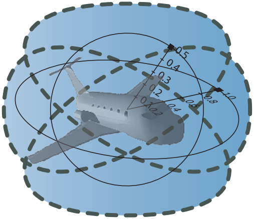
15-819/18-879: Logical Analysis of Hybrid Systems

28: Complete Axiomatization of Differential Dynamic Logic

André Platzer

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



Outline

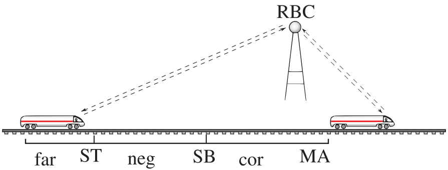
Outline

1. Verification Calculus for Differential Dynamic Logic d$\mathcal{L}$
   - Compositionality Motives
2. Soundness
3. Completeness
   - Incompleteness
   - Completeness
   - Expressibility and Rendition of Hybrid Programs
   - Relative Completeness of First-Order Assertions
   - Relative Completeness of Differential Logic Calculus

$\mathcal{A}$ d$\mathcal{L}$ Motives: The Logic of Hybrid Systems

differential dynamic logic

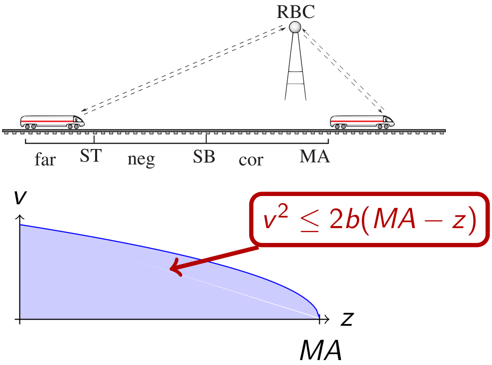
$$d\mathcal{L} = \quad DL + HP$$



d$\mathcal{L}$ Motives: Regions in First-order Logic

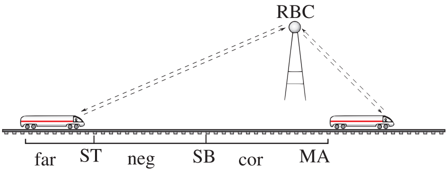
differential dynamic logic

$$\mathrm{d}\mathcal{L} = \mathrm{FOL}_{\mathbb{R}}$$



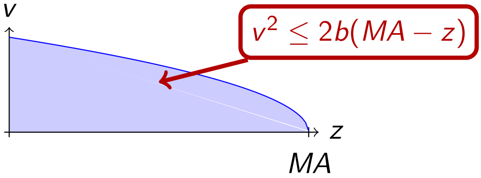
differential dynamic logic

$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}}$



$\forall MA\, \exists SB \ldots$

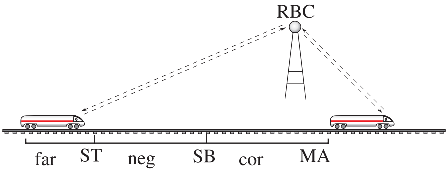
$\forall t{\geq}0 \ldots$



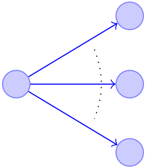
dℒ Motives: State Transitions in Dynamic Logic

differential dynamic logic

$\mathrm{d}\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} +$

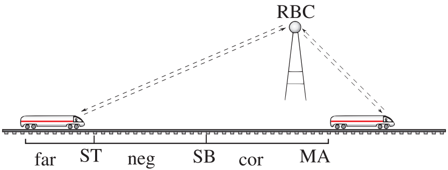


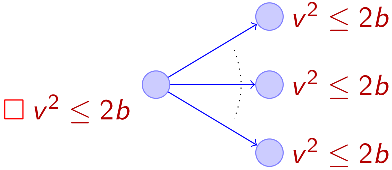
$v^2 \leq 2b$



differential dynamic logic

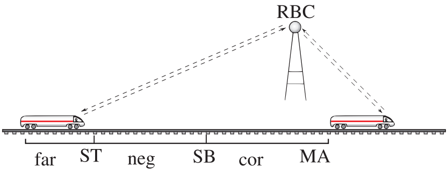
$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{ML}$

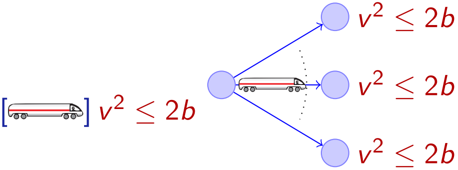




differential dynamic logic

$$\mathrm{d}\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL}$$

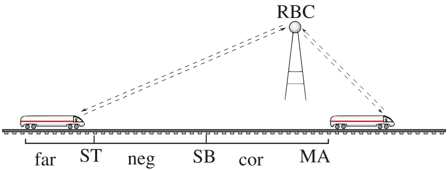




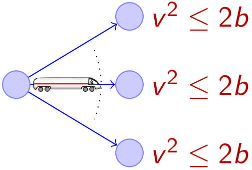
$d\mathcal{L}$ Motives: Hybrid Programs as Uniform Model

differential dynamic logic

$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL} + \mathrm{HP}$



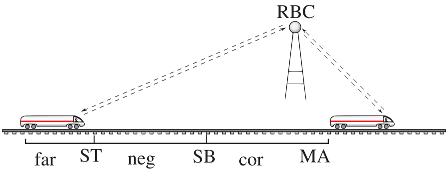
$[z'' = a]\, v^2 \leq 2b$



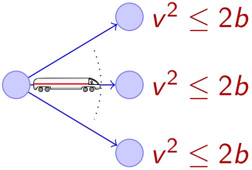
$d\mathcal{L}$ Motives: Hybrid Programs as Uniform Model

differential dynamic logic

$d\mathcal{L} = \text{FOL}_{\mathbb{R}} + \text{DL} + \text{HP}$



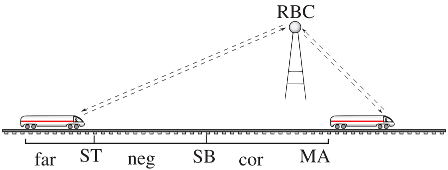
$[\text{if}(z > SB)\ a := -b;\ z'' = a]\ v^2 \le 2b$



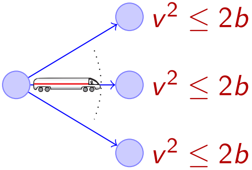
$d\mathcal{L}$ Motives: Hybrid Programs as Uniform Model

differential dynamic logic

$$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL} + \mathrm{HP}$$



$$[\underbrace{\mathtt{if}(z > SB)\, a := -b;\ z'' = a}_{\text{hybrid program}}]\, v^2 \leq 2b$$



10 propositional rules

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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
- Free variables & Skolemization

Outline

1. Verification Calculus for Differential Dynamic Logic $d\mathcal{L}$
   - Compositionality Motives
2. Soundness
3. Completeness
   - Incompleteness
   - Completeness
   - Expressibility and Rendition of Hybrid Programs
   - Relative Completeness of First-Order Assertions
   - Relative Completeness of Differential Logic Calculus

Completeness

Can we prove all valid formulas of d$\mathcal{L}$?

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

Incompleteness

Theorem (Incompleteness)

Both the discrete fragment and the continuous fragment of $\mathrm{d}\mathcal{L}$ are not effectively axiomatisable, i.e., they have no sound and complete effective calculus, because natural numbers are definable in both fragments.

Incompleteness

Theorem (Incompleteness)

Both the discrete fragment and the continuous fragment of $\mathrm{d}\mathcal{L}$ are not effectively axiomatisable, i.e., they have no sound and complete effective calculus, because natural numbers are definable in both fragments.

Theorem (Gödels's Incompleteness'31)

First-order logic with (non-linear) arithmetic of natural numbers has no sound and complete effective calculus.

Incompleteness

Proof (Incompleteness).

Discrete fragment:

$$\langle (x := x+1)^* \rangle\ x = n$$

$$\xrightarrow{+1}\xrightarrow{+1}\xrightarrow{+1}\xrightarrow{+1}\xrightarrow{+1}$$

$\square$

Incompleteness

Proof (Incompleteness).

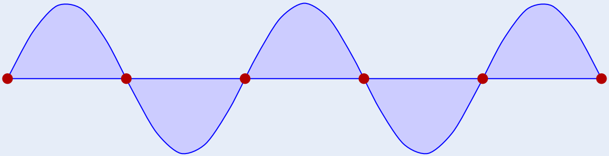
Discrete fragment:

$$\langle (x := x + 1)^* \rangle \; x = n$$

$$\xrightarrow{+1}\xrightarrow{+1}\xrightarrow{+1}\xrightarrow{+1}\xrightarrow{+1}$$

Continuous fragment:

$$\langle s'' = -s, \tau' = 1 \rangle (s = 0 \land \tau = n) \qquad \rightsquigarrow s = \sin$$



$\square$

Incompleteness

Proof (Incompleteness).

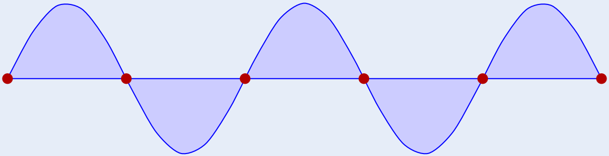
Discrete fragment:

$$\langle (x := x + 1)^* \rangle\ x = n$$

$$\xrightarrow{+1}\xrightarrow{+1}\xrightarrow{+1}\xrightarrow{+1}\xrightarrow{+1}$$

Continuous fragment:

$$\langle s'' = -s, \tau' = 1 \rangle (s = 0 \land \tau = n) \qquad \rightsquigarrow s = \sin$$



What's missing in characterization? $\square$

Incompleteness

Proof (Incompleteness).

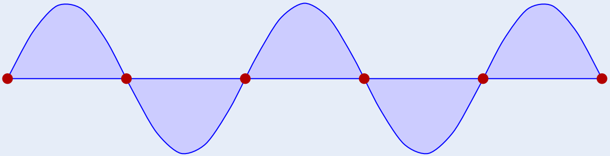
Discrete fragment:

$$\langle (x := x+1)^* \rangle \; x = n$$

$$\xrightarrow{+1}\xrightarrow{+1}\xrightarrow{+1}\xrightarrow{+1}\xrightarrow{+1}$$

Continuous fragment:

$$\langle s'' = -s, \tau' = 1 \rangle (s = 0 \land \tau = n) \qquad \leadsto s = \sin$$



What's missing in characterization? $s \neq 0 \lor s'(0) \neq 0$ $\square$

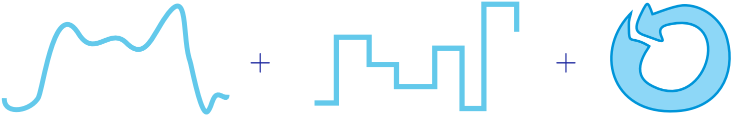
Incomplete! But are we missing proof rules?

Incomplete! But are we missing proof rules?

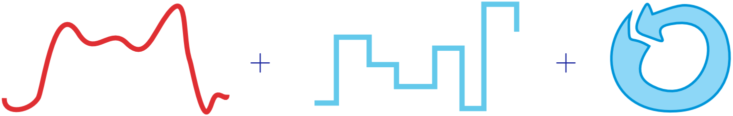
Relativity

Cook,Harel: discrete-DL/data$_{\mathbb{N}}$ hybrid-d$\mathcal{L}$/data$_{\mathbb{R}}$??

