Differential Dynamic Logic for Verifying Parametric Hybrid Systems

André Platzer[1,2]

[1]University of Oldenburg, Department of Computing Science, Germany

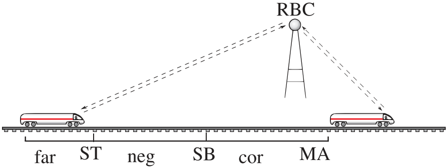
[2]Carnegie Mellon University, Computer Science Department, Pittsburgh, PA, USA

Tableaux'07

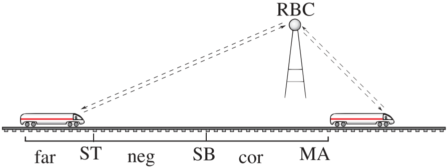
Outline

1. Motivation
2. Differential Logic d$\mathcal{L}$
   - Design Motives
   - Syntax
   - Transition Semantics
   - Speed Supervision in Train Control
3. Verification Calculus for d$\mathcal{L}$
   - Sequent Calculus
   - Modular Combination by Side Deduction
   - Verifying Speed Supervision in Train Control
   - Soundness
4. Conclusions & Future Work

Verifying Parametric Hybrid Systems

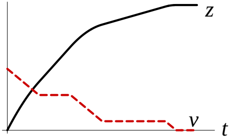


Verifying Parametric Hybrid Systems

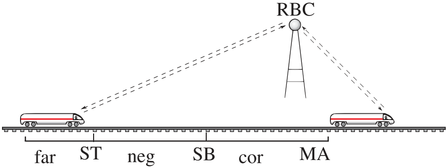


Hybrid Systems

continuous evolution along differential equations + discrete change

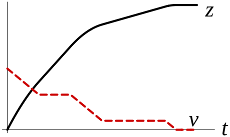


Verifying Parametric Hybrid Systems



Parametric Hybrid Systems

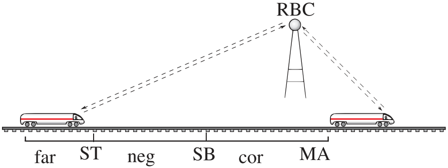
continuous evolution along differential equations + discrete change



- Fix parameter $SB = 10000$ and hope?
- Handle SB as free symbolic parameter?
- Which constraints for SB?

$$\forall MA\, \exists SB\, \textbf{all}(\textit{train-runs})\text{safe}$$

Verifying Parametric Hybrid Systems



Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

differential dynamic logic

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

J. M. Davoren and A. Nerode.
Logics for hybrid systems.
Proceedings of the IEEE, 88(7):985–1010, July 2000.

M. Rönkkö, A. P. Ravn, and K. Sere.
Hybrid action systems.
Theor. Comput. Sci., 290(1):937–973, 2003.

W. C. Rounds.
A spatial logic for the hybrid π-calculus.
In R. Alur and G. J. Pappas, editors, *HSCC*, volume 2993 of *LNCS*, pages 508–522. Springer, 2004.

C. Zhou, A. P. Ravn, and M. R. Hansen.
An extended duration calculus for hybrid real-time systems.
In R. L. Grossman, A. Nerode, A. P. Ravn, and H. Rischel, editors, *Hybrid Systems*, volume 736 of *LNCS*, pages 36–59. Springer, 1992.

Outline

1. Motivation
2. Differential Logic d$\mathcal{L}$
   - Design Motives
   - Syntax
   - Transition Semantics
   - Speed Supervision in Train Control
3. Verification Calculus for d$\mathcal{L}$
   - Sequent Calculus
   - Modular Combination by Side Deduction
   - Verifying Speed Supervision in Train Control
   - Soundness
4. Conclusions & Future Work

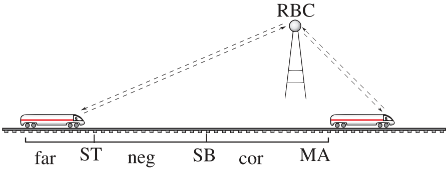
Outline

1. Motivation
2. Differential Logic d$\mathcal{L}$
   - Design Motives
   - Syntax
   - Transition Semantics
   - Speed Supervision in Train Control
3. Verification Calculus for d$\mathcal{L}$
   - Sequent Calculus
   - Modular Combination by Side Deduction
   - Verifying Speed Supervision in Train Control
   - Soundness
4. Conclusions & Future Work

d$\mathcal{L}$ Motives:

differential dynamic logic

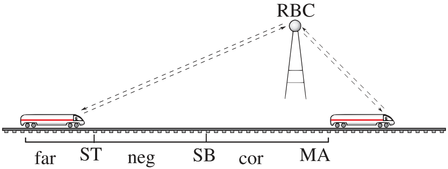
$$d\mathcal{L} = \qquad DL + HP$$

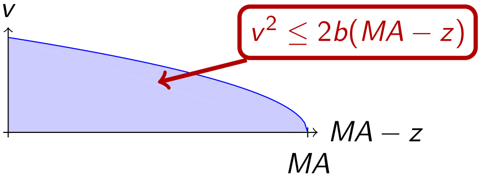


dℒ Motives: Regions in First-order Logic

differential dynamic logic

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

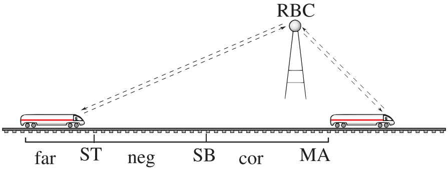


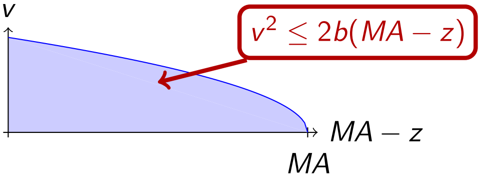


d$\mathcal{L}$ Motives: Regions in First-order Logic

differential dynamic logic

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





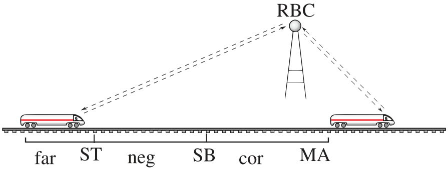
$$v^2 \le 2b(MA - z)$$

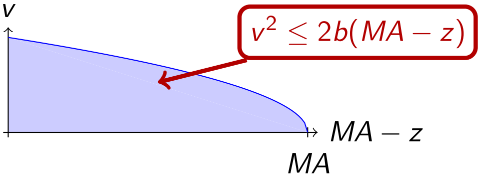
$$\forall t\, \textbf{after}(\text{train-runs}(t))(v^2 \le 2b(MA - z))$$

