Differential Dynamic Logic for 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

KeY'07

CARL VON OSSIETZKY universität OLDENBURG

Carnegie Mellon

ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG

UNIVERSITÄT DES SAARLANDES

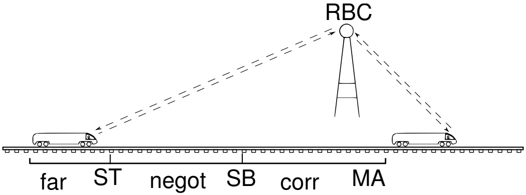
DAAD
Deutscher Akademischer Austausch Dienst
German Academic Exchange Service

Deutsche Forschungsgemeinschaft
DFG

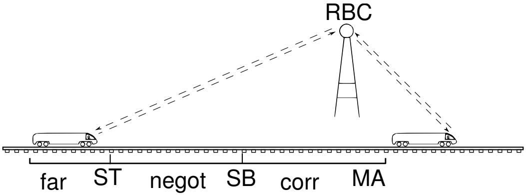
Outline

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

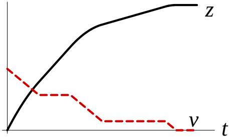


Verifying Parametric Hybrid Systems

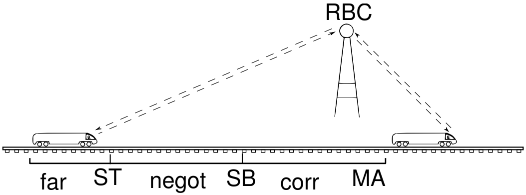


Hybrid Systems

continuous evolution along differential equations + discrete change



Verifying Parametric Hybrid Systems

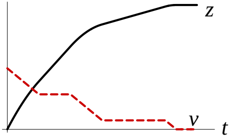


Parametric Hybrid Systems

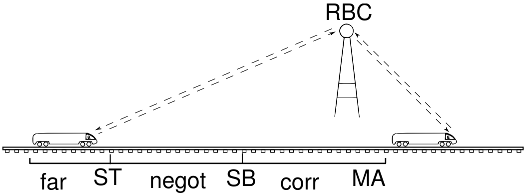
continuous evolution along differential equations + discrete change

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

$$\forall MA\, \exists SB\, [Train]\mathrm{safe}$$



Verifying Parametric Hybrid Systems



Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

differential dynamic logic

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

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

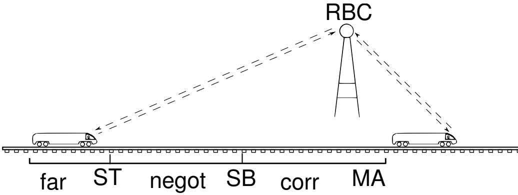
Outline

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: Regions in First-order Logic

differential dynamic logic

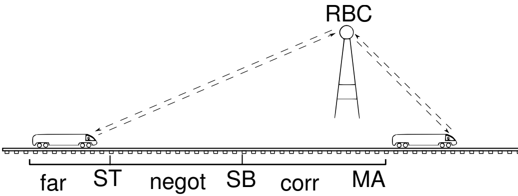
$$d\mathcal{L} = \qquad \text{DL} + \text{HP}$$