Sources of Incompleteness

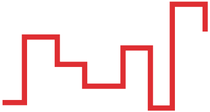
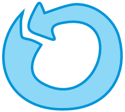


Sources of Incompleteness



continuous

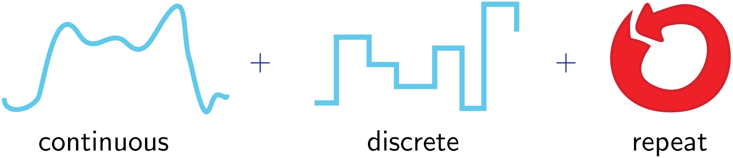
Sources of Incompleteness

 +  + 

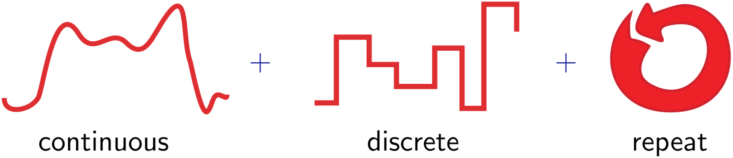
continuous

discrete

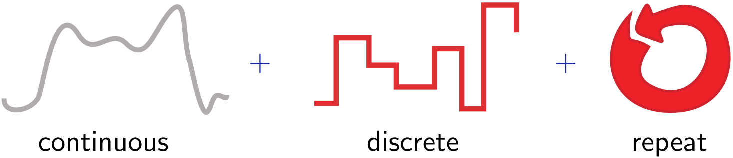
Sources of Incompleteness



Sources of Incompleteness



Relative Completeness



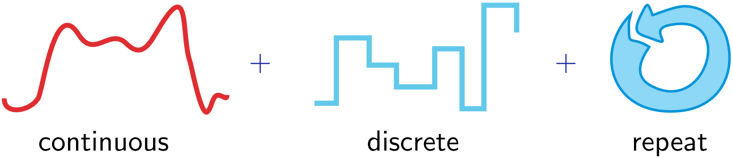
Relative Completeness

continuous + discrete + repeat

Theorem (Relative Completeness)

d$\mathcal{L}$ *calculus is a sound & complete axiomatisation of hybrid systems relative to differential equations.*

Proof Outline 15p

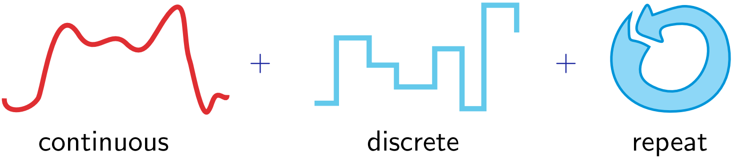


Relative Completeness

Theorem (Relative Completeness)

d$\mathcal{L}$ *calculus is a sound & complete axiomatisation of hybrid systems relative to differential equations.*

Proof Outline 15p



$\Downarrow$

Relativity

Cook,Harel: discrete-DL/data P.: hybrid-d$\mathcal{L}$/differential equations

First-Order Logic of Differential Equations FOD

Definition (First-Order Logic of Differential Equations)

$$\mathsf{FOD} = \mathsf{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$$

$$\mathsf{FOD}\ \phi ::= \theta_1 \geq \theta_2 \mid \neg\phi \mid \phi_1 \land \phi_2 \mid \forall x\, \phi \mid \exists x\, \phi \mid [x_1' = \theta_1, \ldots, x_n' = \theta_n]\phi$$

First-Order Logic of Differential Equations FOD

Definition (First-Order Logic of Differential Equations)

$$\mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$$

$$\mathrm{FOD}\ \phi ::= \theta_1 \geq \theta_2 \mid \neg\phi \mid \phi_1 \land \phi_2 \mid \forall x\, \phi \mid \exists x\, \phi \mid [x_1' = \theta_1, \ldots, x_n' = \theta_n]\phi$$

$$\mathrm{FOD}\ \phi ::= \theta_1 \geq \theta_2 \mid \neg\phi \mid \phi_1 \land \phi_2 \mid \forall x\, \phi \mid \exists x\, \phi \mid [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$$

with $\mathrm{FOL}_{\mathbb{R}}$-formula F

First-Order Logic of Differential Equations FOD

Definition (First-Order Logic of Differential Equations)

$$\text{FOD} = \text{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \dots, x_n' = \theta_n]F$$

$$\text{FOD} \quad \phi ::= \theta_1 \geq \theta_2 \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \forall x\, \phi \mid \exists x\, \phi \mid [x_1' = \theta_1, \dots, x_n' = \theta_n]\phi$$

$$\text{FOD} \quad \phi ::= \theta_1 \geq \theta_2 \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \forall x\, \phi \mid \exists x\, \phi \mid [x_1' = \theta_1, \dots, x_n' = \theta_n]F$$

with $\text{FOL}_{\mathbb{R}}$-formula F

both will do

Relative Completeness

Theorem (Relative Completeness)

d$\mathcal{L}$ *calculus is complete relative to first-order logic of differential equations.*

$$\vDash \phi \quad \textit{iff} \quad \mathit{Taut}_{\mathit{FOD}} \vdash \phi$$

where $\quad \mathit{FOD} = \mathit{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

▸ Proof Outline 15p

Relative Completeness

Theorem (Relative Completeness)

d$\mathcal{L}$ *calculus is complete relative to first-order logic of differential equations.*

$$\vDash \phi \quad \textit{iff} \quad Taut_{FOD} \vdash \phi$$

where $\quad FOD = FOL_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

▸ Proof Outline 15p

Corollary (Proof-theoretical Alignment)

verification of hybrid systems = verification of dynamical systems!

Relative Completeness Proof

$$\vDash \phi \quad \text{iff} \quad Taut_{\mathrm{FOD}} \vdash \phi$$

where $\quad \mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \dots, x_n' = \theta_n]F$

Return

Proof (Relative Completeness, 15 pages).

1. Strong enough invariants and variants expressible in d$\mathcal{L}$
2. d$\mathcal{L}$ expressible in FOD
3. valid d$\mathcal{L}$ formulas d$\mathcal{L}$-derivable from corresponding FOD axioms
4. finite FOD formula characterising unbounded hybrid repetition
5. FOD characterises $\mathbb{R}$-Gödel encoding
6. First-order expressible & program rendition:
   for each ϕ there is $F \in \mathrm{FOD}$ $\vDash \phi \leftrightarrow F$
7. Propositionally & first-order complete
8. Relative complete for first-order safety $F \to [\alpha]G$
9. Relative complete for first-order liveness $F \to \langle\alpha\rangle G$

Return

Relative Completeness Proof

$$\vDash \phi \quad \text{iff} \quad Taut_{\mathrm{FOD}} \vdash \phi$$

where $\quad \mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

Return

Proof (Relative Completeness, 15 pages).

1. Strong enough invariants and variants expressible in d$\mathcal{L}$
2. d$\mathcal{L}$ expressible in FOD
3. valid d$\mathcal{L}$ formulas d$\mathcal{L}$-derivable from corresponding FOD axioms
4. finite FOD formula characterising unbounded hybrid repetition
5. FOD characterises $\mathbb{R}$-Gödel encoding
6. First-order expressible & program rendition:
   for each ϕ there is $F \in \mathrm{FOD}$ $\vDash \phi \leftrightarrow F$
7. Propositionally & first-order complete
8. Relative complete for first-order safety $F \rightarrow [\alpha]G$
9. Relative complete for first-order liveness $F \rightarrow \langle\alpha\rangle G$

Return

Relative Completeness Proof

$$\vDash \phi \quad \text{iff} \quad Taut_{\mathsf{FOD}} \vdash \phi$$

where $\quad \mathsf{FOD} = \mathsf{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

◂ Return

Proof (Relative Completeness, 15 pages).

1. Strong enough invariants and variants expressible in d$\mathcal{L}$
2. d$\mathcal{L}$ expressible in FOD
3. valid d$\mathcal{L}$ formulas d$\mathcal{L}$-derivable from corresponding FOD axioms
4. finite FOD formula characterising unbounded hybrid repetition
5. FOD characterises $\mathbb{R}$-Gödel encoding
6. First-order expressible & program rendition:
   for each ϕ there is $F \in \mathsf{FOD}$ $\vDash \phi \leftrightarrow F$
7. Propositionally & first-order complete
8. Relative complete for first-order safety $F \rightarrow [\alpha]G$
9. Relative complete for first-order liveness $F \rightarrow \langle\alpha\rangle G$

◂ Return

$$\vDash \phi \quad \text{iff} \quad Taut_{\mathsf{FOD}} \vdash \phi$$

where $\mathsf{FOD} = \mathsf{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

◂ Return

Proof (Relative Completeness, 15 pages).

1. Strong enough invariants and variants expressible in d$\mathcal{L}$
2. d$\mathcal{L}$ expressible in FOD
3. valid d$\mathcal{L}$ formulas d$\mathcal{L}$-derivable from corresponding FOD axioms
4. finite FOD formula characterising unbounded hybrid repetition
5. FOD characterises $\mathbb{R}$-Gödel encoding
6. First-order expressible & program rendition:
   for each ϕ there is $F \in \mathsf{FOD}$ $\vDash \phi \leftrightarrow F$
7. Propositionally & first-order complete
8. Relative complete for first-order safety $F \rightarrow [\alpha]G$
9. Relative complete for first-order liveness $F \rightarrow \langle\alpha\rangle G$

◂ Return

Relative Completeness Proof

$$\vDash \phi \quad \text{iff} \quad Taut_{\mathsf{FOD}} \vdash \phi$$

where $\mathsf{FOD} = \mathsf{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

Return

Proof (Relative Completeness, 15 pages).

1. Strong enough invariants and variants expressible in d$\mathcal{L}$
2. d$\mathcal{L}$ expressible in FOD
3. valid d$\mathcal{L}$ formulas d$\mathcal{L}$-derivable from corresponding FOD axioms
4. finite FOD formula characterising unbounded hybrid repetition
5. FOD characterises $\mathbb{R}$-Gödel encoding
6. First-order expressible & program rendition:
   for each ϕ there is $F \in \mathsf{FOD}$ $\vDash \phi \leftrightarrow F$
7. Propositionally & first-order complete
8. Relative complete for first-order safety $F \to [\alpha]G$
9. Relative complete for first-order liveness $F \to \langle\alpha\rangle G$

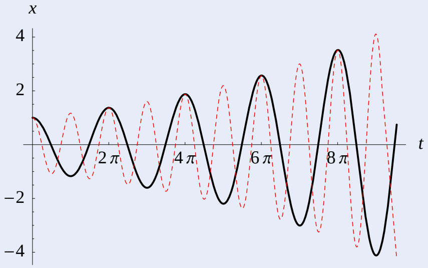
Return

Relative Completeness Proof

where $\quad \text{FOD} = \text{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \dots, x_n' = \theta_n]F$ ◂ Return

Proof ($\mathbb{R}$-Gödel encoding).

FOD characterises constructive bijection $\mathbb{R} \to \mathbb{R}^2$



□

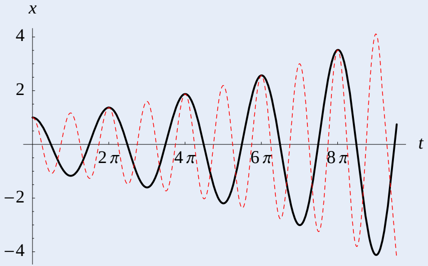
Relative Completeness Proof

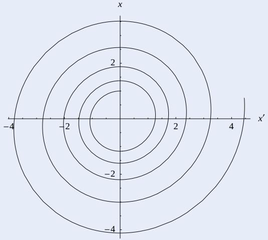
where $\quad \text{FOD} = \text{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

◂ Return

Proof ($\mathbb{R}$-Gödel encoding).

FOD characterises constructive bijection $\mathbb{R} \to \mathbb{R}^2$





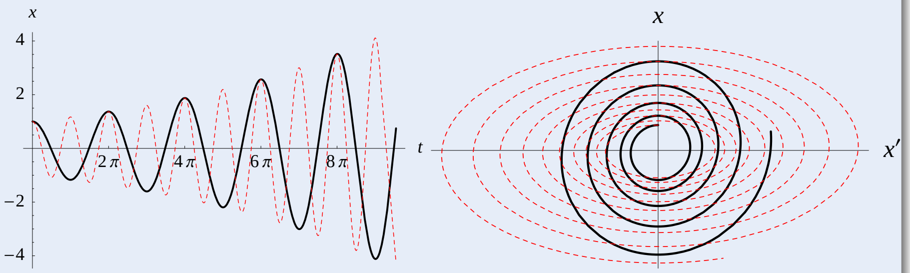
□

Relative Completeness Proof

where FOD $= \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$ Return

Proof ($\mathbb{R}$-Gödel encoding).