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

differential dynamic logic

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





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

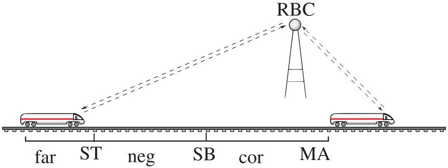
$$\forall t\, \textbf{after}(\text{train-runs}(t))(v^2 \leq 2b(MA - z))$$

$$[\text{train-runs}]v^2 \leq 2b(MA - z)$$

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

differential dynamic logic

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

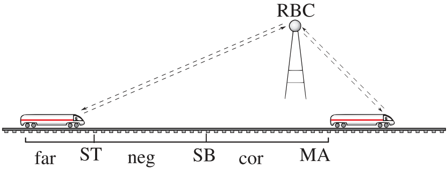


$$[\text{train-runs}]v^2 \leq 2b(MA - z)$$

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

differential dynamic logic

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

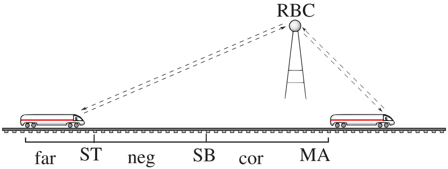


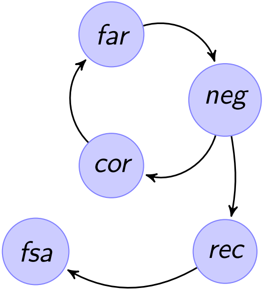
[ ]$v^2 \leq 2b(MA - z)$

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

differential dynamic logic

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

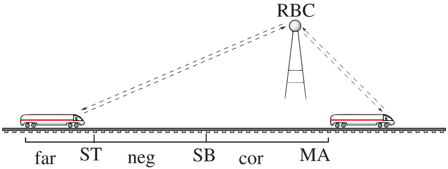


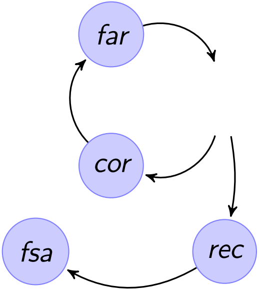


d$\mathcal{L}$ Motives: Hybrid Programs as Uniform Model

differential dynamic logic

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

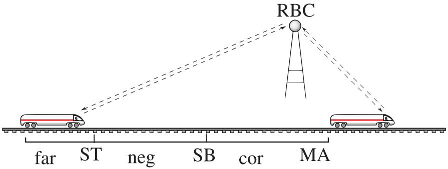


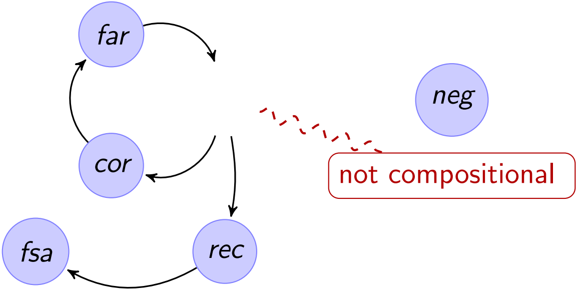


d$\mathcal{L}$ Motives: Hybrid Programs as Uniform Model

differential dynamic logic

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





Differential Logic d$\mathcal{L}$: Syntax

Definition (Hybrid program α)

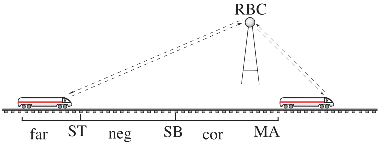
$x' = f(x)$	(continuous evolution)
$x := \theta$	(discrete jump)
$?\chi$	(conditional execution)
$\alpha;\beta$	(seq. composition)
$\alpha \cup \beta$	(nondet. choice)
α^*	(nondet. repetition)

Differential Logic d$\mathcal{L}$: Syntax

Definition (Hybrid program α)

$x' = f(x)$	(continuous evolution)
$x := \theta$	(discrete jump)
$?\chi$	(conditional execution)
$\alpha; \beta$	(seq. composition)
$\alpha \cup \beta$	(nondet. choice)
α^*	(nondet. repetition)

$$\begin{aligned}
ETCS &\equiv (cor\,; drive)^* \\
cor &\equiv (?MA - z \leq SB; a := -b) \\
&\quad \cup (?MA - z \geq SB; a := 0) \\
drive &\equiv \tau := 0; z'' = a \\
&\quad \& \, v \geq 0 \wedge \tau \leq \varepsilon
\end{aligned}$$

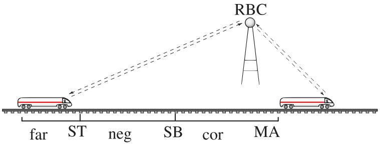


Differential Logic d$\mathcal{L}$: Syntax

Definition (Hybrid program α)

$x' = f(x)$	(continuous evolution)
$x := \theta$	(discrete jump)
$?\chi$	(conditional execution)
$\alpha ; \beta$	(seq. composition)
$\alpha \cup \beta$	(nondet. choice)
α^*	(nondet. repetition)

$$
\begin{aligned}
ETCS &\equiv (cor\,;drive)^* \\
cor &\equiv (?MA - z \leq SB;\, a := -b) \\
&\quad \cup (?MA - z \geq SB;\, a \leq a_{\max}) \\
drive &\equiv \tau := 0;\, z'' = a \\
&\quad \& \, v \geq 0 \wedge \tau \leq \varepsilon
\end{aligned}
$$

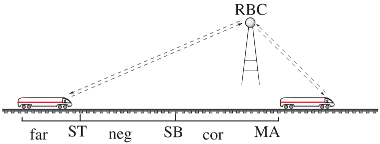


Differential Logic d$\mathcal{L}$: Syntax

Definition (Hybrid program α)

$x' = f(x)$	(continuous evolution)
$x := \theta$	(discrete jump)
$?\chi$	(conditional execution)
$\alpha; \beta$	(seq. composition)
$\alpha \cup \beta$	(nondet. choice)
α^*	(nondet. repetition)

$$\begin{aligned}
ETCS &\equiv (cor\,; drive)^* \\
cor &\equiv (?MA - z \leq SB; a := -b) \\
&\quad \cup (?MA - z \geq SB; a \leq a_{\mathrm{max}}) \\
drive &\equiv \tau := 0; z' = v, v' = a, \tau' = 1 \\
&\quad \& \; v \geq 0 \wedge \tau \leq \varepsilon
\end{aligned}$$

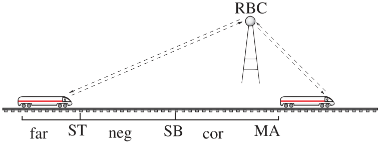


Differential Logic d$\mathcal{L}$: Syntax

Definition (Hybrid program α)

