \quad \dots \quad \Phi_n \vdash \Psi_n}$$

X only in branches $\Phi_i \vdash \Psi_i$

Proof (i∃ sound).

- For any I, v let η be such that $I, \eta, v \models \mathrm{QE}(\exists X \bigwedge_i (\Phi_i \vdash \Psi_i))$.
- QE yields equivalence, thus $I, \eta, v \models \exists X \bigwedge_i (\Phi_i \vdash \Psi_i)$.
- Pick witness $d \in \mathbb{R}$ for this existential quantifier.
- As X does not occur anywhere else in the proof, it disappears from all open premisses of the proof by applying i∃. Hence, by coincidence lemma, value of X does not change truth value of premise.
- Consequently, η can be extended to η' by changing the interpretation of X to the witness d such that $I, \eta', v \models \bigwedge_i (\Phi_i \vdash \Psi_i)$.
- Thus, η' extends I, η, v to a simultaneous model of all conclusions.

Soundness Proof

$$\frac{\vdash \forall^\alpha(\phi \to \psi)}{\langle\alpha\rangle\phi \vdash \langle\alpha\rangle\psi}$$

Proof ($\langle\rangle$gen locally sound).

- Simple refinement of coincidence lemma using that the universal closure $\forall^\alpha$ comprises all variables that change in α.

$\square$

Soundness Proof

$$\frac{\vdash \forall^\alpha(\phi \to \psi)}{\langle\alpha\rangle\phi \vdash \langle\alpha\rangle\psi}$$

Proof ($\langle\rangle$gen locally sound).

- Simple refinement of coincidence lemma using that the universal closure $\forall^\alpha$ comprises all variables that change in α.
- Let $I, \eta, v \models \langle\alpha\rangle\phi$, i.e., let $(v, \nu') \in \rho_{I,\eta}(\alpha)$ with $I, \eta, \nu' \models \phi$.

$\square$

Soundness Proof

$$\frac{\vdash \forall^\alpha(\phi \to \psi)}{\langle\alpha\rangle\phi \vdash \langle\alpha\rangle\psi}$$

Proof ($\langle\rangle$gen locally sound).

- Simple refinement of coincidence lemma using that the universal closure $\forall^\alpha$ comprises all variables that change in α.
- Let $I, \eta, v \models \langle\alpha\rangle\phi$, i.e., let $(v, \nu') \in \rho_{I,\eta}(\alpha)$ with $I, \eta, \nu' \models \phi$.
- As α can only change its bound variables, which are quantified universally in the universal closure $\forall^\alpha$, the premiss implies $I, \eta, \nu' \models \phi \to \psi$, thus $I, \eta, \nu' \models \psi$ and $I, \eta, v \models \langle\alpha\rangle\psi$.

□

Soundness Proof

$$\frac{\vdash \forall^\alpha(\phi \to [\alpha]\phi)}{\phi \vdash [\alpha^*]\phi}$$

Proof (ind locally sound).

- For any I, η, v with $I, \eta, v \models \forall^\alpha(\phi \to [\alpha]\phi)$, we conclude $I, \eta, \nu' \models \phi \to [\alpha]\phi$ for all ν' with $(v, \nu') \in \rho_{I,\eta}(\alpha)$.

$\square$

Soundness Proof

$$\frac{\vdash \forall^{\alpha}(\phi \to [\alpha]\phi)}{\phi \vdash [\alpha^*]\phi}$$

Proof (ind locally sound).

- For any I, η, v with $I, \eta, v \models \forall^{\alpha}(\phi \to [\alpha]\phi)$, we conclude $I, \eta, \nu' \models \phi \to [\alpha]\phi$ for all ν' with $(v, \nu') \in \rho_{I,\eta}(\alpha)$.
- As these share the same η, we conclude $I, \eta, v \models \phi \to [\alpha^*]\phi$ by induction along the series of states ν' reached from v by repeating α.

$\square$

Soundness Proof

$$\frac{\vdash \forall^\alpha(\phi \to [\alpha]\phi)}{\phi \vdash [\alpha^*]\phi}$$

Proof (ind locally sound).

- For any I, η, v with $I, \eta, v \models \forall^\alpha(\phi \to [\alpha]\phi)$, we conclude $I, \eta, \nu' \models \phi \to [\alpha]\phi$ for all ν' with $(v, \nu') \in \rho_{I,\eta}(\alpha)$.
- As these share the same η, we conclude $I, \eta, v \models \phi \to [\alpha^*]\phi$ by induction along the series of states ν' reached from v by repeating α.
- The universal closure is necessary as, otherwise, the premiss may yield different η in different states ν'.

$\square$

Soundness Proof

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

Proof (con locally sound).

- Assume antecedent and premiss hold in I, η, v.

Soundness Proof

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

Proof (con locally sound).

- Assume antecedent and premiss hold in I, η, v.
- By premiss, $I, \eta[v \mapsto d], \nu' \models v > 0 \land \varphi(v) \to \langle\alpha\rangle\varphi(v-1)$ for all $d \in \mathbb{R}$ and all states ν' that are reachable by α^* from v, because $\forall^\alpha$ comprises all variables that are bound by α or by α^*.

Soundness Proof

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

Proof (con locally sound).