FOD characterises constructive bijection $\mathbb{R} \to \mathbb{R}^2$

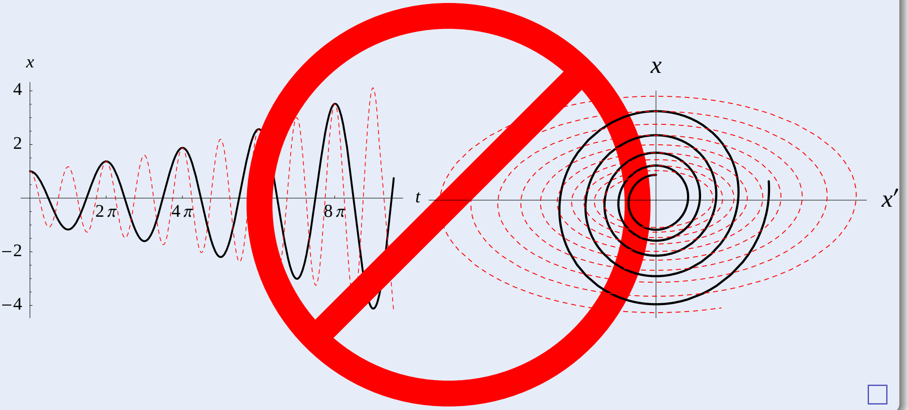


$\square$

where $\text{FOD} = \text{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$ Return

Proof ($\mathbb{R}$-Gödel encoding).

FOD characterises constructive bijection $\mathbb{R} \to \mathbb{R}^2$ not differentiable!



□

Relative Completeness Proof

where $\quad \text{FOD} = \text{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$ ◂ Return

Proof ($\mathbb{R}$-Gödel encoding).

FOD characterises constructive bijection $\mathbb{R} \to \mathbb{R}^2$

$$\sum_{i=0}^{\infty} \frac{a_i}{2^i} = a_0.a_1a_2\ldots$$

$$\sum_{i=0}^{\infty} \frac{b_i}{2^i} = b_0.b_1b_2\ldots$$

$$\sum_{i=0}^{\infty} \left(\frac{a_i}{2^{2i-1}} + \frac{b_i}{2^{2i}} \right) = a_0b_0.a_1b_1a_2b_2\ldots$$

□

Relative Completeness Proof

where $\quad \text{FOD} = \text{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$ Return

Proof ($\mathbb{R}$-Gödel encoding).

FOD characterises constructive bijection $\mathbb{R} \to \mathbb{R}^2$

$$\sum_{i=0}^{\infty} \frac{a_i}{2^i} = a_0.a_1a_2\ldots \qquad \sum_{i=0}^{\infty} \frac{b_i}{2^i} = b_0.b_1b_2\ldots$$

$$\sum_{i=0}^{\infty} \left(\frac{a_i}{2^{2i-1}} + \frac{b_i}{2^{2i}}\right) = a_0b_0.a_1b_1a_2b_2\ldots$$

$$\begin{aligned}
\text{at}(Z,n,j,z) &\leftrightarrow \forall i\!:\!\mathbb{Z}\ \ \text{digit}(z,i) = \text{digit}(Z, n(i-1)+j) \wedge n > 0 \wedge n,j \in \mathbb{N} \\
\text{digit}(a,i) &= \text{intpart}(2\,\text{frac}(2^{i-1}a)) \\
\text{intpart}(a) &= a - \text{frac}(a) \\
\text{frac}(a) = z &\leftrightarrow \exists i\!:\!\mathbb{Z}\ \ z = a - i \wedge -1 < z \wedge z < 1 \wedge az \geq 0 \quad \text{“keep sign”}
\end{aligned}$$

$\square$

where $\quad \mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$ Return

Proof ($\mathbb{R}$-Gödel encoding).

FOD characterises constructive bijection $\mathbb{R} \to \mathbb{R}^2$

$$\sum_{i=0}^{\infty} \frac{a_i}{2^i} = a_0.a_1a_2\ldots \qquad \sum_{i=0}^{\infty} \frac{b_i}{2^i} = b_0.b_1b_2\ldots$$

$$\sum_{i=0}^{\infty} \left(\frac{a_i}{2^{2i-1}} + \frac{b_i}{2^{2i}} \right) = a_0b_0.a_1b_1a_2b_2\ldots$$

$$\mathrm{at}(Z,n,j,z) \leftrightarrow \forall i{:}\mathbb{Z}\ \ \mathrm{digit}(z,i) = \mathrm{digit}(Z, n(i-1)+j) \land n > 0 \land n,j \in \mathbb{N}$$

$$\mathrm{digit}(a,i) = \mathrm{intpart}(2\,\mathrm{frac}(2^{i-1}a))$$

$$\mathrm{intpart}(a) = a - \mathrm{frac}(a)$$

$$\mathrm{frac}(a) = z \leftrightarrow \exists i{:}\mathbb{Z}\ \ z = a - i \land -1 < z \land z < 1 \land az \geq 0 \qquad \text{“keep sign”}$$

□

Relative Completeness Proof

where $\quad \text{FOD} = \text{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

Return

Proof ($\mathbb{R}$-Gödel encoding).

FOD characterises constructive bijection $\mathbb{R} \to \mathbb{R}^2$

$$\begin{array}{l} \displaystyle\sum_{i=0}^{\infty} \frac{a_i}{2^i} = a_0.a_1a_2\ldots \\ \displaystyle\sum_{i=0}^{\infty} \frac{b_i}{2^i} = b_0.b_1b_2\ldots \end{array} \rightarrow \sum_{i=0}^{\infty} \left(\frac{a_i}{2^{2i-1}} + \frac{b_i}{2^{2i}} \right) = a_0b_0.a_1b_1a_2b_2\ldots$$

$$\begin{aligned} 2^i = z \leftrightarrow\ & i \geq 0 \land \langle x := 1; t := 0; x' = x \ln 2, t' = 1 \rangle (t = i \land x = z) \\ \lor\ & i < 0 \land \langle x := 1; t := 0; x' = -x \ln 2, t' = -1 \rangle (t = i \land x = z) \end{aligned}$$

$$\ln 2 = z \leftrightarrow \langle x := 1; t := 0; x' = x, t' = 1 \rangle (x = 2 \land t = z)$$

$\square$

Relative Completeness Proof

$$\vDash \phi \quad \text{iff} \quad Taut_{\mathrm{FOD}} \vdash \phi$$

where $\quad \mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

Return

Proof (Relative Completeness, 15 pages).

1. Strong enough invariants and variants expressible in $\mathsf{d}\mathcal{L}$
2. $\mathsf{d}\mathcal{L}$ expressible in FOD
3. valid $\mathsf{d}\mathcal{L}$ formulas $\mathsf{d}\mathcal{L}$-derivable from corresponding FOD axioms
4. finite FOD formula characterising unbounded hybrid repetition
5. FOD characterises $\mathbb{R}$-Gödel encoding
6. First-order expressible & program rendition:
   for each ϕ there is $F \in \mathrm{FOD}$ $\vDash \phi \leftrightarrow F$
7. Propositionally & first-order complete
8. Relative complete for first-order safety $F \to [\alpha]G$
9. Relative complete for first-order liveness $F \to \langle\alpha\rangle G$

Return

□

Relative Completeness Proof

$$\vDash \phi \quad \text{iff} \quad Taut_{\mathrm{FOD}} \vdash \phi$$

where $\quad \mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \dots, x_n' = \theta_n]F$

Return

Proof (Relative Completeness, 15 pages).

1. Strong enough invariants and variants expressible in d$\mathcal{L}$
2. d$\mathcal{L}$ expressible in FOD
3. valid d$\mathcal{L}$ formulas d$\mathcal{L}$-derivable from corresponding FOD axioms
4. finite FOD formula characterising unbounded hybrid repetition
5. FOD characterises $\mathbb{R}$-Gödel encoding
6. First-order expressible & program rendition:
   for each ϕ there is $F \in \mathrm{FOD}$ $\vDash \phi \leftrightarrow F$
7. Propositionally & first-order complete
8. Relative complete for first-order safety $F \rightarrow [\alpha]G$
9. Relative complete for first-order liveness $F \rightarrow \langle\alpha\rangle G$

Return

$\square$

Relative Completeness Proof

$$\vDash \phi \quad \text{iff} \quad Taut_{\mathrm{FOD}} \vdash \phi$$

where $\quad \mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

Return

Proof (Relative Completeness, 15 pages).

1. Strong enough invariants and variants expressible in d$\mathcal{L}$
2. d$\mathcal{L}$ expressible in FOD
3. valid d$\mathcal{L}$ formulas d$\mathcal{L}$-derivable from corresponding FOD axioms
4. finite FOD formula characterising unbounded hybrid repetition
5. FOD characterises $\mathbb{R}$-Gödel encoding
6. First-order expressible & program rendition:
   for each ϕ there is $F \in \mathrm{FOD}$ $\vDash \phi \leftrightarrow F$
7. Propositionally & first-order complete
8. Relative complete for first-order safety $F \to [\alpha]G$
9. Relative complete for first-order liveness $F \to \langle\alpha\rangle G$

Return

□

Relative Completeness Proof

$$\vDash \phi \quad \text{iff} \quad Taut_{\mathrm{FOD}} \vdash \phi$$

where $\quad \mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

Return

Proof (Relative Completeness, 15 pages).

1. Strong enough invariants and variants expressible in d$\mathcal{L}$
2. d$\mathcal{L}$ expressible in FOD
3. valid d$\mathcal{L}$ formulas d$\mathcal{L}$-derivable from corresponding FOD axioms
4. finite FOD formula characterising unbounded hybrid repetition
5. FOD characterises $\mathbb{R}$-Gödel encoding
6. First-order expressible & program rendition:
   for each ϕ there is $F \in \mathrm{FOD}$ $\vDash \phi \leftrightarrow F$
7. Propositionally & first-order complete
8. Relative complete for first-order safety $F \rightarrow [\alpha]G$
9. Relative complete for first-order liveness $F \rightarrow \langle\alpha\rangle G$

Return

□

Program Rendition in FOD

Lemma (Program rendition)

For every HP α with variables among $\vec{x} = x_1, \ldots, x_k$ there is a FOD-formula $\mathcal{S}_\alpha(\vec{x}, \vec{v})$ with variables among the $2k$ distinct variables $\vec{x} = x_1, \ldots, x_k$ and $\vec{v} = v_1, \ldots, v_k$ such that

$$\vDash \mathcal{S}_\alpha(\vec{x}, \vec{v}) \leftrightarrow \langle\alpha\rangle \vec{x} = \vec{v}$$

or, equivalently, for every I, η, v,

$$I, \eta, v \models \mathcal{S}_\alpha(\vec{x}, \vec{v}) \text{ iff } (v, v[\vec{x} \mapsto [\![\vec{v}]\!]_{I,v,\eta}]) \in \rho_{I,\eta}(\alpha) \ .$$

Program Rendition Proof

Proof.