$x' = f(x) \,\&\, \chi$	(continuous evolution within invariant region)
$x := \theta$	(discrete jump)
$?\chi$	(conditional execution)
$\alpha; \beta$	(seq. composition)
$\alpha \cup \beta$	(nondet. choice)
α^*	(nondet. repetition)

$$
\begin{aligned}
ETCS &\equiv (cor\,;drive)^* \\
cor &\equiv (?MA - z \leq SB; a := -b) \\
&\quad \cup (?MA - z \geq SB; a \leq a_{\max}) \\
drive &\equiv \tau := 0; z' = v, v' = a, \tau' = 1 \\
&\quad \& \, v \geq 0 \land \tau \leq \varepsilon
\end{aligned}
$$



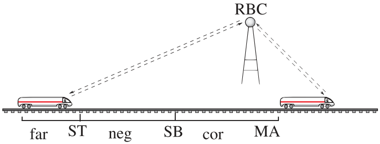
Differential Logic d$\mathcal{L}$: Syntax

Definition (Formulas ϕ)

$\neg, \wedge, \vee, \rightarrow, \ \forall x, \exists x, \ =, \leq, \ +, \cdot$ (**R**-first-order part)

$[\alpha]\phi, \quad \langle\alpha\rangle\phi$ (dynamic part)

$$\psi \ \rightarrow \ [(cor\,;drive)^*]\, z \leq MA$$

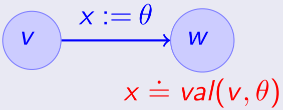


All trains respect MA

$\Rightarrow$ system safe

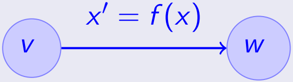
Differential Logic d$\mathcal{L}$: Transition Semantics

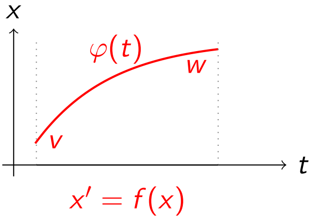
Definition (Hybrid programs α: transition semantics)



Differential Logic d$\mathcal{L}$: Transition Semantics

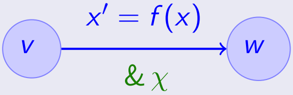
Definition (Hybrid programs α: transition semantics)





Differential Logic d$\mathcal{L}$: Transition Semantics

Definition (Hybrid programs α: transition semantics)

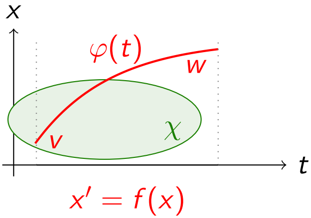


$x' = f(x)$

v

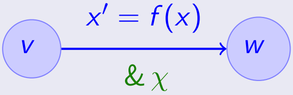
w

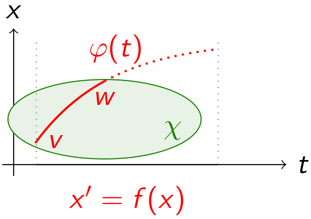
$\& \chi$



Differential Logic d$\mathcal{L}$: Transition Semantics

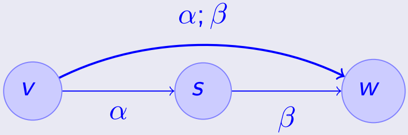
Definition (Hybrid programs α: transition semantics)





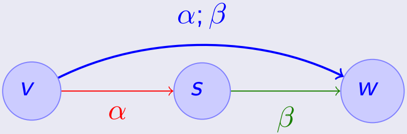
Differential Logic d$\mathcal{L}$: Transition Semantics

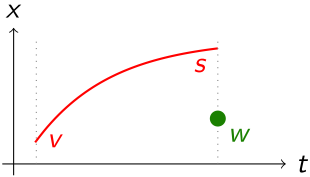
Definition (Hybrid programs α: transition semantics)



Differential Logic d$\mathcal{L}$: Transition Semantics

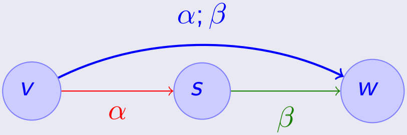
Definition (Hybrid programs α: transition semantics)

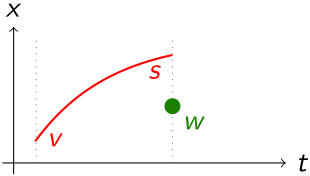




Differential Logic d$\mathcal{L}$: Transition Semantics

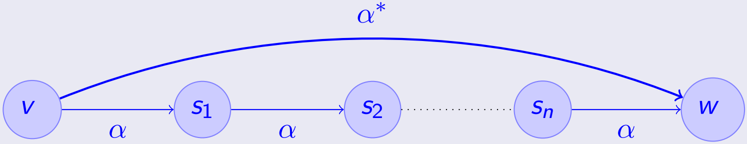
Definition (Hybrid programs α: transition semantics)





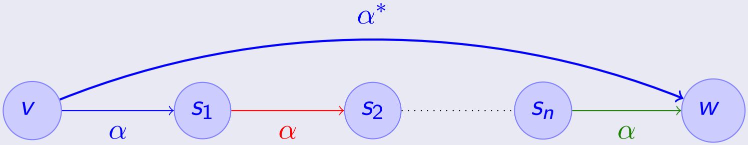
Differential Logic d$\mathcal{L}$: Transition Semantics

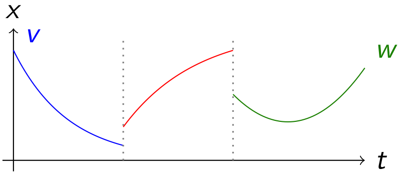
Definition (Hybrid programs α: transition semantics)



Differential Logic d$\mathcal{L}$: Transition Semantics

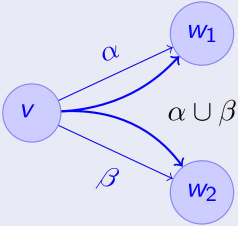
Definition (Hybrid programs α: transition semantics)





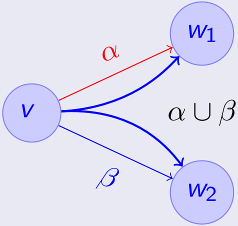
Differential Logic d$\mathcal{L}$: Transition Semantics

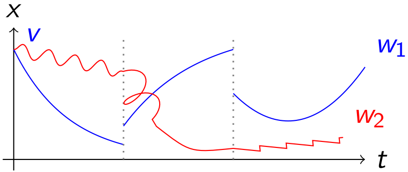
Definition (Hybrid programs α: transition semantics)



Differential Logic d$\mathcal{L}$: Transition Semantics

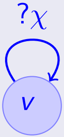
Definition (Hybrid programs α: transition semantics)