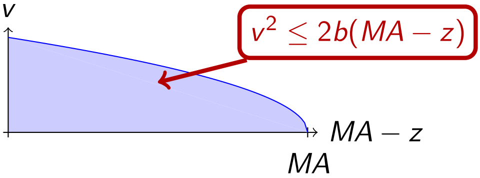


d$\mathcal{L}$ Motives: Regions in First-order Logic

differential dynamic logic

d$\mathcal{L}$ = FOL

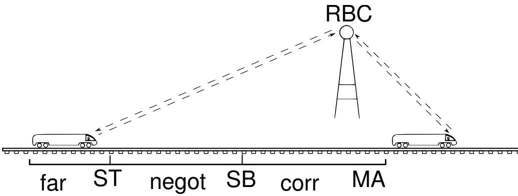


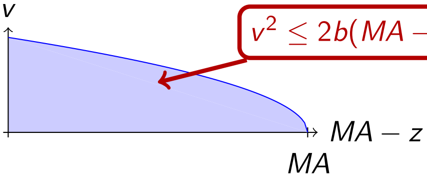


d$\mathcal{L}$ Motives: Regions in First-order Logic

differential dynamic logic

$d\mathcal{L} = \text{FOL}$





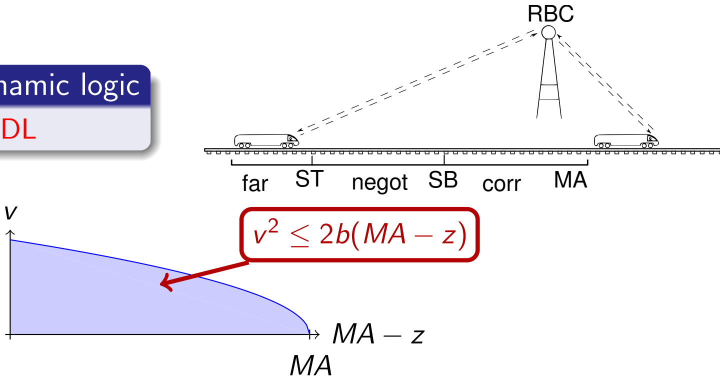
$\boxed{v^2 \leq 2b(MA - z)}$

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

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

differential dynamic logic

d$\mathcal{L}$ = FOL + DL



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

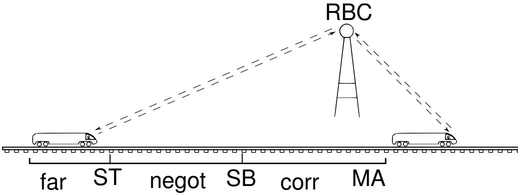
$$\forall t\, \textbf{after}(\text{train-runs}(t))(v^2 \leq 2b(MA - z))$$

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

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

differential dynamic logic

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

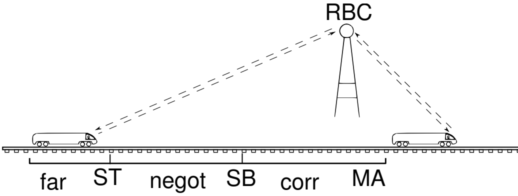


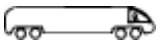
$$[\text{train-runs}]\, v^2 \leq 2b(MA - z)$$