$$\mathcal{S}_{x_1:=\theta_1,..,x_k:=\theta_k}(\vec{x},\vec{v}) \equiv \bigwedge_{i=1}^{k}(v_i = \theta_i)$$

$$\mathcal{S}_{x_1'=\theta_1,..,x_k'=\theta_k}(\vec{x},\vec{v}) \equiv \langle x_1' = \theta_1,\ldots,x_k' = \theta_k\rangle\, \vec{v} = \vec{x}$$

$$\mathcal{S}_{x_1'=\theta_1,..,x_k'=\theta_k\wedge\chi}(\vec{x},\vec{v}) \equiv \langle t := 0; x_1'{=}\theta_1,\ldots,x_k'{=}\theta_k, t'{=}1\rangle\big(\vec{v} = \vec{x}$$
$$\wedge\, [x_1' = -\theta_1,\ldots,x_k' = -\theta_k, t' = -1](t \geq 0 \to \chi)\big)$$

$$\mathcal{S}_{?\chi}(\vec{x},\vec{v}) \equiv \vec{v} = \vec{x} \wedge \chi$$

$$\mathcal{S}_{\beta\cup\gamma}(\vec{x},\vec{v}) \equiv \mathcal{S}_\beta(\vec{x},\vec{v}) \vee \mathcal{S}_\gamma(\vec{x},\vec{v})$$

$$\mathcal{S}_{\beta;\gamma}(\vec{x},\vec{v}) \equiv \exists\vec{z}\,(\mathcal{S}_\beta(\vec{x},\vec{z}) \wedge \mathcal{S}_\gamma(\vec{z},\vec{v}))$$

$$\mathcal{S}_{\beta^*}(\vec{x},\vec{v}) \equiv \exists Z\,\exists n:\mathbb{N}\ \big(Z_1^{(n)} = \vec{x} \wedge Z_n^{(n)} = \vec{v}$$
$$\wedge\,\forall i:\mathbb{N}\ (1 \leq i < n \to \mathcal{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)}))\big)$$

□

Program Rendition Proof

Proof.

$$\mathcal{S}_{x_1:=\theta_1,..,x_k:=\theta_k}(\vec{x},\vec{v}) \equiv \bigwedge_{i=1}^{k}(v_i = \theta_i)$$

$$\mathcal{S}_{x_1'=\theta_1,..,x_k'=\theta_k}(\vec{x},\vec{v}) \equiv \langle x_1' = \theta_1, \ldots, x_k' = \theta_k\rangle\, \vec{v} = \vec{x}$$

$$\mathcal{S}_{x_1'=\theta_1,..,x_k'=\theta_k \wedge \chi}(\vec{x},\vec{v}) \equiv \langle t := 0; x_1'=\theta_1, \ldots, x_k'=\theta_k, t'=1\rangle\big(\vec{v} = \vec{x} \wedge [x_1' = -\theta_1, \ldots, x_k' = -\theta_k, t' = -1](t \geq 0 \to \chi)\big)$$

$$\mathcal{S}_{?\chi}(\vec{x},\vec{v}) \equiv \vec{v} = \vec{x} \wedge \chi$$

$$\mathcal{S}_{\beta\cup\gamma}(\vec{x},\vec{v}) \equiv \mathcal{S}_{\beta}(\vec{x},\vec{v}) \vee \mathcal{S}_{\gamma}(\vec{x},\vec{v})$$

$$\mathcal{S}_{\beta;\gamma}(\vec{x},\vec{v}) \equiv \exists \vec{z}\,(\mathcal{S}_{\beta}(\vec{x},\vec{z}) \wedge \mathcal{S}_{\gamma}(\vec{z},\vec{v}))$$

$$\mathcal{S}_{\beta^*}(\vec{x},\vec{v}) \equiv \exists Z\, \exists n : \mathbb{N}\, \Big(Z_1^{(n)} = \vec{x} \wedge Z_n^{(n)} = \vec{v} \wedge \forall i : \mathbb{N}\, (1 \leq i < n \to \mathcal{S}_{\beta}(Z_i^{(n)}, Z_{i+1}^{(n)}))\Big)$$

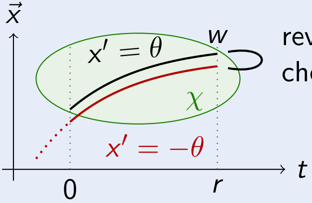
□

Program Rendition Proof

Proof.

$$\mathcal{S}_{x_1'=\theta_1,..,x_k'=\theta_k \wedge \chi}(\vec{x},\vec{v}) \equiv \langle t := 0; x_1'=\theta_1,\ldots,x_k'=\theta_k, t'=1\rangle (\vec{v} = \vec{x}$$

$$\wedge\, [x_1' = -\theta_1,\ldots,x_k' = -\theta_k, t' = -1](t \geq 0 \to \chi))$$



revert flow and time
check χ backwards

$\square$

Expressibility

Lemma (Expressibility)

d$\mathcal{L}$ expressible in FOD: for all d$\mathcal{L}$ formulas $\phi \in \mathrm{Fml}$ there is a FOD-formula $\phi^{\#} \in \mathrm{Fml}_{FOD}$ that is equivalent, i.e., $\vDash \phi \leftrightarrow \phi^{\#}$.

Proof.

The proof follows an induction on the structure of formula ϕ.

1. ϕ first-order, then $\phi^{\#} := \phi$ already is a FOD-formula.

Expressibility

Lemma (Expressibility)

d$\mathcal{L}$ expressible in FOD: for all d$\mathcal{L}$ formulas $\phi \in \mathrm{Fml}$ there is a FOD-formula $\phi^{\#} \in \mathrm{Fml}_{FOD}$ that is equivalent, i.e., $\vDash \phi \leftrightarrow \phi^{\#}$.

Proof.

The proof follows an induction on the structure of formula ϕ.

1. ϕ first-order, then $\phi^{\#} := \phi$ already is a FOD-formula.
2. $\phi \equiv \varphi \vee \psi$, then by IH there are FOD-formulas $\varphi^{\#}, \psi^{\#}$ such that $\vDash \varphi \leftrightarrow \varphi^{\#}$ and $\vDash \psi \leftrightarrow \psi^{\#}$. Thus by congruence $\vDash (\varphi \vee \psi) \leftrightarrow (\varphi^{\#} \vee \psi^{\#})$ giving $\vDash \phi \leftrightarrow \phi^{\#}$ for $\phi^{\#} \equiv \varphi^{\#} \vee \psi^{\#}$.

Expressibility

Lemma (Expressibility)

dℒ expressible in FOD: for all dℒ formulas $\phi \in \mathrm{Fml}$ there is a FOD-formula $\phi^{\#} \in \mathrm{Fml}_{FOD}$ that is equivalent, i.e., $\vDash \phi \leftrightarrow \phi^{\#}$.

Proof.

The proof follows an induction on the structure of formula ϕ.

1. ϕ first-order, then $\phi^{\#} := \phi$ already is a FOD-formula.
2. $\phi \equiv \varphi \vee \psi$, then by IH there are FOD-formulas $\varphi^{\#}, \psi^{\#}$ such that $\vDash \varphi \leftrightarrow \varphi^{\#}$ and $\vDash \psi \leftrightarrow \psi^{\#}$. Thus by congruence $\vDash (\varphi \vee \psi) \leftrightarrow (\varphi^{\#} \vee \psi^{\#})$ giving $\vDash \phi \leftrightarrow \phi^{\#}$ for $\phi^{\#} \equiv \varphi^{\#} \vee \psi^{\#}$.

$$\vDash \quad \langle\alpha\rangle\psi \leftrightarrow \exists \vec{v}\,(\mathcal{S}_\alpha(\vec{x},\vec{v}) \wedge \psi^{\#}{}^{\vec{v}}_{\vec{x}})$$

Expressibility

Lemma (Expressibility)

d$\mathcal{L}$ expressible in FOD: for all d$\mathcal{L}$ formulas $\phi \in \mathrm{Fml}$ there is a FOD-formula $\phi^\# \in \mathrm{Fml}_{FOD}$ that is equivalent, i.e., $\vDash \phi \leftrightarrow \phi^\#$.

Proof.

The proof follows an induction on the structure of formula ϕ.

1. ϕ first-order, then $\phi^\# := \phi$ already is a FOD-formula.
2. $\phi \equiv \varphi \vee \psi$, then by IH there are FOD-formulas $\varphi^\#, \psi^\#$ such that $\vDash \varphi \leftrightarrow \varphi^\#$ and $\vDash \psi \leftrightarrow \psi^\#$. Thus by congruence $\vDash (\varphi \vee \psi) \leftrightarrow (\varphi^\# \vee \psi^\#)$ giving $\vDash \phi \leftrightarrow \phi^\#$ for $\phi^\# \equiv \varphi^\# \vee \psi^\#$.

$$\vDash \quad \langle\alpha\rangle\psi \leftrightarrow \exists \vec{v}\,(\mathcal{S}_\alpha(\vec{x},\vec{v}) \wedge \psi^{\#\vec{v}}_{\;\;\vec{x}})$$

$$\vDash \quad [\alpha]\psi \leftrightarrow \forall \vec{v}\,(\mathcal{S}_\alpha(\vec{x},\vec{v}) \rightarrow \psi^{\#\vec{v}}_{\;\;\vec{x}})$$

Sequent Derivability

Lemma (Derivability of sequents)

$\vdash_{\mathcal{D}} \phi \rightarrow \psi$ *iff the sequent* $\phi \vdash \psi$ *is derivable from* $\mathcal{D}$*, denoted by* $\phi \vdash_{\mathcal{D}} \psi$*.*

Sequent Derivability

Lemma (Derivability of sequents)

$\vdash_{\mathcal{D}} \phi \to \psi$ *iff the sequent* $\phi \vdash \psi$ *is derivable from* $\mathcal{D}$*, denoted by* $\phi \vdash_{\mathcal{D}} \psi$*.*

Proof.

□

Sequent Derivability

Lemma (Derivability of sequents)

$\vdash_{\mathcal{D}} \phi \to \psi$ iff the sequent $\phi \vdash \psi$ is derivable from $\mathcal{D}$, denoted by $\phi \vdash_{\mathcal{D}} \psi$.

Proof.

- When sequents are abbreviations for formulas, both sides are identical.

$\square$

Sequent Derivability

Lemma (Derivability of sequents)

$\vdash_{\mathcal{D}} \phi \rightarrow \psi$ *iff the sequent* $\phi \vdash \psi$ *is derivable from* $\mathcal{D}$*, denoted by* $\phi \vdash_{\mathcal{D}} \psi$*.*

Proof.

- When sequents are abbreviations for formulas, both sides are identical.
- Otherwise, let $\vdash_{\mathcal{D}} \phi \rightarrow \psi$ be derivable from $\mathcal{D}$.

$\square$

Sequent Derivability

Lemma (Derivability of sequents)

$\vdash_{\mathcal{D}} \phi \to \psi$ *iff the sequent* $\phi \vdash \psi$ *is derivable from* $\mathcal{D}$*, denoted by* $\phi \vdash_{\mathcal{D}} \psi$*.*

Proof.

- When sequents are abbreviations for formulas, both sides are identical.
- Otherwise, let $\vdash_{\mathcal{D}} \phi \to \psi$ be derivable from $\mathcal{D}$.
- Using cut (and weakening), derivation can be extended to $\phi \vdash_{\mathcal{D}} \psi$:

$$\text{cut}\,\dfrac{\dfrac{*}{\phi \vdash \phi \to \psi, \psi} \qquad \to\text{l}\,\dfrac{\text{Ax}\,\dfrac{*}{\phi \vdash \phi, \psi} \qquad \text{Ax}\,\dfrac{*}{\psi, \phi \vdash \psi}}{\phi, \phi \to \psi \vdash \psi}}{\phi \vdash \psi}$$

$\square$

Sequent Derivability

Lemma (Derivability of sequents)

$\vdash_{\mathcal{D}} \phi \rightarrow \psi$ *iff the sequent* $\phi \vdash \psi$ *is derivable from* $\mathcal{D}$*, denoted by* $\phi \vdash_{\mathcal{D}} \psi$*.*

Proof.

- When sequents are abbreviations for formulas, both sides are identical.
- Otherwise, let $\vdash_{\mathcal{D}} \phi \rightarrow \psi$ be derivable from $\mathcal{D}$.
- Using cut (and weakening), derivation can be extended to $\phi \vdash_{\mathcal{D}} \psi$:

$$\dfrac{\dfrac{*}{\phi \vdash \phi \rightarrow \psi, \psi} \qquad \dfrac{\dfrac{*}{\phi \vdash \phi, \psi}\,\text{Ax} \qquad \dfrac{*}{\psi, \phi \vdash \psi}\,\text{Ax}}{\phi, \phi \rightarrow \psi \vdash \psi}\,{\rightarrow}\text{l}}{\phi \vdash \psi}\,\text{cut}$$

- The converse direction is by an application of $\rightarrow$r.