Differential Logic d$\mathcal{L}$: Transition Semantics

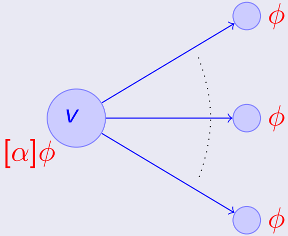
Definition (Hybrid programs α: transition semantics)



if $v \models \chi$

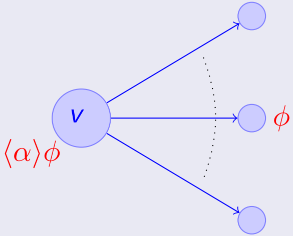
Differential Logic d$\mathcal{L}$: Transition Semantics

Definition (Formulas ϕ)



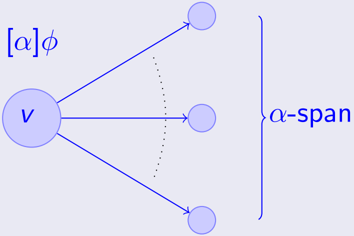
Differential Logic d$\mathcal{L}$: Transition Semantics

Definition (Formulas ϕ)



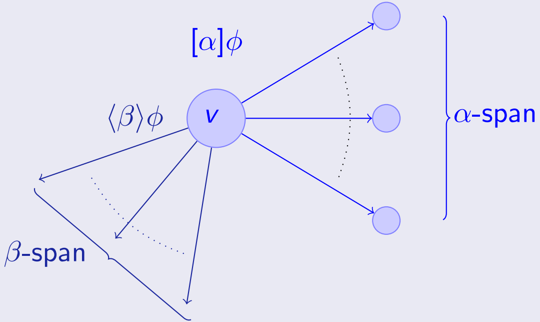
Differential Logic d$\mathcal{L}$: Transition Semantics

Definition (Formulas ϕ)



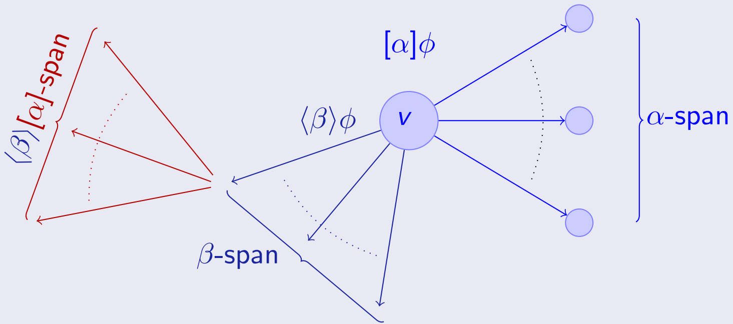
Differential Logic d$\mathcal{L}$: Transition Semantics

Definition (Formulas ϕ)



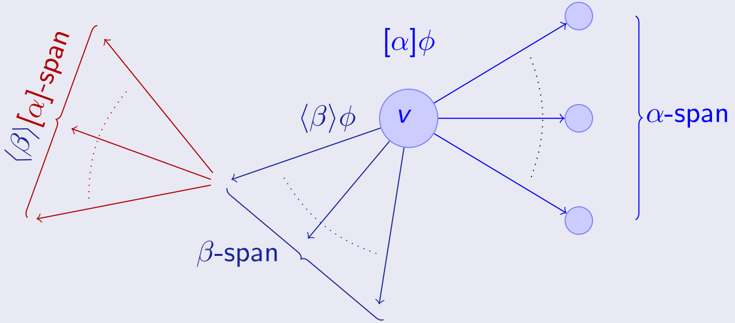
Differential Logic d$\mathcal{L}$: Transition Semantics

Definition (Formulas ϕ)



Differential Logic d$\mathcal{L}$: Transition Semantics

Definition (Formulas ϕ)



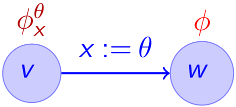
compositional semantics!

Outline

1. Motivation
2. Differential Logic d$\mathcal{L}$
   - Design Motives
   - Syntax
   - Transition Semantics
   - Speed Supervision in Train Control
3. Verification Calculus for d$\mathcal{L}$
   - Sequent Calculus
   - Modular Combination by Side Deduction
   - Verifying Speed Supervision in Train Control
   - Soundness
4. Conclusions & Future Work

Verification Calculus for d$\mathcal{L}$

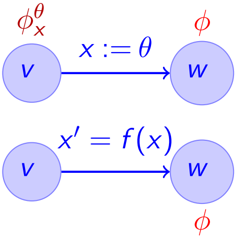
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$



Verification Calculus for d$\mathcal{L}$

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

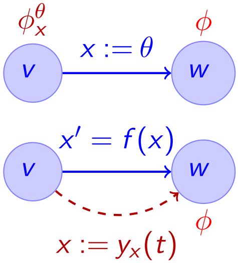
$$\frac{\exists t \geq 0\, \langle x := y_x(t) \rangle \phi}{\langle x' = f(x) \rangle \phi}$$



Verification Calculus for d$\mathcal{L}$

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

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



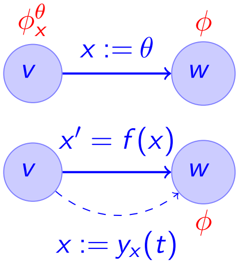
Verification Calculus for d$\mathcal{L}$

Differential Analyser for Solving Differential Equations
invented 1876
built 1927

Verification Calculus for d$\mathcal{L}$

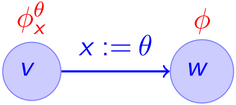
$$\frac{\phi_x^\theta}{\langle x := \theta \rangle \phi}$$

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

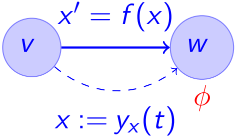


Verification Calculus for d$\mathcal{L}$

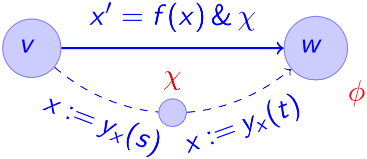
$$\frac{\phi_x^\theta}{\langle x := \theta\rangle\phi}$$



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



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



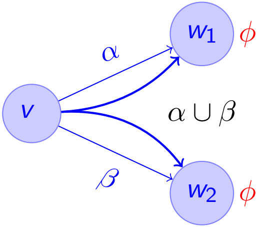
$$\bar\chi \;\equiv\; \forall 0{\leq}s{\leq}t\,\langle x := y_x(s)\rangle\chi$$

Verification Calculus for d$\mathcal{L}$

compositional semantics $\Rightarrow$ other rules as usual!