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

differential dynamic logic

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

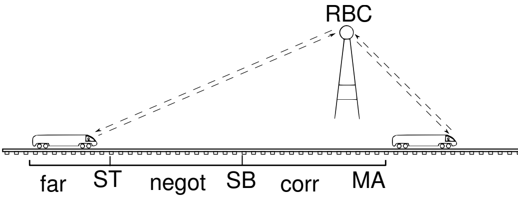


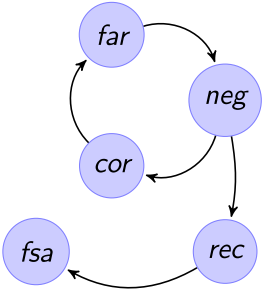
[]$v^2 \leq 2b(MA - z)$

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

differential dynamic logic

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

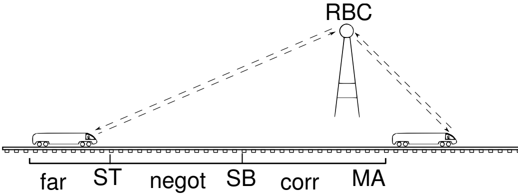


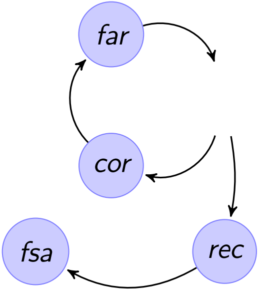


d$\mathcal{L}$ Motives: Hybrid Programs as Uniform Model

differential dynamic logic

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

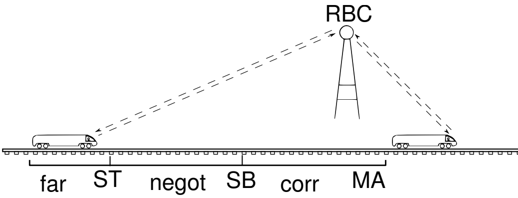


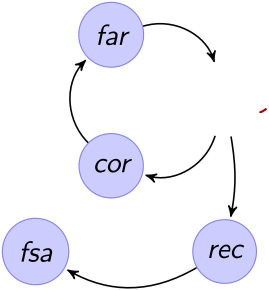


d$\mathcal{L}$ Motives: Hybrid Programs as Uniform Model

differential dynamic logic

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





not compositional

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)

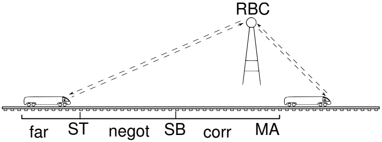
$$ETCS \equiv (cor; drive)^*$$

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

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

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

$$\& \; v \geq 0 \land \tau \leq \varepsilon$$

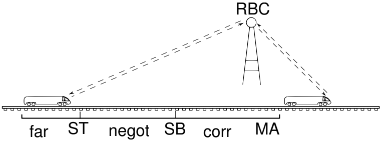


Differential Logic d$\mathcal{L}$: Syntax

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)

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



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)

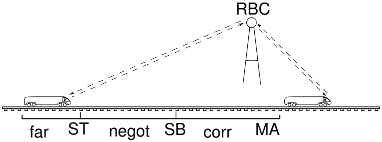
$$ETCS \equiv (cor; drive)^*$$

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

$$\cup\, (?MA - z \geq SB; a \leq a_{\mathrm{max}})$$

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

$$\&\, v \geq 0 \land \tau \leq \varepsilon$$

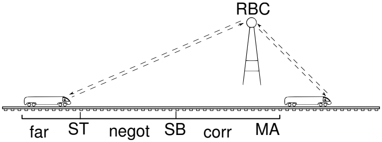


Differential Logic d$\mathcal{L}$: Syntax

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)

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

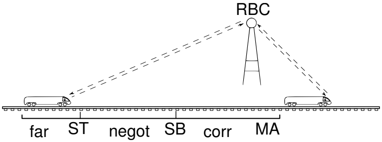


Differential Logic d$\mathcal{L}$: Syntax

Definition (Formulas ϕ)

$\neg, \wedge, \vee, \rightarrow,\ \forall x, \exists x,\ =, \leq,\ +, \cdot$ (first-order part)
$[\alpha]\phi,\ \ \langle\alpha\rangle\phi$ (dynamic part)

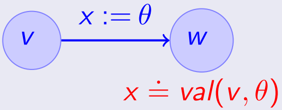
$$\psi \ \rightarrow\ [(cor\,;drive)^*]\,z \leq MA$$



All trains respect MA
$\Rightarrow$ system safe

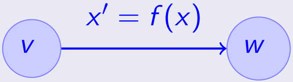
Differential Logic d$\mathcal{L}$: Transition Semantics

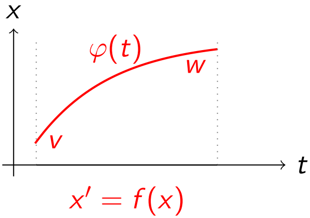
Definition (Hybrid programs α: transition semantics)



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

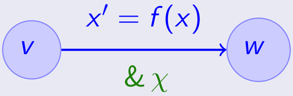
Definition (Hybrid programs α: transition semantics)

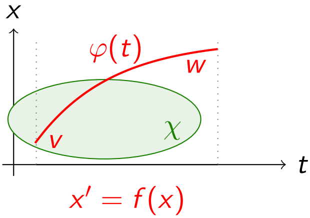




Differential Logic d$\mathcal{L}$: Transition Semantics

Definition (Hybrid programs α: transition semantics)