$\square$

Generalization

Lemma (Generalization)

If $\vdash_{\mathcal{D}} \phi$ *is provable without free logical variables, then so are* $\vdash_{\mathcal{D}} \forall x\, \phi$ *and* $\vdash_{\mathcal{D}} \langle x_1 := \theta_1, \ldots x_n := \theta_n \rangle \phi$.

Generalization

Lemma (Generalization)

If $\vdash_{\mathcal{D}} \phi$ *is provable without free logical variables, then so are* $\vdash_{\mathcal{D}} \forall x\, \phi$ *and* $\vdash_{\mathcal{D}} \langle x_1 := \theta_1, \dots x_n := \theta_n \rangle \phi$.

Proof Sketch.

$\square$

Generalization

Lemma (Generalization)

If $\vdash_{\mathcal{D}} \phi$ *is provable without free logical variables, then so are* $\vdash_{\mathcal{D}} \forall x\, \phi$ *and* $\vdash_{\mathcal{D}} \langle x_1 := \theta_1, \dots x_n := \theta_n \rangle \phi$.

Proof Sketch.

- Second part: Induction on the structure of proofs with inductive jump prefix transformation (1page proof).

$\square$

Generalization

Lemma (Generalization)

If $\vdash_{\mathcal{D}} \phi$ *is provable without free logical variables, then so are* $\vdash_{\mathcal{D}} \forall x\, \phi$ *and* $\vdash_{\mathcal{D}} \langle x_1 := \theta_1, \ldots x_n := \theta_n \rangle \phi$.

Proof Sketch.

- Second part: Induction on the structure of proofs with inductive jump prefix transformation (1page proof).
- For reducing the first part of this lemma to the second, let s be a Skolem constant for state variable x.

$\square$

Generalization

Lemma (Generalization)

If $\vdash_{\mathcal{D}} \phi$ is provable without free logical variables, then so are $\vdash_{\mathcal{D}} \forall x\, \phi$ and $\vdash_{\mathcal{D}} \langle x_1 := \theta_1, \dots x_n := \theta_n \rangle \phi$.

Proof Sketch.

- Second part: Induction on the structure of proofs with inductive jump prefix transformation (1page proof).
- For reducing the first part of this lemma to the second, let s be a Skolem constant for state variable x.
- By first proof, derive $\vdash_{\mathcal{D}} \langle x := s \rangle \phi$.

□

Generalization

Lemma (Generalization)

If $\vdash_{\mathcal{D}} \phi$ *is provable without free logical variables, then so are* $\vdash_{\mathcal{D}} \forall x\, \phi$ *and* $\vdash_{\mathcal{D}} \langle x_1 := \theta_1, \dots x_n := \theta_n \rangle \phi$.

Proof Sketch.

- Second part: Induction on the structure of proofs with inductive jump prefix transformation (1page proof).
- For reducing the first part of this lemma to the second, let s be a Skolem constant for state variable x.
- By first proof, derive $\vdash_{\mathcal{D}} \langle x := s \rangle \phi$.
- Using $\forall$r, continue derivation to a proof of $\forall X\, \langle x := X \rangle \phi$, which we abbreviate as $\forall x\, \phi$.

$\square$

Generalization

Lemma (Generalization)

If $\vdash_{\mathcal{D}} \phi$ *is provable without free logical variables, then so are* $\vdash_{\mathcal{D}} \forall x\, \phi$ *and* $\vdash_{\mathcal{D}} \langle x_1 := \theta_1, \ldots x_n := \theta_n \rangle \phi$.

Proof Sketch.

- Second part: Induction on the structure of proofs with inductive jump prefix transformation (1page proof).
- For reducing the first part of this lemma to the second, let s be a Skolem constant for state variable x.
- By first proof, derive $\vdash_{\mathcal{D}} \langle x := s \rangle \phi$.
- Using $\forall$r, continue derivation to a proof of $\forall X\, \langle x := X \rangle \phi$, which we abbreviate as $\forall x\, \phi$.
- Rule $\forall$r is applicable for Skolem constant s as no free logical variables occur in the proof.

□

Relative Completeness on First-Order Safety Assertions

Proposition (Relative completeness of first-order safety)

For every $\alpha \in \mathsf{HP}(\Sigma)$ *and each* $F, G \in \mathsf{Fml}_{\mathsf{FOL}}$

$$\vDash F \rightarrow [\alpha]G \textit{ implies } \vdash_{\mathcal{D}} F \rightarrow [\alpha]G \quad (\textit{thus } F \vdash_{\mathcal{D}} [\alpha]G)$$

Proof (α of the form $x_1 := \theta_1, \dots, x_n := \theta_n$, $?\chi$, $\beta \cup \gamma$, or $\beta;\gamma$).

- This follows from soundness of symmetric rules (equivalent transformations):

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form $x_1 := \theta_1, \dots, x_n := \theta_n$, $?\chi$, $\beta \cup \gamma$, or $\beta;\gamma$).

- This follows from soundness of symmetric rules (equivalent transformations):
- Premiss is valid iff conclusion valid.

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form $x_1 := \theta_1, \ldots, x_n := \theta_n$, $?\chi$, $\beta \cup \gamma$, or $\beta;\gamma$).

- This follows from soundness of symmetric rules (equivalent transformations):
- Premiss is valid iff conclusion valid.
- Premiss is valid and of smaller complexity (HP get simpler), hence derivable by IH.

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form $x_1 := \theta_1, \ldots, x_n := \theta_n$, $?\chi$, $\beta \cup \gamma$, or $\beta; \gamma$).

- This follows from soundness of symmetric rules (equivalent transformations):
- Premiss is valid iff conclusion valid.
- Premiss is valid and of smaller complexity (HP get simpler), hence derivable by IH.
- Thus, we can derive $F \to [\alpha]G$ by applying the respective rule.

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form $x_1 := \theta_1, \ldots, x_n := \theta_n$, $?\chi$, $\beta \cup \gamma$, or $\beta;\gamma$).

- This follows from soundness of symmetric rules (equivalent transformations):
- Premiss is valid iff conclusion valid.
- Premiss is valid and of smaller complexity (HP get simpler), hence derivable by IH.
- Thus, we can derive $F \rightarrow [\alpha]G$ by applying the respective rule.
- $\vDash F \rightarrow [x_1' = f(x_1)_1, \ldots, x_n' = f(x_n)_n]G$ is a FOD-formula and hence derivable as a $\mathcal{D}$ axiom.

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form $\beta;\gamma$).

- $\vDash F \to [\beta;\gamma]G$, which implies $\vDash F \to [\beta][\gamma]G$.

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form $\beta;\gamma$).

- $\vDash F \rightarrow [\beta;\gamma]G$, which implies $\vDash F \rightarrow [\beta][\gamma]G$.
- By Expr, there is a FOD-formula $G^{\#}$ such that $\vDash G^{\#} \leftrightarrow [\gamma]G$.

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form $\beta;\gamma$).

- $\vDash F \rightarrow [\beta;\gamma]G$, which implies $\vDash F \rightarrow [\beta][\gamma]G$.
- By Expr, there is a FOD-formula $G^\#$ such that $\vDash G^\# \leftrightarrow [\gamma]G$.
- From $\vDash F \rightarrow [\beta]G^\#$, IH implies $F \vdash_{\mathcal{D}} [\beta]G^\#$ is derivable.

$\square$

Proof (α of the form $\beta;\gamma$).

- $\vDash F \rightarrow [\beta;\gamma]G$, which implies $\vDash F \rightarrow [\beta][\gamma]G$.
- By Expr, there is a FOD-formula $G^{\#}$ such that $\vDash G^{\#} \leftrightarrow [\gamma]G$.
- From $\vDash F \rightarrow [\beta]G^{\#}$, IH implies $F \vdash_{\mathcal{D}} [\beta]G^{\#}$ is derivable.
- By $\vDash G^{\#} \rightarrow [\gamma]G$, we conclude $\vdash_{\mathcal{D}} G^{\#} \rightarrow [\gamma]G$ by IH.

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form $\beta;\gamma$).

- $\vDash F \to [\beta;\gamma]G$, which implies $\vDash F \to [\beta][\gamma]G$.
- By Expr, there is a FOD-formula $G^\#$ such that $\vDash G^\# \leftrightarrow [\gamma]G$.
- From $\vDash F \to [\beta]G^\#$, IH implies $F \vdash_{\mathcal{D}} [\beta]G^\#$ is derivable.
- By $\vDash G^\# \to [\gamma]G$, we conclude $\vdash_{\mathcal{D}} G^\# \to [\gamma]G$ by IH.
- Using Gen, we conclude $\vdash_{\mathcal{D}} \forall^\beta(G^\# \to [\gamma]G)$.

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form $\beta;\gamma$).

- $\vDash F \rightarrow [\beta;\gamma]G$, which implies $\vDash F \rightarrow [\beta][\gamma]G$.
- By Expr, there is a FOD-formula $G^{\#}$ such that $\vDash G^{\#} \leftrightarrow [\gamma]G$.
- From $\vDash F \rightarrow [\beta]G^{\#}$, IH implies $F \vdash_{\mathcal{D}} [\beta]G^{\#}$ is derivable.
- By $\vDash G^{\#} \rightarrow [\gamma]G$, we conclude $\vdash_{\mathcal{D}} G^{\#} \rightarrow [\gamma]G$ by IH.
- Using Gen, we conclude $\vdash_{\mathcal{D}} \forall^{\beta}(G^{\#} \rightarrow [\gamma]G)$.
- Extends with []gen to $[\beta]G^{\#} \vdash_{\mathcal{D}} [\beta][\gamma]G$.

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form $\beta;\gamma$).

- $\vDash F \rightarrow [\beta;\gamma]G$, which implies $\vDash F \rightarrow [\beta][\gamma]G$.
- By Expr, there is a FOD-formula $G^{\#}$ such that $\vDash G^{\#} \leftrightarrow [\gamma]G$.
- From $\vDash F \rightarrow [\beta]G^{\#}$, IH implies $F \vdash_{\mathcal{D}} [\beta]G^{\#}$ is derivable.
- By $\vDash G^{\#} \rightarrow [\gamma]G$, we conclude $\vdash_{\mathcal{D}} G^{\#} \rightarrow [\gamma]G$ by IH.
- Using Gen, we conclude $\vdash_{\mathcal{D}} \forall^{\beta}(G^{\#} \rightarrow [\gamma]G)$.
- Extends with []gen to $[\beta]G^{\#} \vdash_{\mathcal{D}} [\beta][\gamma]G$.
- Combining propositionally by cut with $[\beta]G^{\#}$, derive $F \vdash_{\mathcal{D}} [\beta][\gamma]G$,

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form $\beta;\gamma$).

- $\vDash F \rightarrow [\beta;\gamma]G$, which implies $\vDash F \rightarrow [\beta][\gamma]G$.
- By Expr, there is a FOD-formula $G^\#$ such that $\vDash G^\# \leftrightarrow [\gamma]G$.
- From $\vDash F \rightarrow [\beta]G^\#$, IH implies $F \vdash_{\mathcal{D}} [\beta]G^\#$ is derivable.
- By $\vDash G^\# \rightarrow [\gamma]G$, we conclude $\vdash_{\mathcal{D}} G^\# \rightarrow [\gamma]G$ by IH.
- Using Gen, we conclude $\vdash_{\mathcal{D}} \forall^\beta(G^\# \rightarrow [\gamma]G)$.
- Extends with []gen to $[\beta]G^\# \vdash_{\mathcal{D}} [\beta][\gamma]G$.
- Combining propositionally by cut with $[\beta]G^\#$, derive $F \vdash_{\mathcal{D}} [\beta][\gamma]G$,
- from which composition $[;]$ yields $F \vdash_{\mathcal{D}} [\beta;\gamma]G$.