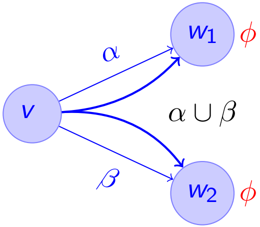
Verification Calculus for d$\mathcal{L}$

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

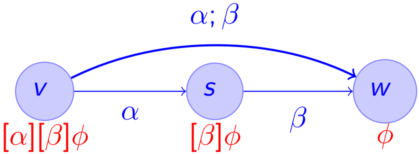


Verification Calculus for d$\mathcal{L}$

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

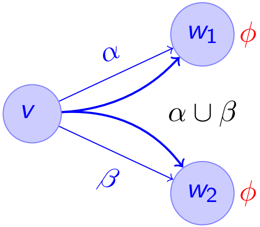


$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$

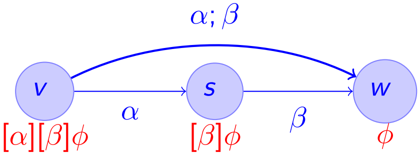


Verification Calculus for d$\mathcal{L}$

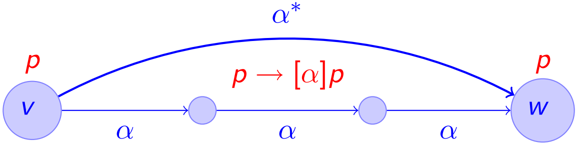
$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$



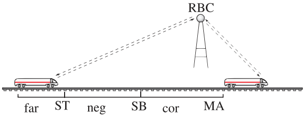
$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$



$$\frac{\vdash p \quad \vdash (p \rightarrow [\alpha]p)}{\vdash [\alpha^*]p}$$

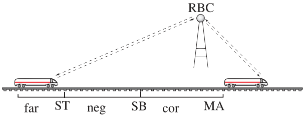


Modular Combination by Side Deduction



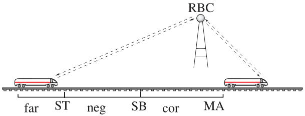
$$\vdash v > 0 \land z < MA \rightarrow \langle z' = v, v' = -b \rangle\ z \geq MA$$

Modular Combination by Side Deduction



$$\dfrac{\dfrac{\overline{v > 0, z < MA \vdash \exists t{\geq}0\, \langle z := -\frac{b}{2}t^2 + vt + z\rangle z \geq MA}}{v > 0, z < MA \vdash \langle z' = v, v' = -b\rangle z \geq MA}}{\vdash v > 0 \land z < MA \rightarrow \langle z' = v, v' = -b\rangle\ z \geq MA}$$

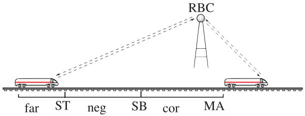
Modular Combination by Side Deduction



QE not applicable!

$$\cfrac{\cfrac{\overline{v > 0, z < MA \vdash \exists t{\geq}0\, \langle z := -\frac{b}{2}t^2 + vt + z\rangle z \geq MA}}{v > 0, z < MA \vdash \langle z' = v, v' = -b\rangle z \geq MA}}{\vdash v > 0 \land z < MA \rightarrow \langle z' = v, v' = -b\rangle\; z \geq MA}$$

Modular Combination by Side Deduction

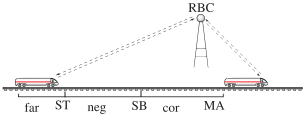


$$\frac{}{v > 0, z < MA \vdash t \geq 0 \land \langle z := -\frac{b}{2}t^2 + vt + z\rangle z \geq MA}$$

start side

$$\cfrac{\cfrac{\cfrac{}{v > 0, z < MA \vdash \exists t{\geq}0 \, \langle z := -\frac{b}{2}t^2 + vt + z\rangle z \geq MA}}{v > 0, z < MA \vdash \langle z' = v, v' = -b\rangle z \geq MA}}{\vdash v > 0 \land z < MA \to \langle z' = v, v' = -b\rangle \; z \geq MA}$$

Modular Combination by Side Deduction

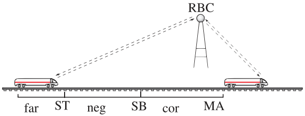


$$\cfrac{v > 0, z < MA \vdash t \geq 0 \qquad \cfrac{v > 0, z < MA \vdash -\frac{b}{2}t^2 + vt + z \geq MA}{v > 0, z < MA \vdash \langle z := -\frac{b}{2}t^2 + vt + z\rangle z \geq M}}{v > 0, z < MA \vdash t \geq 0 \land \langle z := -\frac{b}{2}t^2 + vt + z\rangle z \geq MA}$$

start
side

$$\cfrac{\cfrac{\cfrac{}{v > 0, z < MA \vdash \exists t \geq 0\, \langle z := -\frac{b}{2}t^2 + vt + z\rangle z \geq MA}}{v > 0, z < MA \vdash \langle z' = v, v' = -b\rangle z \geq MA}}{\vdash v > 0 \land z < MA \rightarrow \langle z' = v, v' = -b\rangle\ z \geq MA}$$

Modular Combination by Side Deduction



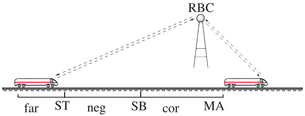
$$\dfrac{v>0,z<MA \vdash t{\geq}0 \qquad \dfrac{v>0,z<MA \vdash -\frac{b}{2}t^2+vt+z \geq MA}{v>0,z<MA \vdash \langle z:=-\frac{b}{2}t^2+vt+z\rangle z \geq M}}{v>0,z<MA \vdash t\geq 0 \land \langle z:=-\frac{b}{2}t^2+vt+z\rangle z \geq MA}$$

QE

start side

$$\dfrac{\dfrac{\dfrac{v>0,z<MA \vdash v^2 \geq 2b(MA-z)}{v>0,z<MA \vdash \exists t{\geq}0\,\langle z:=-\frac{b}{2}t^2+vt+z\rangle z \geq MA}}{v>0,z<MA \vdash \langle z'=v,v'=-b\rangle z \geq MA}}{\vdash v>0 \land z<MA \rightarrow \langle z'=v,v'=-b\rangle\ z \geq MA}$$

Modular Combination by Side Deduction



$$\dfrac{v>0, z<MA \vdash t{\geq}0 \qquad \dfrac{v>0, z<MA \vdash -\frac{b}{2}t^2+vt+z \geq MA}{v>0, z<MA \vdash \langle z := -\frac{b}{2}t^2+vt+z\rangle z \geq M}}{v>0, z<MA \vdash t \geq 0 \wedge \langle z := -\frac{b}{2}t^2+vt+z\rangle z \geq MA}$$