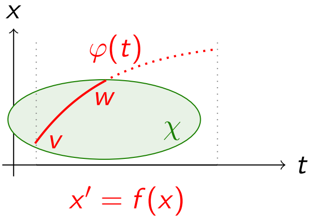




Differential Logic d$\mathcal{L}$: Transition Semantics

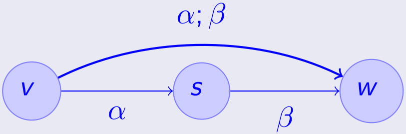
Definition (Hybrid programs α: transition semantics)

$$v \xrightarrow[\&\,\chi]{x' = f(x)} w$$



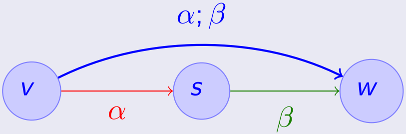
Differential Logic d$\mathcal{L}$: Transition Semantics

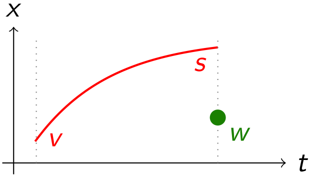
Definition (Hybrid programs α: transition semantics)



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

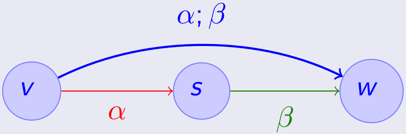
Definition (Hybrid programs α: transition semantics)

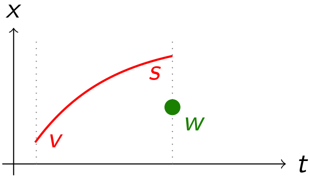




Differential Logic d$\mathcal{L}$: Transition Semantics

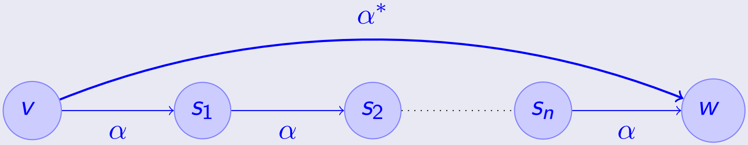
Definition (Hybrid programs α: transition semantics)





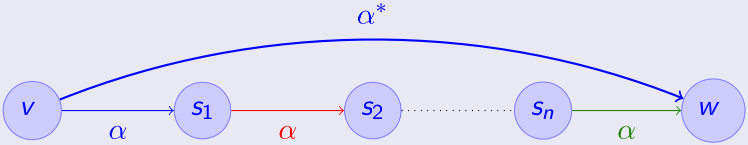
Differential Logic d$\mathcal{L}$: Transition Semantics

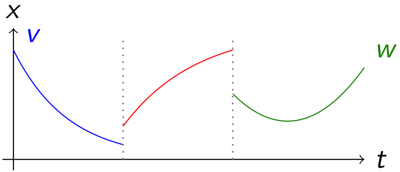
Definition (Hybrid programs α: transition semantics)



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

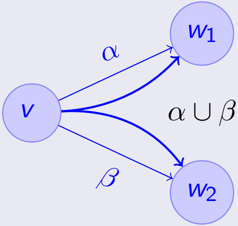
Definition (Hybrid programs α: transition semantics)





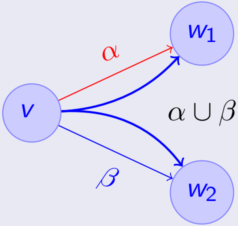
Differential Logic d$\mathcal{L}$: Transition Semantics

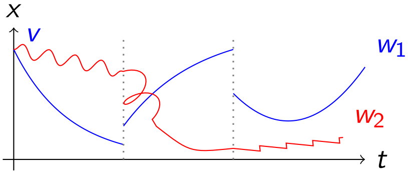
Definition (Hybrid programs α: transition semantics)



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

Definition (Hybrid programs α: transition semantics)