$\square$

Proof (α of the form β^*).

- $\vDash F \rightarrow [\beta^*]G$ derivable by invariant induction:

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form β^*).

- $\vDash F \to [\beta^*]G$ derivable by invariant induction:
- Define invariant as FOD representation of $[\beta^*]G$:

$$\phi \equiv ([\beta^*]G)^\# \equiv \forall \vec{v}\,(\mathcal{S}_{\beta^*}(\vec{x},\vec{v}) \to G_{\vec{x}}^{\vec{v}}) \ .$$

$\square$

Proof (α of the form β^*).

- $\vDash F \rightarrow [\beta^*]G$ derivable by invariant induction:
- Define invariant as FOD representation of $[\beta^*]G$:

$$\phi \equiv ([\beta^*]G)^{\#} \equiv \forall \vec{v} \left(\mathcal{S}_{\beta^*}(\vec{x}, \vec{v}) \rightarrow G_{\vec{x}}^{\vec{v}}\right) \ .$$

- $F \rightarrow \phi$ and $\phi \rightarrow G$ are valid FOD-formulas, thus derivable by $\mathcal{D}$

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form β^*).

- $\vDash F \rightarrow [\beta^*]G$ derivable by invariant induction:
- Define invariant as FOD representation of $[\beta^*]G$:

$$\phi \equiv ([\beta^*]G)^\# \equiv \forall \vec{v} \, (\mathcal{S}_{\beta^*}(\vec{x}, \vec{v}) \rightarrow G_{\vec{x}}^{\vec{v}}) \ .$$

- $F \rightarrow \phi$ and $\phi \rightarrow G$ are valid FOD-formulas, thus derivable by $\mathcal{D}$
- Hence $F \vdash_{\mathcal{D}} \phi$ derivable by lemma.

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form β^*).

- $\vDash F \to [\beta^*]G$ derivable by invariant induction:
- Define invariant as FOD representation of $[\beta^*]G$:

$$\phi \equiv ([\beta^*]G)^{\#} \equiv \forall \vec{v}\, (\mathcal{S}_{\beta^*}(\vec{x}, \vec{v}) \to G_{\vec{x}}^{\vec{v}}) \ .$$

- $F \to \phi$ and $\phi \to G$ are valid FOD-formulas, thus derivable by $\mathcal{D}$
- Hence $F \vdash_{\mathcal{D}} \phi$ derivable by lemma.
- By Gen and []gen, $[\beta^*]\phi \vdash_{\mathcal{D}} [\beta^*]G$ is derivable.

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form β^*).

- $\vDash F \to [\beta^*]G$ derivable by invariant induction:
- Define invariant as FOD representation of $[\beta^*]G$:

$$\phi \equiv ([\beta^*]G)^{\#} \equiv \forall \vec{v}\, (\mathcal{S}_{\beta^*}(\vec{x}, \vec{v}) \to G_{\vec{x}}^{\vec{v}})\ .$$

- $F \to \phi$ and $\phi \to G$ are valid FOD-formulas, thus derivable by $\mathcal{D}$
- Hence $F \vdash_{\mathcal{D}} \phi$ derivable by lemma.
- By Gen and []gen, $[\beta^*]\phi \vdash_{\mathcal{D}} [\beta^*]G$ is derivable.
- Likewise, $\phi \to [\beta]\phi$ valid according to semantics of repetition, thus derivable by IH, since β less complex.

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form β^*).

- $\vDash F \to [\beta^*]G$ derivable by invariant induction:
- Define invariant as FOD representation of $[\beta^*]G$:

$$\phi \equiv ([\beta^*]G)^\# \equiv \forall \vec{v}\, (\mathcal{S}_{\beta^*}(\vec{x}, \vec{v}) \to G_{\vec{x}}^{\vec{v}}) \ .$$

- $F \to \phi$ and $\phi \to G$ are valid FOD-formulas, thus derivable by $\mathcal{D}$
- Hence $F \vdash_{\mathcal{D}} \phi$ derivable by lemma.
- By Gen and []gen, $[\beta^*]\phi \vdash_{\mathcal{D}} [\beta^*]G$ is derivable.
- Likewise, $\phi \to [\beta]\phi$ valid according to semantics of repetition, thus derivable by IH, since β less complex.
- By Gen, derive $\vdash_{\mathcal{D}} \forall^\beta(\phi \to [\beta]\phi)$, from which ind yields $\phi \vdash_{\mathcal{D}} [\beta^*]\phi$.

$\square$

Relative Completeness on First-Order Safety Assertions

Proof (α of the form β^*).

- $\vDash F \rightarrow [\beta^*]G$ derivable by invariant induction:
- Define invariant as FOD representation of $[\beta^*]G$:

$$\phi \equiv ([\beta^*]G)^\# \equiv \forall \vec{v}\,(\mathcal{S}_{\beta^*}(\vec{x}, \vec{v}) \rightarrow G_{\vec{x}}^{\vec{v}}) \ .$$

- $F \rightarrow \phi$ and $\phi \rightarrow G$ are valid FOD-formulas, thus derivable by $\mathcal{D}$
- Hence $F \vdash_{\mathcal{D}} \phi$ derivable by lemma.
- By Gen and []gen, $[\beta^*]\phi \vdash_{\mathcal{D}} [\beta^*]G$ is derivable.
- Likewise, $\phi \rightarrow [\beta]\phi$ valid according to semantics of repetition, thus derivable by IH, since β less complex.
- By Gen, derive $\vdash_{\mathcal{D}} \forall^\beta(\phi \rightarrow [\beta]\phi)$, from which ind yields $\phi \vdash_{\mathcal{D}} [\beta^*]\phi$.
- Combining propositionally by cut with $[\beta^*]\phi$ and ϕ yields $F \vdash_{\mathcal{D}} [\beta^*]G$.

$\square$

Relative Completeness of First-Order Liveness Assertions

Proposition (Relative completeness of first-order liveness)

For every $\alpha \in \mathrm{HP}(\Sigma)$ *and each* $F, G \in \mathrm{Fml}_{\mathrm{FOL}}$

$$\vDash F \rightarrow \langle\alpha\rangle G \text{ implies } \vdash_{\mathcal{D}} F \rightarrow \langle\alpha\rangle G \quad (\text{thus } F \vdash_{\mathcal{D}} \langle\alpha\rangle G) .$$

Relative Completeness of First-Order Liveness Assertions

Proof (α of the form β^*).

- $\vDash F \rightarrow \langle \beta^* \rangle G$ derivable by variant convergence:

Proof (α of the form β^*).

- $\vDash F \to \langle \beta^* \rangle G$ derivable by variant convergence:
- Define FOD-formula $\varphi(n)$ expressing that, after n iterations, β can lead to a state satisfying G, essentially $(\langle \beta^* \rangle G)^{\#}$:

  $\exists \vec{v}\, \exists Z \left(Z_1^{(n)} = \vec{x} \wedge Z_n^{(n)} = \vec{v} \wedge \forall i : \mathbb{N}\ (1 \leq i < n \to \mathcal{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)})) \wedge G_{\vec{x}}^{\vec{v}} \right)$

Proof (α of the form β^*).

- $\vDash F \rightarrow \langle \beta^* \rangle G$ derivable by variant convergence:
- Define FOD-formula $\varphi(n)$ expressing that, after n iterations, β can lead to a state satisfying G, essentially $(\langle \beta^* \rangle G)^\#$:

  $\exists \vec{v} \, \exists Z \, \big(Z_1^{(n)} = \vec{x} \wedge Z_n^{(n)} = \vec{v} \wedge \forall i : \mathbb{N} \, (1 \leq i < n \rightarrow \mathcal{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)})) \wedge G_{\vec{x}}^{\vec{v}} \big)$
- $\varphi(n)$ can only hold true if n is a natural number.

Proof (α of the form β^*).

- $\vDash F \to \langle \beta^* \rangle G$ derivable by variant convergence:
- Define FOD-formula $\varphi(n)$ expressing that, after n iterations, β can lead to a state satisfying G, essentially $(\langle \beta^* \rangle G)^{\#}$:

$$\exists \vec{v}\, \exists Z\, \left(Z_1^{(n)} = \vec{x} \wedge Z_n^{(n)} = \vec{v} \wedge \forall i : \mathbb{N}\, (1 \leq i < n \to \mathcal{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)})) \wedge G_{\vec{x}}^{\vec{v}} \right)$$

- $\varphi(n)$ can only hold true if n is a natural number.
- According to loop semantics, $\vDash n > 0 \wedge \varphi(n) \to \langle \beta \rangle \varphi(n-1)$ valid:

Proof (α of the form β^*).

- $\vDash F \to \langle\beta^*\rangle G$ derivable by variant convergence:
- Define FOD-formula $\varphi(n)$ expressing that, after n iterations, β can lead to a state satisfying G, essentially $(\langle\beta^*\rangle G)^\#$:

  $$\exists \vec{v}\, \exists Z\, \left(Z_1^{(n)} = \vec{x} \land Z_n^{(n)} = \vec{v} \land \forall i : \mathbb{N}\, (1 \le i < n \to \mathcal{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)})) \land G_{\vec{x}}^{\vec{v}}\right)$$
- $\varphi(n)$ can only hold true if n is a natural number.
- According to loop semantics, $\vDash n > 0 \land \varphi(n) \to \langle\beta\rangle\varphi(n-1)$ valid:
- If $n > 0$ is natural number then so is $n - 1$. If β reaches G after n repetitions, then, after executing β, $n - 1$ repetitions of β reach G.

Relative Completeness of First-Order Liveness Assertions

Proof (α of the form β^*).

- $\vDash F \rightarrow \langle\beta^*\rangle G$ derivable by variant convergence:
- Define FOD-formula $\varphi(n)$ expressing that, after n iterations, β can lead to a state satisfying G, essentially $(\langle\beta^*\rangle G)^\#$:

  $$\exists\vec{v}\,\exists Z\,\left(Z_1^{(n)} = \vec{x} \wedge Z_n^{(n)} = \vec{v} \wedge \forall i : \mathbb{N}\,(1 \leq i < n \rightarrow \mathcal{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)})) \wedge G_{\vec{x}}^{\vec{v}}\right)$$

- $\varphi(n)$ can only hold true if n is a natural number.
- According to loop semantics, $\vDash n > 0 \wedge \varphi(n) \rightarrow \langle\beta\rangle\varphi(n-1)$ valid:
- If $n > 0$ is natural number then so is $n-1$. If β reaches G after n repetitions, then, after executing β, $n-1$ repetitions of β reach G.
- By IH, this formula is derivable, since β contains less loops.

Relative Completeness of First-Order Liveness Assertions

Proof (α of the form β^*).

- $\vDash F \rightarrow \langle\beta^*\rangle G$ derivable by variant convergence:
- Define FOD-formula $\varphi(n)$ expressing that, after n iterations, β can lead to a state satisfying G, essentially $(\langle\beta^*\rangle G)^\#$:

  $$\exists \vec{v}\, \exists Z \left(Z_1^{(n)} = \vec{x} \wedge Z_n^{(n)} = \vec{v} \wedge \forall i : \mathbb{N}\ (1 \leq i < n \rightarrow \mathcal{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)})) \wedge G_{\vec{x}}^{\vec{v}}\right)$$
- $\varphi(n)$ can only hold true if n is a natural number.
- According to loop semantics, $\vDash n > 0 \wedge \varphi(n) \rightarrow \langle\beta\rangle\varphi(n-1)$ valid:
- If $n > 0$ is natural number then so is $n - 1$. If β reaches G after n repetitions, then, after executing β, $n - 1$ repetitions of β reach G.
- By IH, this formula is derivable, since β contains less loops.
- By Gen, extends to $\vdash_{\mathcal{D}} \forall^\beta \forall n{>}0\, (\varphi(n) \rightarrow \langle\beta\rangle\varphi(n-1))$.