QE

$$\dfrac{\dfrac{\dfrac{v>0, z<MA \vdash \color{red}{v^2 \geq 2b(MA-z)}}{v>0, z<MA \vdash \exists t{\geq}0\, \langle z := -\frac{b}{2}t^2+vt+z\rangle z \geq MA}}{v>0, z<MA \vdash \langle z'=v, v'=-b\rangle z \geq MA}}{\vdash v>0 \wedge z<MA \rightarrow \langle z'=v, v'=-b\rangle\ z \geq MA}$$

start
side

Verification Calculus for d$\mathcal{L}$

Dynamic Rules

11 dynamic rules

$$\text{(D1)}\quad \frac{\phi \land \psi}{\langle ?\phi\rangle\psi}$$

$$\text{(D2)}\quad \frac{\phi \to \psi}{[?\phi]\psi}$$

$$\text{(D3)}\quad \frac{\langle\alpha\rangle\phi \lor \langle\beta\rangle\phi}{\langle\alpha \cup \beta\rangle\phi}$$

$$\text{(D4)}\quad \frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$

$$\text{(D5)}\quad \frac{\phi \lor \langle\alpha;\alpha^*\rangle\phi}{\langle\alpha^*\rangle\phi}$$

$$\text{(D6)}\quad \frac{\phi \land [\alpha;\alpha^*]\phi}{[\alpha^*]\phi}$$

$$\text{(D7)}\quad \frac{\langle\alpha\rangle\langle\beta\rangle\phi}{\langle\alpha;\beta\rangle\phi}$$

$$\text{(D8)}\quad \frac{\phi_x^\theta}{\langle x := \theta\rangle\phi}$$

$$\text{(D9)}\quad \frac{\exists t{\geq}0\,(\bar{\chi} \land \langle x := y_x}{\langle x' = \theta \,\&\, \chi\rangle}$$

$$\text{(D10)}\quad \frac{\forall t{\geq}0\,(\bar{\chi} \to [x := y}{[x' = \theta \,\&\, \chi]}$$

$$\text{(D11)}\quad \frac{\vdash p \qquad \vdash [\alpha^*](p \to [\alpha]p)}{\vdash [\alpha^*]p}$$

Verification Calculus for d$\mathcal{L}$

Propositional/Quantifier Rules

9 propositional rules + 4 quantifier rules

$$\text{(P1)}\ \frac{\vdash \phi}{\neg\phi \vdash} \qquad \text{(P4)}\ \frac{\phi, \psi \vdash}{\phi \wedge \psi \vdash} \qquad \text{(P7)}\ \frac{\phi \vdash \qquad \psi \vdash}{\phi \vee \psi \vdash}$$

$$\text{(P2)}\ \frac{\phi \vdash}{\vdash \neg\phi} \qquad \text{(P5)}\ \frac{\vdash \phi \qquad \vdash \psi}{\vdash \phi \wedge \psi} \qquad \text{(P8)}\ \frac{\vdash \phi, \psi}{\vdash \phi \vee \psi}$$

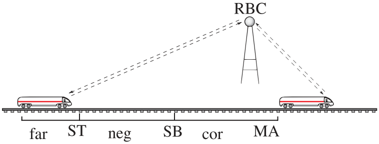
$$\text{(P3)}\ \frac{\phi \vdash \psi}{\vdash \phi \rightarrow \psi} \qquad \text{(P6)}\ \frac{\vdash \phi \qquad \psi \vdash}{\phi \rightarrow \psi \vdash} \qquad \text{(P9)}\ \frac{}{\phi \vdash \phi}$$

$$\text{(F1)}\ \frac{\mathrm{QE}(\exists x \bigwedge_i (\Gamma_i \vdash \Delta_i))}{\Gamma \vdash \Delta, \exists x\, \phi} \qquad \text{(F3)}\ \frac{\mathrm{QE}(\forall x \bigwedge_i (\Gamma_i \vdash \Delta_i))}{\Gamma \vdash \Delta, \forall x\, \phi}$$

$$\text{(F2)}\ \frac{\mathrm{QE}(\forall x \bigwedge_i (\Gamma_i \vdash \Delta_i))}{\Gamma, \exists x\, \phi \vdash \Delta} \qquad \text{(F4)}\ \frac{\mathrm{QE}(\exists x \bigwedge_i (\Gamma_i \vdash \Delta_i))}{\Gamma, \forall x\, \phi \vdash \Delta}$$

Verify Safety in Train Control

$$
\begin{aligned}
\psi \;\rightarrow\; & [(cor\,; drive)^*]\, z \leq MA \\
cor \equiv\; & (?MA - z < SB;\, a := -b) \\
& \cup (?MA - z \geq SB;\, a := 0) \\
drive \equiv\; & \tau := 0;\, z' = v, v' = a, \tau' = 1 \\
& \&\, v \geq 0 \land \tau \leq \varepsilon
\end{aligned}
$$



Verify Safety in Train Control

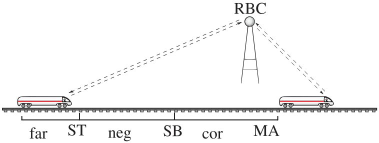
$$\psi \;\rightarrow\; [(cor\,;drive)^*]\,z \le MA$$

$$cor \equiv (?MA - z < SB;\, a := -b)$$

$$\cup\,(?MA - z \ge SB;\, a := 0)$$

$$drive \equiv \tau := 0;\, z' = v, v' = a, \tau' = 1$$

$$\&\; v \ge 0 \land \tau \le \varepsilon$$

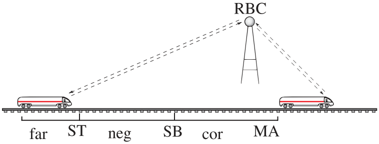


$$\begin{array}{l}
*\\ \hline
p\vdash\ \forall t{\ge}0\,(\langle v := -bt + v\rangle v \ge 0 \rightarrow \langle z := -\frac{b}{2}t^2 + vt + z;\, v := -bt + v\rangle p)\\ \hline
p\vdash\ [z' = v, v' = -b\,\&\, v \ge 0]p\\ \hline
p\vdash\ \langle a := -b\rangle[drive]p
\end{array}$$

$$\begin{array}{l}
\dots\\ \hline
p,\, MA{-}z{\ge}SB\vdash\ v^2 \le 2b(MA - \varepsilon v - z)\\ \hline
p,\, MA{-}z{\ge}SB\vdash\ \forall t{\ge}0\,(\langle\tau := t\rangle\tau \le \varepsilon \rightarrow \langle z := vt\\ \hline
p,\, MA{-}z{\ge}SB\vdash\ \langle\tau := 0\rangle\forall t{\ge}0\,(\langle\tau := t + \tau\rangle\tau \le \varepsilon\\ \hline
p,\, MA{-}z{\ge}SB\vdash\ \langle\tau := 0\rangle[z' = v, v' = 0, \tau' = 1\,\&\\ \hline
p,\, MA{-}z{\ge}SB\vdash\ \langle a := 0\rangle\langle\tau := 0\rangle[z' = v, v' = a, \tau\\ \hline
p,\, MA{-}z{\ge}SB\vdash\ \langle a := 0\rangle[drive]p\\ \hline
p\vdash\ [?MA{-}z{\ge}SB;\, a := 0][drive]p
\end{array}$$

$$\begin{array}{l}
\hline
p\vdash\ [cor][drive]p\\ \hline
p\vdash\ [cor\,;drive]p
\end{array}$$

