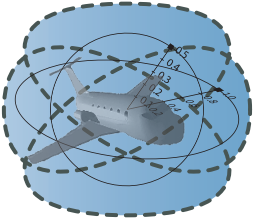
15-819/18-879: Hybrid Systems Analysis & Theorem Proving

10: Completeness 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

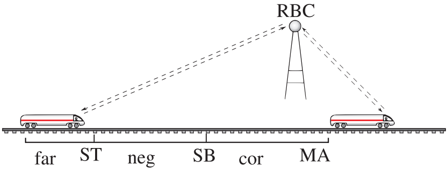
2. Soundness

3. Completeness
   - Incompleteness
   - Completeness

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

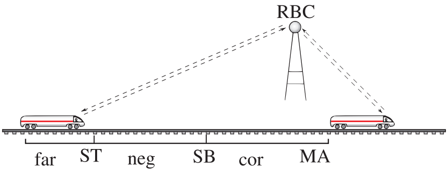
differential dynamic logic

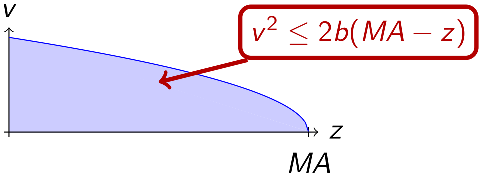
$$\mathrm{d}\mathcal{L} = \quad \mathrm{DL} + \mathrm{HP}$$



differential dynamic logic

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

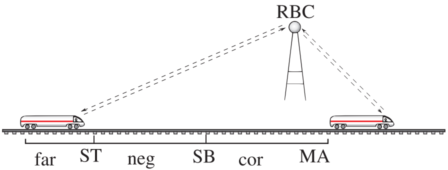




$\mathcal{R}$ d$\mathcal{L}$ Motives: Regions in First-order Logic

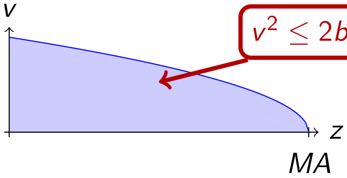
differential dynamic logic

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



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

$\forall t \geq 0 \ \ldots$

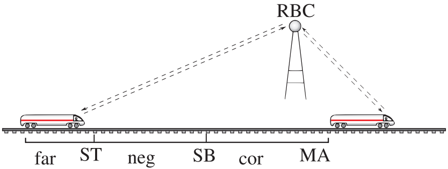


$\boxed{v^2 \leq 2b(MA - z)}$

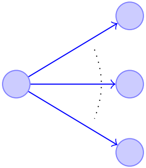
d$\mathcal{L}$ Motives: State Transitions in Dynamic Logic

differential dynamic logic

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

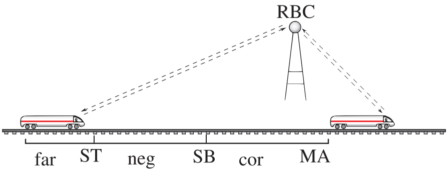


$v^2 \leq 2b$

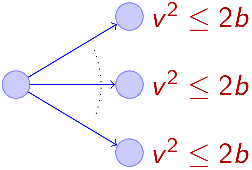


differential dynamic logic

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

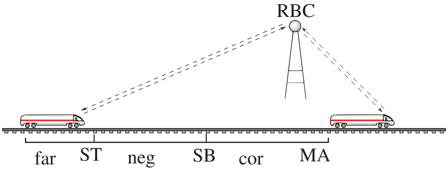


$\square\, v^2 \leq 2b$

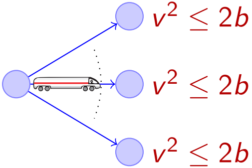


differential dynamic logic

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



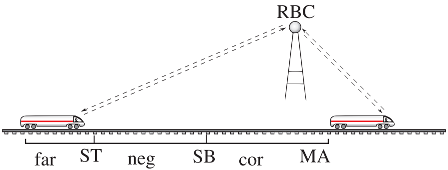
[] $v^2 \leq 2b$



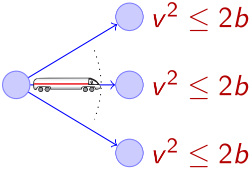
d$\mathcal{L}$ Motives: Hybrid Programs as Uniform Model

differential dynamic logic

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



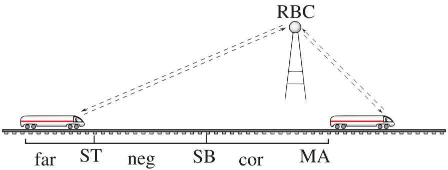
$[z'' = a]\, v^2 \leq 2b$



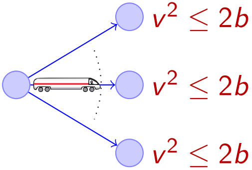
dℒ Motives: Hybrid Programs as Uniform Model

differential dynamic logic

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



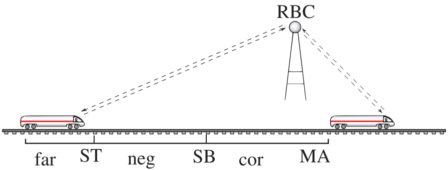
$[\mathtt{if}(z > SB)\, a := -b;\ z'' = a]\, v^2 \leq 2b$