Relative Completeness of First-Order Liveness Assertions

Proof (α of the form β^*).

- $\vDash F \to \langle\beta^*\rangle G$ derivable by variant convergence:
- Define FOD-formula $\varphi(n)$ expressing that, after n iterations, β can lead to a state satisfying G, essentially $(\langle\beta^*\rangle G)^\#$:

  $\exists\vec{v}\,\exists Z\,\big(Z_1^{(n)} = \vec{x} \wedge Z_n^{(n)} = \vec{v} \wedge \forall i : \mathbb{N}\,(1 \le i < n \to \mathcal{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)})) \wedge G_{\vec{x}}^{\vec{v}}\big)$
- $\varphi(n)$ can only hold true if n is a natural number.
- According to loop semantics, $\vDash n > 0 \wedge \varphi(n) \to \langle\beta\rangle\varphi(n-1)$ valid:
- If $n > 0$ is natural number then so is $n-1$. If β reaches G after n repetitions, then, after executing β, $n-1$ repetitions of β reach G.
- By IH, this formula is derivable, since β contains less loops.
- By Gen, extends to $\vdash_{\mathcal{D}} \forall^\beta \forall n{>}0\,(\varphi(n) \to \langle\beta\rangle\varphi(n-1))$.
- Thus $\exists v\,\varphi(v) \vdash_{\mathcal{D}} \langle\beta^*\rangle\exists v{\le}0\,\varphi(v)$ by convergence con.

Proof (α of the form β^*).

- $\vDash F \to \langle\beta^*\rangle G$ derivable by variant convergence:
-

$$\exists\vec{v}\,\exists Z\,\left(Z_1^{(n)} = \vec{x} \wedge Z_n^{(n)} = \vec{v} \wedge \forall i : \mathbb{N}\,(1 \leq i < n \to \mathcal{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)})) \wedge G_{\vec{x}}^{\vec{v}}\right)$$

- Thus $\exists v\,\varphi(v) \vdash_{\mathcal{D}} \langle\beta^*\rangle\exists v{\leq}0\,\varphi(v)$ by convergence con.
- From assumption, conclude valid FOD-formulas, hence $\mathcal{D}$-axioms:

Relative Completeness of First-Order Liveness Assertions

Proof (α of the form β^*).

- $\vDash F \to \langle\beta^*\rangle G$ derivable by variant convergence:
- $$\exists\vec{v}\,\exists Z\,\left(Z_1^{(n)} = \vec{x} \land Z_n^{(n)} = \vec{v} \land \forall i : \mathbb{N}\,(1 \le i < n \to \mathcal{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)})) \land G_{\vec{x}}^{\vec{v}}\right)$$
- Thus $\exists v\,\varphi(v) \vdash_{\mathcal{D}} \langle\beta^*\rangle \exists v{\le}0\,\varphi(v)$ by convergence con.
- From assumption, conclude valid FOD-formulas, hence $\mathcal{D}$-axioms:
  - $\vDash F \to \exists v\,\varphi(v)$, because $\vDash F \to \langle\beta^*\rangle G$

Proof (α of the form β^*).

- $\vDash F \rightarrow \langle\beta^*\rangle G$ derivable by variant convergence:
- $$\exists\vec{v}\,\exists Z\,\left(Z_1^{(n)} = \vec{x} \wedge Z_n^{(n)} = \vec{v} \wedge \forall i : \mathbb{N}\,(1 \leq i < n \rightarrow \mathcal{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)})) \wedge G_{\vec{x}}^{\vec{v}}\right)$$
- Thus $\exists v\,\varphi(v) \vdash_{\mathcal{D}} \langle\beta^*\rangle\exists v{\leq}0\,\varphi(v)$ by convergence con.
- From assumption, conclude valid FOD-formulas, hence $\mathcal{D}$-axioms:
  - $\vDash F \rightarrow \exists v\,\varphi(v)$, because $\vDash F \rightarrow \langle\beta^*\rangle G$
  - $\vDash (\exists v{\leq}0\,\varphi(v)) \rightarrow G$, because $v{\leq}0$ and the fact, that, by Gödel, $\varphi(v)$ only holds true for natural numbers, imply $\varphi(0)$. Further, $\varphi(0)$ entails G, because zero repetitions of β have no effect.

Relative Completeness of First-Order Liveness Assertions

Proof (α of the form β^*).

- $\vDash F \to \langle\beta^*\rangle G$ derivable by variant convergence:
- $$\exists\vec{v}\,\exists Z\,\left(Z_1^{(n)} = \vec{x} \land Z_n^{(n)} = \vec{v} \land \forall i\,{:}\,\mathbb{N}\,(1 \le i < n \to \mathcal{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)})) \land G_{\vec{x}}^{\vec{v}}\right)$$
- Thus $\exists v\,\varphi(v) \vdash_{\mathcal{D}} \langle\beta^*\rangle\exists v{\le}0\,\varphi(v)$ by convergence con.
- From assumption, conclude valid FOD-formulas, hence $\mathcal{D}$-axioms:
  - $\vDash F \to \exists v\,\varphi(v)$, because $\vDash F \to \langle\beta^*\rangle G$
  - $\vDash (\exists v{\le}0\,\varphi(v)) \to G$, because $v{\le}0$ and the fact, that, by Gödel, $\varphi(v)$ only holds true for natural numbers, imply $\varphi(0)$. Further, $\varphi(0)$ entails G, because zero repetitions of β have no effect.
- Derive $\vdash_{\mathcal{D}} \forall^\beta(\exists v{\le}0\,\varphi(v) \to G)$ by Gen

Proof (α of the form β^*).

- $\vDash F \rightarrow \langle\beta^*\rangle G$ derivable by variant convergence:
- $$\exists\vec{v}\,\exists Z\,\left(Z_1^{(n)} = \vec{x} \land Z_n^{(n)} = \vec{v} \land \forall i : \mathbb{N}\,(1 \le i < n \rightarrow \mathcal{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)})) \land G_{\vec{x}}^{\vec{v}}\right)$$
- Thus $\exists v\,\varphi(v) \vdash_{\mathcal{D}} \langle\beta^*\rangle\exists v{\le}0\,\varphi(v)$ by convergence con.
- From assumption, conclude valid FOD-formulas, hence $\mathcal{D}$-axioms:
  - $\vDash F \rightarrow \exists v\,\varphi(v)$, because $\vDash F \rightarrow \langle\beta^*\rangle G$
  - $\vDash (\exists v{\le}0\,\varphi(v)) \rightarrow G$, because $v{\le}0$ and the fact, that, by Gödel, $\varphi(v)$ only holds true for natural numbers, imply $\varphi(0)$. Further, $\varphi(0)$ entails G, because zero repetitions of β have no effect.
- Derive $\vdash_{\mathcal{D}} \forall^\beta(\exists v{\le}0\,\varphi(v) \rightarrow G)$ by Gen
- Extend to $\langle\beta^*\rangle\exists v{\le}0\,\varphi(v) \vdash_{\mathcal{D}} \langle\beta^*\rangle G$ by $\langle\rangle$gen.

Proof (α of the form β^*).

- $\vDash F \to \langle\beta^*\rangle G$ derivable by variant convergence:
-

$$\exists \vec{v}\, \exists Z\, \left(Z_1^{(n)} = \vec{x} \land Z_n^{(n)} = \vec{v} \land \forall i : \mathbb{N}\, (1 \le i < n \to \mathcal{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)})) \land G_{\vec{x}}^{\vec{v}}\right)$$

- Thus $\exists v\, \varphi(v) \vdash_{\mathcal{D}} \langle\beta^*\rangle \exists v{\le}0\, \varphi(v)$ by convergence con.
- From assumption, conclude valid FOD-formulas, hence $\mathcal{D}$-axioms:
  - $\vDash F \to \exists v\, \varphi(v)$, because $\vDash F \to \langle\beta^*\rangle G$
  - $\vDash (\exists v{\le}0\, \varphi(v)) \to G$, because $v{\le}0$ and the fact, that, by Gödel, $\varphi(v)$ only holds true for natural numbers, imply $\varphi(0)$. Further, $\varphi(0)$ entails G, because zero repetitions of β have no effect.
- Derive $\vdash_{\mathcal{D}} \forall^\beta(\exists v{\le}0\, \varphi(v) \to G)$ by Gen
- Extend to $\langle\beta^*\rangle \exists v{\le}0\, \varphi(v) \vdash_{\mathcal{D}} \langle\beta^*\rangle G$ by $\langle\rangle$gen.
- From $\vdash_{\mathcal{D}} F \to \exists v\, \varphi(v)$ conclude $F \vdash_{\mathcal{D}} \exists v\, \varphi(v)$.

Relative Completeness of First-Order Liveness Assertions

Proof (α of the form β^*).

- $\vDash F \to \langle\beta^*\rangle G$ derivable by variant convergence:
- $$\exists\vec{v}\,\exists Z\,\left(Z_1^{(n)} = \vec{x} \land Z_n^{(n)} = \vec{v} \land \forall i : \mathbb{N}\,(1 \le i < n \to \mathcal{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)})) \land G_{\vec{x}}^{\vec{v}}\right)$$
- Thus $\exists v\,\varphi(v) \vdash_{\mathcal{D}} \langle\beta^*\rangle\exists v{\le}0\,\varphi(v)$ by convergence con.
- From assumption, conclude valid FOD-formulas, hence $\mathcal{D}$-axioms:
  - $\vDash F \to \exists v\,\varphi(v)$, because $\vDash F \to \langle\beta^*\rangle G$
  - $\vDash (\exists v{\le}0\,\varphi(v)) \to G$, because $v{\le}0$ and the fact, that, by Gödel, $\varphi(v)$ only holds true for natural numbers, imply $\varphi(0)$. Further, $\varphi(0)$ entails G, because zero repetitions of β have no effect.
- Derive $\vdash_{\mathcal{D}} \forall^\beta(\exists v{\le}0\,\varphi(v) \to G)$ by Gen
- Extend to $\langle\beta^*\rangle\exists v{\le}0\,\varphi(v) \vdash_{\mathcal{D}} \langle\beta^*\rangle G$ by $\langle\rangle$gen.
- From $\vdash_{\mathcal{D}} F \to \exists v\,\varphi(v)$ conclude $F \vdash_{\mathcal{D}} \exists v\,\varphi(v)$.
- Combine propositionally by a cut to $F \vdash_{\mathcal{D}} \langle\beta^*\rangle G$.

Relative Completeness of Differential Logic Calculus

Theorem (Relative Completeness)

d$\mathcal{L}$ *calculus is complete relative to first-order logic of differential equations.*

$$\vDash \phi \quad \textit{iff} \quad Taut_{FOD} \vdash \phi$$

$$\textit{where} \quad FOD = FOL_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$$

Relative Completeness of Differential Logic Calculus

Proof Idea.

- By propositional recombination, inductively identify fragments of ϕ that correspond to $\phi_1 \to [\alpha]\phi_2$ or $\phi_1 \to \langle\alpha\rangle\phi_2$ logically.

$\square$

Relative Completeness of Differential Logic Calculus

Proof Idea.

- By propositional recombination, inductively identify fragments of ϕ that correspond to $\phi_1 \to [\alpha]\phi_2$ or $\phi_1 \to \langle\alpha\rangle\phi_2$ logically.
- Express subformulas ϕ_i equivalently in FOD and resolve these first-order safety or liveness assertions by previous propositions.

$\square$

Proof Idea.

- By propositional recombination, inductively identify fragments of ϕ that correspond to $\phi_1 \rightarrow [\alpha]\phi_2$ or $\phi_1 \rightarrow \langle\alpha\rangle\phi_2$ logically.
- Express subformulas ϕ_i equivalently in FOD and resolve these first-order safety or liveness assertions by previous propositions.
- Finally, prove that the original d$\mathcal{L}$ formula can be re-derived from the subproofs.