Verify Safety in Train Control



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

$$\ldots$$

$$p,\ MA{-}z{\ge}SB \vdash\ v^2 \le 2b(MA - \varepsilon v - z)$$

$$p,\ MA{-}z{\ge}SB \vdash\ \forall t{\ge}0\,(\langle \tau := t\rangle \tau \le \varepsilon \rightarrow \langle z := vt$$

$$p,\ MA{-}z{\ge}SB \vdash\ \langle \tau := 0\rangle \forall t{\ge}0\,(\langle \tau := t + \tau\rangle \tau \le \varepsilon$$

$$p,\ MA{-}z{\ge}SB \vdash\ \langle \tau := 0\rangle [z' = v, v' = 0, \tau' = 1 \,\&$$

$$p,\ MA{-}z{\ge}SB \vdash\ \langle a := 0\rangle \langle \tau := 0\rangle [z' = v, v' = a, \tau$$

$$p,\ MA{-}z{\ge}SB \vdash\ \langle a := 0\rangle [drive]p$$

$$*$$

$$p \vdash\ \forall t{\ge}0\,(\langle v := -bt + v\rangle v \ge 0 \rightarrow \langle z := -\tfrac{b}{2}t^2 + vt + z; v := -bt + v\rangle p)$$

$$p \vdash\ [z' = v, v' = -b \,\&\, v \ge 0]p$$

$$p \vdash\ \langle a := -b\rangle [drive]p$$

$$p \vdash\ [?MA{-}z{\ge}SB;\ a := 0][drive]p$$

$$p \vdash\ [cor][drive]p$$

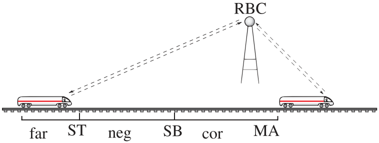
$$p \vdash\ [cor\,;\, drive]p$$

Verify Safety in Train Control

$$\boxed{SB \geq \varepsilon v + \frac{v^2}{2b}}$$

$$\Big\uparrow \text{QE}$$

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



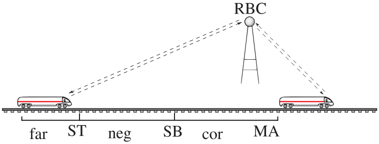
$$\begin{array}{l|l}
 & \cdots \\ \hline
 & p, MA-z\geq SB \vdash v^2 \leq 2b(MA - \varepsilon v - z) \\ \hline
 & p, MA-z\geq SB \vdash \forall t\geq 0\,(\langle \tau := t\rangle \tau \leq \varepsilon \rightarrow \langle z := vt \\ \hline
 & p, MA-z\geq SB \vdash \langle \tau := 0\rangle \forall t\geq 0\,(\langle \tau := t + \tau\rangle \tau \leq \varepsilon \\ \hline
* & p, MA-z\geq SB \vdash \langle \tau := 0\rangle [z' = v, v' = 0, \tau' = 1 \,\& \\ \hline
p\vdash \forall t\geq 0\,(\langle v := -bt + v\rangle v \geq 0 \rightarrow \langle z := -\frac{b}{2}t^2 + vt + z; v := -bt + v\rangle p) & p, MA-z\geq SB \vdash \langle a := 0\rangle \langle \tau := 0\rangle [z' = v, v' = a, \tau \\ \hline
p\vdash [z' = v, v' = -b \,\&\, v \geq 0]p & p, MA-z\geq SB \vdash \langle a := 0\rangle [drive]p \\ \hline
p\vdash \langle a := -b\rangle [drive]p & p\vdash [?MA-z\geq SB; a := 0][drive]p \\ \hline
\multicolumn{2}{c}{p\vdash [cor][drive]p} \\ \hline
\multicolumn{2}{c}{p\vdash [cor\,; drive]p}
\end{array}$$

Verify Safety in Train Control

$$\boxed{SB \ \geq \ \frac{v^2}{2b} + \left(\frac{a}{b} + 1\right)\left(\frac{a}{2}\varepsilon^2 + \varepsilon v\right)}$$

QE

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



$$\ast$$

$$p \vdash \ \forall t {\geq} 0 \left(\langle v := -bt + v\rangle v \geq 0 \rightarrow \langle z := -\tfrac{b}{2}t^2 + vt + z; v := -bt + v\rangle p\right)$$

$$p \vdash \ [z' = v, v' = -b \,\&\, v \geq 0]p$$

$$p \vdash \ \langle a := -b\rangle[drive]p$$

$$\ldots$$

$$p, MA{-}z{\geq}SB \vdash \ v^2 \leq 2b(MA - \varepsilon v - z)$$

$$p, MA{-}z{\geq}SB \vdash \ \forall t{\geq}0 \left(\langle \tau := t\rangle \tau \leq \varepsilon \rightarrow \langle z := vt\right.$$

$$p, MA{-}z{\geq}SB \vdash \ \langle \tau := 0\rangle \forall t{\geq}0 \left(\langle \tau := t + \tau\rangle \tau \leq \varepsilon\right.$$

$$p, MA{-}z{\geq}SB \vdash \ \langle \tau := 0\rangle[z' = v, v' = 0, \tau' = 1 \,\&$$

$$p, MA{-}z{\geq}SB \vdash \ \langle a := 0\rangle\langle \tau := 0\rangle[z' = v, v' = a, \tau$$

$$p, MA{-}z{\geq}SB \vdash \ \langle a := 0\rangle[drive]p$$

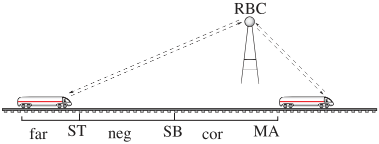
$$p \vdash \ [?MA{-}z{\geq}SB; a := 0][drive]p$$

$$p \vdash \ [cor][drive]p$$

$$p \vdash \ [cor\,; drive]p$$

Verify Safety in Train Control

$$\boxed{\text{inv} \;\equiv\; v^2 \le 2b(MA - z)}$$

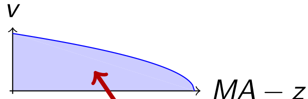


$$\dfrac{\dfrac{\dfrac{\dfrac{*}{p \vdash \forall t{\ge}0\,(\langle v := -bt + v\rangle v \ge 0 \rightarrow \langle z := -\frac{b}{2}t^2 + vt + z;\, v := -bt + v\rangle p)}}{p \vdash [z' = v, v' = -b \,\&\, v \ge 0]p}}{p \vdash \langle a := -b\rangle[drive]p}}{}$$