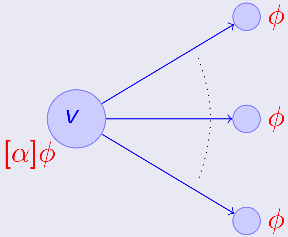
Differential Logic d$\mathcal{L}$: Transition Semantics

Definition (Hybrid programs α: transition semantics)

if $v \models \chi$

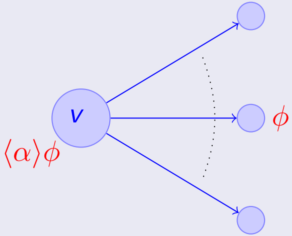
Differential Logic d$\mathcal{L}$: Transition Semantics

Definition (Formulas ϕ)



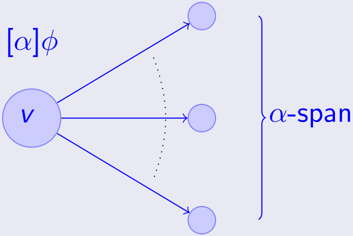
Differential Logic d$\mathcal{L}$: Transition Semantics

Definition (Formulas ϕ)



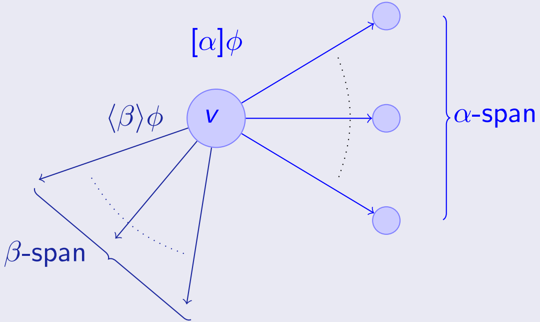
Differential Logic d$\mathcal{L}$: Transition Semantics

Definition (Formulas ϕ)



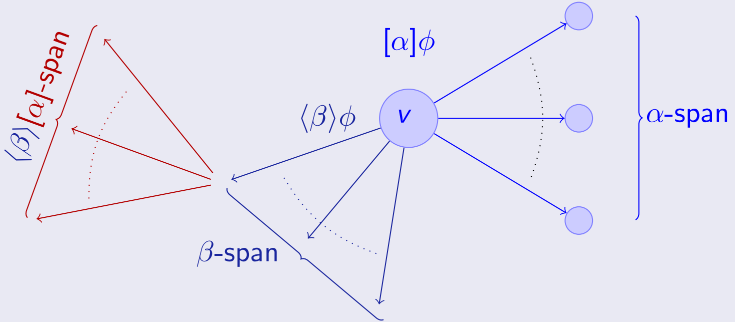
Differential Logic d$\mathcal{L}$: Transition Semantics

Definition (Formulas ϕ)



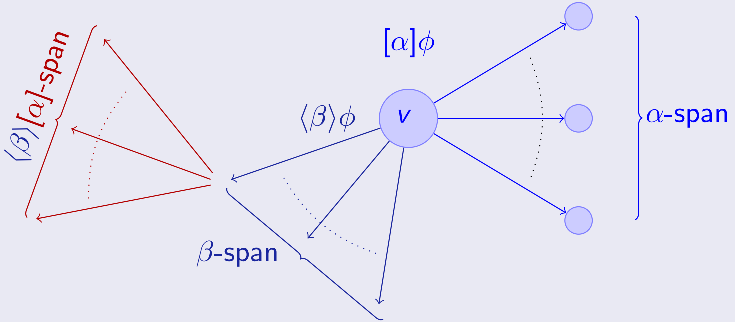
Differential Logic d$\mathcal{L}$: Transition Semantics

Definition (Formulas ϕ)



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

Definition (Formulas ϕ)



compositional semantics!