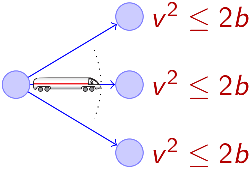
$\mathcal{R}$ d$\mathcal{L}$ Motives: Hybrid Programs as Uniform Model

differential dynamic logic

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



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



10 propositional rules

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

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

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

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

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

$$\frac{\langle\alpha\rangle\phi \vee \langle\beta\rangle\phi}{\langle\alpha\cup\beta\rangle\phi} \qquad \frac{\chi \wedge \psi}{\langle ?\chi\rangle\psi} \qquad \frac{\exists t{\ge}0\, \big((\forall 0{\le}\tilde{t}{\le}t\, \langle\mathcal{S}(\tilde{t})\rangle\chi) \wedge \langle\mathcal{S}(t)\rangle\phi\big)}{\langle x_1' = \theta_1, .., x_n' = \theta_n \wedge \chi\rangle\phi}$$

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

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

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

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

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

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

X new variable

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

X new variable

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

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

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.,*

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

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

$\mathcal{R}$ 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

Completeness

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

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 (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)

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

Incompleteness

Proof (Incompleteness).

Discrete fragment:

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

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

□

Incompleteness

Proof (Incompleteness).

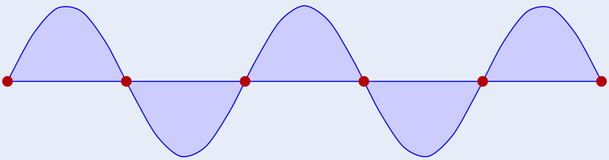
Discrete fragment:

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

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

Continuous fragment:

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



□

Incompleteness

Proof (Incompleteness).

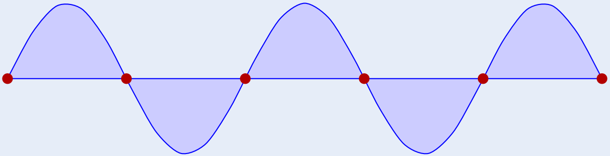
Discrete fragment:

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

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

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).

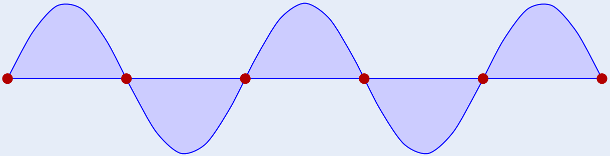
Discrete fragment:

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

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

Continuous fragment:

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



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

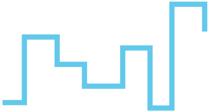
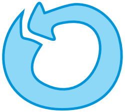
Incomplete! But are we missing proof rules?

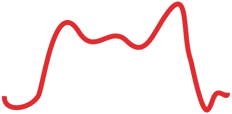
Incomplete! But are we missing proof rules?

Relativity

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

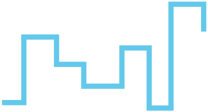
Sources of Incompleteness

 +  + 

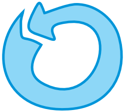


continuous

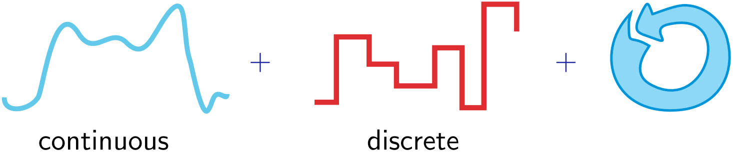
+



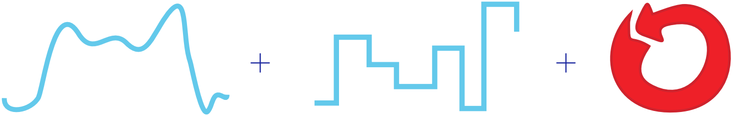
+



Sources of Incompleteness

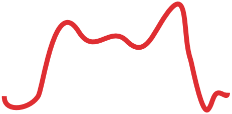


Sources of Incompleteness



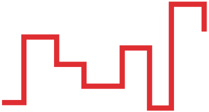
continuous discrete repeat

Sources of Incompleteness



continuous

+



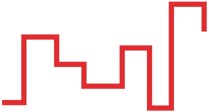
discrete

+

repeat

continuous

+



discrete

+

repeat

Relative Completeness

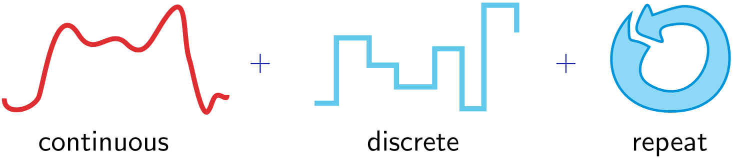
continuous + discrete + repeat

Relative Completeness

Theorem (Relative Completeness)

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

Proof Outline 15p

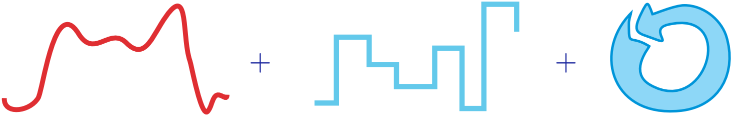


Relative Completeness

Theorem (Relative Completeness)

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

▸ Proof Outline 15p



continuous + discrete + repeat

$\Downarrow$

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)

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

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

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

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

Proof Outline 15p

Relative Completeness

Theorem (Relative Completeness)

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

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

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!