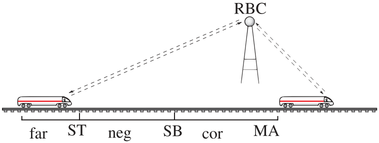
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dots}{p,\, MA{-}z{\ge}SB \vdash v^2 \le 2b(MA - \varepsilon v - z)}}{p,\, MA{-}z{\ge}SB \vdash \forall t{\ge}0\,(\langle \tau := t\rangle \tau \le \varepsilon \rightarrow \langle z := vt}}{p,\, MA{-}z{\ge}SB \vdash \langle \tau := 0\rangle \forall t{\ge}0\,(\langle \tau := t + \tau\rangle \tau \le \varepsilon}}{p,\, MA{-}z{\ge}SB \vdash \langle \tau := 0\rangle [z' = v, v' = 0, \tau' = 1 \,\&}}{p,\, MA{-}z{\ge}SB \vdash \langle a := 0\rangle \langle \tau := 0\rangle [z' = v, v' = a, \tau}}{p,\, MA{-}z{\ge}SB \vdash \langle a := 0\rangle [drive]p}}{p \vdash [?MA{-}z{\ge}SB;\, a := 0][drive]p}}{}$$

$$\dfrac{p \vdash [cor][drive]p}{p \vdash [cor\,;\, drive]p}$$

Verify Safety in Train Control



$$\boxed{\mathrm{inv} \;\equiv\; v^2 \le 2b(MA - z)}$$



$$\dfrac{\dfrac{\dfrac{\dfrac{*}{p \vdash\ \forall t{\ge}0\,(\langle v := -bt + v\rangle v \ge 0 \rightarrow \langle z := -\frac{b}{2}t^2 + vt + z; v := -bt + v\rangle p)}}{p \vdash\ [z' = v, v' = -b \,\&\, v \ge 0]p}}{p \vdash\ \langle a := -b\rangle[drive]p}}{}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dots}{p, MA{-}z{\ge}SB \vdash\ v^2 \le 2b(MA - \varepsilon v - z)}}{p, MA{-}z{\ge}SB \vdash\ \forall t{\ge}0\,(\langle \tau := t\rangle \tau \le \varepsilon \rightarrow \langle z := vt}}{p, MA{-}z{\ge}SB \vdash\ \langle \tau := 0\rangle \forall t{\ge}0\,(\langle \tau := t + \tau\rangle \tau \le \varepsilon}}{p, MA{-}z{\ge}SB \vdash\ \langle \tau := 0\rangle[z' = v, v' = 0, \tau' = 1 \,\&}}{p, MA{-}z{\ge}SB \vdash\ \langle a := 0\rangle\langle \tau := 0\rangle[z' = v, v' = a, \tau}}{p, MA{-}z{\ge}SB \vdash\ \langle a := 0\rangle[drive]p}}{p \vdash\ [?MA{-}z{\ge}SB; a := 0][drive]p}$$

$$\dfrac{p \vdash\ [cor][drive]p}{p \vdash\ [cor\,; drive]p}$$

Soundness

Theorem (Soundness)

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

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

Proposition (Incompleteness)

The discrete or continuous fragments of d$\mathcal{L}$ *are inherently incomplete. (Yet, reachability in hybrid systems is undecidable)*

Soundness

Proof

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

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

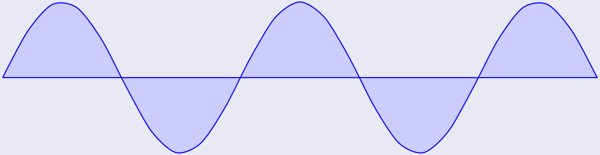
Soundness

Proof

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

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

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



Verified ETCS Model

$$
\begin{array}{lcl}
\text{system} & : & \big(\text{poll};\ (\text{negot} \cup (\text{speedControl};\ \text{atp};\ \text{move}))\big)^* \\
\text{init} & : & drive := 0;\ brake := 1 \\
\text{poll} & : & SB := \frac{v^2-d^2}{2b} + \left(\frac{a_{max}}{b} + 1\right)\left(\frac{a_{max}}{2}\varepsilon^2 + \varepsilon v\right);\ ST := * \\
\text{negot} & : & (?m - z > ST) \cup (?m - z \le ST;\ \text{rbc}) \\
\text{rbc} & : & (vdes := *;\ ?vdes > 0) \cup (state := brake) \\
 & & \cup\ \big(d_{old} := d;\ m_{old} := m;\ m := *;\ d := *; \\
 & & \quad ?d \ge 0 \land d_{old}^2 - d^2 \le 2b(m - m_{old})\big) \\
\text{speedCtrl} & : & (?state = brake;\ a := -b) \\
 & & \cup \Big(?state = drive; \\
 & & \quad \big((?v \le v_{des};\ a := *;\ ? - b \le a \le a_{max}) \\
 & & \quad \cup(?v \ge v_{des};\ a := *;\ ?0 > a \ge\ - b)\big)\Big) \\
\text{atp} & : & (?m - z \le SB;\ a := -b) \cup (?m - z > SB) \\
\text{move} & : & t := 0;\ \{\dot{z} = v, \dot{v} = a, \dot{t} = 1, (v \ge 0 \land t \le \varepsilon)\}
\end{array}
$$

Outline

1 Motivation

2 Differential Logic $d\mathcal{L}$
- Design Motives
- Syntax
- Transition Semantics
- Speed Supervision in Train Control

3 Verification Calculus for $d\mathcal{L}$
- Sequent Calculus
- Modular Combination by Side Deduction
- Verifying Speed Supervision in Train Control
- Soundness

4 Conclusions & Future Work

Future Work

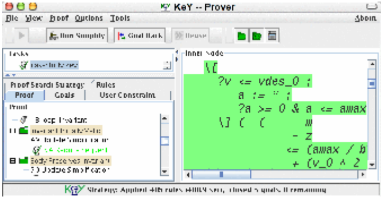
- Prove relative completeness of d$\mathcal{L}$/ODE
- Dynamic reconfiguration of system structures

Conclusions

differential dynamic logic

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

- Deductively verify hybrid systems
- Train control (ETCS) verification
- Constructive deduction modulo by side deduction
- Verification tool HyKeY
- Parameter discovery



```
\[
  ?v <= vdes_0 ;
    a := * ;
    ?a >= 0 & a <= amax
  \] ( (     m
          - z
       <= (amax / b
        + (v_0 ^ 2
```