Outline

1. Motivation

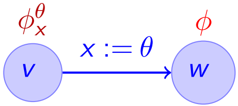
2. Differential Logic d$\mathcal{L}$
   - Design Motives
   - Syntax
   - Transition Semantics
   - Speed Supervision in Train Control

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$\mathcal{L}$

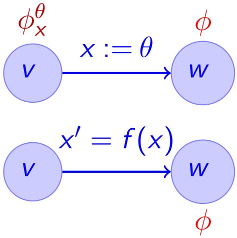
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$



Verification Calculus for d$\mathcal{L}$

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

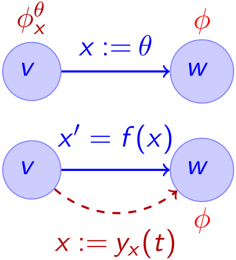
$$\frac{\exists t {\geq} 0\, \langle x := y_x(t) \rangle \phi}{\langle x' = f(x) \rangle \phi}$$



Verification Calculus for d$\mathcal{L}$

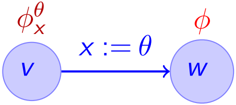
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$

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

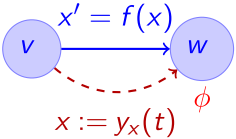


Verification Calculus for d$\mathcal{L}$

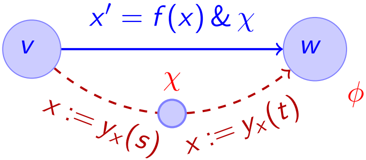
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$



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

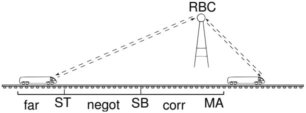


$$\frac{\exists t \geq 0\, (\bar{\chi} \land \langle x := y_x(t) \rangle \phi)}{\langle x' = f(x) \,\&\, \chi \rangle \phi}$$



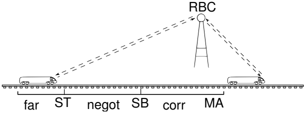
$$\bar{\chi} \;\equiv\; \forall 0 \leq s \leq t\, \langle x := y_x(s) \rangle \chi$$

Modular Combination by Side Deduction



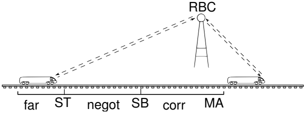
$$\vdash v > 0 \land z < MA \rightarrow \langle z' = v, v' = -b \rangle\ z \geq MA$$

Modular Combination by Side Deduction



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

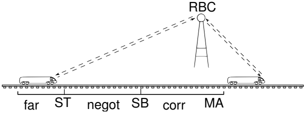
Modular Combination by Side Deduction



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

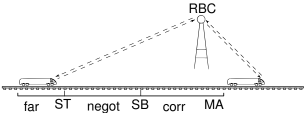


$$\frac{}{v > 0, z < MA \vdash t \geq 0 \land \langle z := -\frac{b}{2}t^2 + vt + z\rangle z \geq MA}$$

start
side

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

Modular Combination by Side Deduction

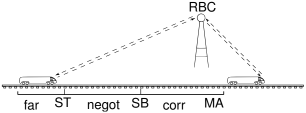


$$\dfrac{v > 0, z < MA \vdash t \geq 0 \qquad \dfrac{v > 0, z < MA \vdash -\frac{b}{2}t^2 + vt + z \geq MA}{v > 0, z < MA \vdash \langle z := -\frac{b}{2}t^2 + vt + z\rangle z \geq}}{v > 0, z < MA \vdash t \geq 0 \land \langle z := -\frac{b}{2}t^2 + vt + z\rangle z \geq MA}$$

start
side

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

Modular Combination by Side Deduction



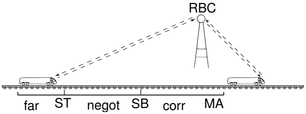
$$\dfrac{v > 0, z < MA \vdash t \geq 0 \qquad \dfrac{v > 0, z < MA \vdash -\frac{b}{2}t^2 + vt + z \geq MA}{v > 0, z < MA \vdash \langle z := -\frac{b}{2}t^2 + vt + z\rangle z \geq M}}{v > 0, z < MA \vdash t \geq 0 \land \langle z := -\frac{b}{2}t^2 + vt + z\rangle z \geq MA}$$