$\square$

Proof Idea.

- Assume ϕ to be given in conjunctive normal form by appropriate propositional reasoning:

Proof Idea.

- Assume ϕ to be given in conjunctive normal form by appropriate propositional reasoning:
- Push negations inside over modalities using dualities

$$\neg[\alpha]\phi \equiv \langle\alpha\rangle\neg\phi$$
$$\neg\langle\alpha\rangle\phi \equiv [\alpha]\neg\phi$$

Relative Completeness of Differential Logic Calculus

Proof Idea.

- Assume ϕ to be given in conjunctive normal form by appropriate propositional reasoning:
- Push negations inside over modalities using dualities

$$\neg[\alpha]\phi \equiv \langle\alpha\rangle\neg\phi$$
$$\neg\langle\alpha\rangle\phi \equiv [\alpha]\neg\phi$$

- Remainder of proof follows induction on a measure $|\phi|$ defined as the number of modalities in ϕ.

Proof Idea.

- Assume ϕ to be given in conjunctive normal form by appropriate propositional reasoning:
- Push negations inside over modalities using dualities

$$\neg[\alpha]\phi \equiv \langle\alpha\rangle\neg\phi$$
$$\neg\langle\alpha\rangle\phi \equiv [\alpha]\neg\phi$$

- Remainder of proof follows induction on a measure $|\phi|$ defined as the number of modalities in ϕ.
- For a simple and uniform proof, assume quantifiers to be abbreviations for modal formulas:

$$\exists x\,\phi \equiv \langle x' = 1\rangle\phi \vee \langle x' = -1\rangle\phi$$
$$\forall x\,\phi \equiv [x' = 1]\phi \wedge [x' = -1]\phi$$

Proof.

- $|\phi| = 0$ then ϕ is a first-order formula, hence derivable by $\mathcal{D}$.

Proof.

- $|\phi| = 0$ then ϕ is a first-order formula, hence derivable by $\mathcal{D}$.
- ϕ is of the form $\neg\phi_1$, then ϕ_1 is first-order by NNF, hence $|\phi| = 0$.

Relative Completeness of Differential Logic Calculus

Proof.

- $|\phi| = 0$ then ϕ is a first-order formula, hence derivable by $\mathcal{D}$.
- ϕ is of the form $\neg\phi_1$, then ϕ_1 is first-order by NNF, hence $|\phi| = 0$.
- ϕ is of the form $\phi_1 \wedge \phi_2$, then individually deduce the simpler proofs for $\vdash_{\mathcal{D}} \phi_1$ and $\vdash_{\mathcal{D}} \phi_2$ by IH, which can be combined by $\wedge$r.

Proof.

- $|\phi| = 0$ then ϕ is a first-order formula, hence derivable by $\mathcal{D}$.
- ϕ is of the form $\neg\phi_1$, then ϕ_1 is first-order by NNF, hence $|\phi| = 0$.
- ϕ is of the form $\phi_1 \land \phi_2$, then individually deduce the simpler proofs for $\vdash_{\mathcal{D}} \phi_1$ and $\vdash_{\mathcal{D}} \phi_2$ by IH, which can be combined by $\land$r.
- ϕ disjunction, hence (otherwise use associativity and commutativity):

$$\begin{array}{ccc} \phi_1 & \lor & [\alpha]\phi_2 \\ \phi_1 & \lor & \langle\alpha\rangle\phi_2 \end{array}$$

Proof.

- Unified notation: $\phi_1 \lor \langle\![\alpha]\!\rangle\phi_2$.

Relative Completeness of Differential Logic Calculus

Proof.

- Unified notation: $\phi_1 \vee \langle\![\alpha]\!\rangle \phi_2$.
- Then, $|\phi_2| < |\phi|$, since ϕ_2 has less modalities.

Proof.

- Unified notation: $\phi_1 \vee \langle\![\alpha]\!\rangle\phi_2$.
- Then, $|\phi_2| < |\phi|$, since ϕ_2 has less modalities.
- $|\phi_1| < |\phi|$ as $\langle\![\alpha]\!\rangle\phi_2$ contributes one modality to $|\phi|$ that is not in ϕ_1.

Proof.

- Unified notation: $\phi_1 \vee \langle\![\alpha]\!\rangle \phi_2$.
- Then, $|\phi_2| < |\phi|$, since ϕ_2 has less modalities.
- $|\phi_1| < |\phi|$ as $\langle\![\alpha]\!\rangle \phi_2$ contributes one modality to $|\phi|$ that is not in ϕ_1.
- There are equivalent FOD-formulas $\phi_1^{\#}, \phi_2^{\#}$ with $\vDash \phi_i \leftrightarrow \phi_i^{\#}$.

Relative Completeness of Differential Logic Calculus

Proof.

- Unified notation: $\phi_1 \lor \langle\![\alpha]\!\rangle\phi_2$.
- Then, $|\phi_2| < |\phi|$, since ϕ_2 has less modalities.
- $|\phi_1| < |\phi|$ as $\langle\![\alpha]\!\rangle\phi_2$ contributes one modality to $|\phi|$ that is not in ϕ_1.
- There are equivalent FOD-formulas $\phi_1^\#, \phi_2^\#$ with $\vDash \phi_i \leftrightarrow \phi_i^\#$.
- By congruence, $\vDash \phi$ yields $\vDash \phi_1^\# \lor \langle\![\alpha]\!\rangle\phi_2^\#$, thus $\vDash \neg\phi_1^\# \to \langle\![\alpha]\!\rangle\phi_2^\#$.

Relative Completeness of Differential Logic Calculus

Proof.

- Unified notation: $\phi_1 \vee \langle\!\![\alpha]\!\!\rangle \phi_2$.
- Then, $|\phi_2| < |\phi|$, since ϕ_2 has less modalities.
- $|\phi_1| < |\phi|$ as $\langle\!\![\alpha]\!\!\rangle \phi_2$ contributes one modality to $|\phi|$ that is not in ϕ_1.
- There are equivalent FOD-formulas $\phi_1^\#, \phi_2^\#$ with $\vDash \phi_i \leftrightarrow \phi_i^\#$.
- By congruence, $\vDash \phi$ yields $\vDash \phi_1^\# \vee \langle\!\![\alpha]\!\!\rangle \phi_2^\#$, thus $\vDash \neg\phi_1^\# \rightarrow \langle\!\![\alpha]\!\!\rangle \phi_2^\#$.
- By previous propositions derive

$$\neg\phi_1^\# \vdash_{\mathcal{D}} \langle\!\![\alpha]\!\!\rangle \phi_2^\# \tag{1}$$

Proof.

- Unified notation: $\phi_1 \lor \langle\![\alpha]\!\rangle\phi_2$.
- Then, $|\phi_2| < |\phi|$, since ϕ_2 has less modalities.
- $|\phi_1| < |\phi|$ as $\langle\![\alpha]\!\rangle\phi_2$ contributes one modality to $|\phi|$ that is not in ϕ_1.
- There are equivalent FOD-formulas $\phi_1^\#, \phi_2^\#$ with $\vDash \phi_i \leftrightarrow \phi_i^\#$.
- By congruence, $\vDash \phi$ yields $\vDash \phi_1^\# \lor \langle\![\alpha]\!\rangle\phi_2^\#$, thus $\vDash \neg\phi_1^\# \to \langle\![\alpha]\!\rangle\phi_2^\#$.
- By previous propositions derive

$$\neg\phi_1^\# \vdash_{\mathcal{D}} \langle\![\alpha]\!\rangle\phi_2^\# \tag{1}$$

- $\vDash \phi_1 \leftrightarrow \phi_1^\#$ implies $\vDash \neg\phi_1 \to \neg\phi_1^\#$, which is derivable by IH, because $|\phi_1| < |\phi|$. By lemma, $\neg\phi_1 \vdash_{\mathcal{D}} \neg\phi_1^\#$, which we combine with (1) by a cut with $\neg\phi_1^\#$ to

$$\neg\phi_1 \vdash_{\mathcal{D}} \langle\![\alpha]\!\rangle\phi_2^\# \quad . \tag{2}$$

Proof.

- $\vDash \phi_2 \leftrightarrow \phi_2^{\#}$ implies $\vDash \phi_2^{\#} \to \phi_2$, which is derivable by IH, as $|\phi_2| < |\phi|$.

$\square$

Relative Completeness of Differential Logic Calculus

Proof.

- $\vDash \phi_2 \leftrightarrow \phi_2^{\#}$ implies $\vDash \phi_2^{\#} \to \phi_2$, which is derivable by IH, as $|\phi_2| < |\phi|$.
- Extend derivation of $\vdash_{\mathcal{D}} \phi_2^{\#} \to \phi_2$ to one of $\vdash_{\mathcal{D}} \forall^{\alpha}(\phi_2^{\#} \to \phi_2)$ by Gen

$\square$

Relative Completeness of Differential Logic Calculus

Proof.

- $\vDash \phi_2 \leftrightarrow \phi_2^\#$ implies $\vDash \phi_2^\# \to \phi_2$, which is derivable by IH, as $|\phi_2| < |\phi|$.
- Extend derivation of $\vdash_{\mathcal{D}} \phi_2^\# \to \phi_2$ to one of $\vdash_{\mathcal{D}} \forall^\alpha(\phi_2^\# \to \phi_2)$ by Gen
- Thus $\langle\!\![\alpha]\!\!\rangle\phi_2^\# \vdash_{\mathcal{D}} \langle\!\![\alpha]\!\!\rangle\phi_2$ by []gen or ⟨⟩gen.

$\square$

Proof.

- $\vDash \phi_2 \leftrightarrow \phi_2^{\#}$ implies $\vDash \phi_2^{\#} \to \phi_2$, which is derivable by IH, as $|\phi_2| < |\phi|$.
- Extend derivation of $\vdash_{\mathcal{D}} \phi_2^{\#} \to \phi_2$ to one of $\vdash_{\mathcal{D}} \forall^{\alpha}(\phi_2^{\#} \to \phi_2)$ by Gen
- Thus $\langle\!\![\alpha]\!\!\rangle\phi_2^{\#} \vdash_{\mathcal{D}} \langle\!\![\alpha]\!\!\rangle\phi_2$ by []gen or $\langle\rangle$gen.
- Combine propositionally with (2) by a cut with $\langle\!\![\alpha]\!\!\rangle\phi_2^{\#}$ to derive $\neg\phi_1 \vdash_{\mathcal{D}} \langle\!\![\alpha]\!\!\rangle\phi_2$

$\square$

Relative Completeness of Differential Logic Calculus

Proof.

- $\vDash \phi_2 \leftrightarrow \phi_2^\#$ implies $\vDash \phi_2^\# \rightarrow \phi_2$, which is derivable by IH, as $|\phi_2| < |\phi|$.
- Extend derivation of $\vdash_{\mathcal{D}} \phi_2^\# \rightarrow \phi_2$ to one of $\vdash_{\mathcal{D}} \forall^\alpha(\phi_2^\# \rightarrow \phi_2)$ by Gen
- Thus $⟨\![\alpha]\!⟩\phi_2^\# \vdash_{\mathcal{D}} ⟨\![\alpha]\!⟩\phi_2$ by []gen or $\langle\rangle$gen.
- Combine propositionally with (2) by a cut with $⟨\![\alpha]\!⟩\phi_2^\#$ to derive $\neg\phi_1 \vdash_{\mathcal{D}} ⟨\![\alpha]\!⟩\phi_2$
- Conclude $\vdash_{\mathcal{D}} \phi_1 \vee ⟨\![\alpha]\!⟩\phi_2$ with a cut.

$\square$

Relative Completeness

Theorem (Relative Completeness)

d$\mathcal{L}$ *calculus is a sound & complete axiomatisation of hybrid systems relative to differential equations.*

▸ Proof Outline 15p

continuous discrete repeat

$\Downarrow$

Relativity

Cook,Harel:	discrete-DL/data	P.:	hybrid-d$\mathcal{L}$/differential equations