- Assume antecedent and premiss hold in I, η, ν.
- By premiss, $I, \eta[v \mapsto d], \nu' \models v > 0 \land \varphi(v) \to \langle\alpha\rangle\varphi(v-1)$ for all $d \in \mathbb{R}$ and all states ν' that are reachable by α^* from ν, because $\forall^\alpha$ comprises all variables that are bound by α or by α^*.
- By antecedent, there is a $d \in \mathbb{R}$ such that $I, \eta[v \mapsto d], \nu \models \varphi(v)$.

Soundness Proof

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

Proof (con locally sound).

- If $d \leq 0$, we have $I, \eta, v \models \langle\alpha^*\rangle\exists v{\le}0\, \varphi(v)$ for zero repetitions.

$\square$

Soundness Proof

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

Proof (con locally sound).

- If $d \le 0$, we have $I, \eta, v \models \langle\alpha^*\rangle\exists v{\le}0\, \varphi(v)$ for zero repetitions.
- Otherwise, if $d > 0$, we have, by premiss, that

$$I, \eta[v \mapsto d], v \models v > 0 \land \varphi(v) \to \langle\alpha\rangle\varphi(v-1)$$

$\square$

Soundness Proof

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

Proof (con locally sound).

- If $d \le 0$, we have $I, \eta, \nu \models \langle\alpha^*\rangle\exists v{\le}0\, \varphi(v)$ for zero repetitions.
- Otherwise, if $d > 0$, we have, by premiss, that

$$I, \eta[v \mapsto d], \nu \models v > 0 \land \varphi(v) \to \langle\alpha\rangle\varphi(v-1)$$

- As $v > 0 \land \varphi(v)$, we have for some ν' with $(\nu, \nu') \in \rho_{I,\eta[v\mapsto d]}(\alpha)$ that $I, \eta[v \mapsto d], \nu' \models \varphi(v-1)$.

$\square$

Soundness Proof

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

Proof (con locally sound).

- If $d \leq 0$, we have $I, \eta, v \models \langle\alpha^*\rangle\exists v{\leq}0\,\varphi(v)$ for zero repetitions.
- Otherwise, if $d > 0$, we have, by premiss, that

$$I, \eta[v \mapsto d], v \models v > 0 \wedge \varphi(v) \rightarrow \langle\alpha\rangle\varphi(v-1)$$

- As $v > 0 \wedge \varphi(v)$, we have for some ν' with $(v, \nu') \in \rho_{I,\eta[v\mapsto d]}(\alpha)$ that $I, \eta[v \mapsto d], \nu' \models \varphi(v-1)$.
- Thus, $I, \eta[v \mapsto d-1], \nu' \models \varphi(v)$ satisfies IH for a smaller d and a reachable ν', because $(v, \nu') \in \rho_{I,\eta}(\alpha)$ as v does not occur in α.

□

Soundness Proof

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

Proof (con locally sound).

- If $d \leq 0$, we have $I, \eta, v \models \langle\alpha^*\rangle\exists v{\leq}0\,\varphi(v)$ for zero repetitions.
- Otherwise, if $d > 0$, we have, by premiss, that

$$I, \eta[v \mapsto d], v \models v > 0 \land \varphi(v) \to \langle\alpha\rangle\varphi(v-1)$$

- As $v > 0 \land \varphi(v)$, we have for some ν' with $(v, \nu') \in \rho_{I,\eta[v\mapsto d]}(\alpha)$ that $I, \eta[v \mapsto d], \nu' \models \varphi(v-1)$.
- Thus, $I, \eta[v \mapsto d-1], \nu' \models \varphi(v)$ satisfies IH for a smaller d and a reachable ν', because $(v, \nu') \in \rho_{I,\eta}(\alpha)$ as v does not occur in α.
- Induction well-founded, because d decreases by 1 down to $d \leq 0$.

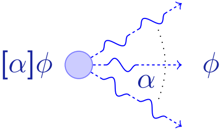
$\square$

Outline

Summary

differential dynamic logic

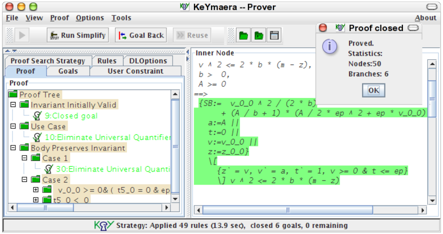
$$d\mathcal{L} = \text{DL} + \text{HP}$$



Verifying parametric hybrid systems:

- Logics for hybrid systems
- Compositional calculi
- $\mathbb{R}$-Skolem and free variables for automation
- Sound & complete / ODE

KeYmaera



Landscape


Logical Analysis of Hybrid Systems
Logic
Proof Calculus
Theorem Proving
Model Checking
Algebra
Computer Algebra
Algebraic Geometry
Differential Algebra
Algorithms
Fixedpoint Loops
Proof Strategies
Decision Procedures
Analysis
Differential Equations
Dynamical Systems
Differen-tiation

A. Platzer.
Differential dynamic logic for verifying parametric hybrid systems.
In N. Olivetti, editor, *TABLEAUX*, volume 4548 of *LNCS*, pages 216–232. Springer, 2007.

A. Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

A. Platzer.
Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.
Springer, Heidelberg, 2010.