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



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

QE

start side

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

Verification Calculus for d$\mathcal{L}$

Dynamic Rules

11 dynamic rules

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

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

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

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

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

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

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

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

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

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

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

Verification Calculus for d$\mathcal{L}$

Propositional/Quantifier Rules

9 propositional rules + 4 quantifier rules

$$\text{(P1)}\quad \frac{\vdash \phi}{\neg\phi \vdash}$$

$$\text{(P2)}\quad \frac{\phi \vdash}{\vdash \neg\phi}$$

$$\text{(P3)}\quad \frac{\phi \vdash \psi}{\vdash \phi \rightarrow \psi}$$

$$\text{(P4)}\quad \frac{\phi, \psi \vdash}{\phi \land \psi \vdash}$$

$$\text{(P5)}\quad \frac{\vdash \phi \qquad \vdash \psi}{\vdash \phi \land \psi}$$

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

$$\text{(P7)}\quad \frac{\phi \vdash \qquad \psi \vdash}{\phi \lor \psi \vdash}$$

$$\text{(P8)}\quad \frac{\vdash \phi, \psi}{\vdash \phi \lor \psi}$$

$$\text{(P9)}\quad \frac{}{\phi \vdash \phi}$$

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

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

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

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

Verify Safety in Train Control

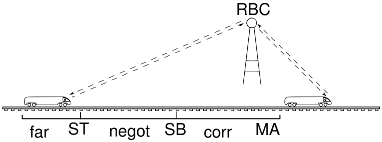
$$\psi \;\rightarrow\; [(cor\,;drive)^*]\,z \leq MA$$

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

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

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

$$\&\; v \geq 0 \wedge \tau \leq \varepsilon$$



Verify Safety in Train Control

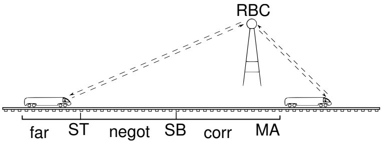
$$\psi \;\rightarrow\; [(cor\,;drive)^*]\, z \leq MA$$

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

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

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

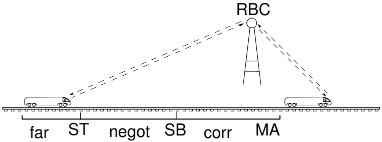
$$\&\; v \geq 0 \wedge \tau \leq \varepsilon$$



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

Verify Safety in Train Control

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



$$\ldots$$

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

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

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

$$*$$

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

$$p \vdash \forall t{\geq}0\,(\langle v := -bt + v\rangle v \geq 0 \rightarrow \langle z := -\tfrac{b}{2}t^2 + vt + z; v := -bt + v\rangle p) \qquad p, MA{-}z{\geq}SB \vdash \langle a := 0\rangle\langle \tau := 0\rangle [z' = v, v' = a, \tau$$

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

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

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

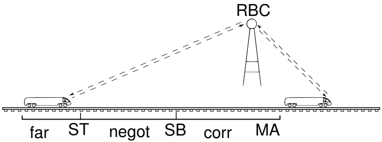
$$p \vdash [cor\,; drive]p$$

Verify Safety in Train Control

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

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

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



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

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

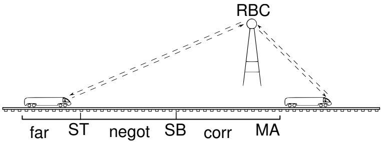
$$\begin{array}{l}
\hline
p\vdash \ [cor][drive]p \\
\hline
p\vdash \ [cor\,; drive]p
\end{array}$$

Verify Safety in Train Control

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

QE

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



$*$

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

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

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

$\ldots$

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

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

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

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

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

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

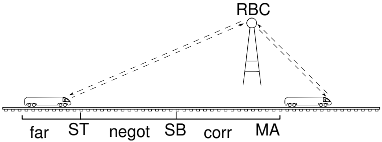
$p \vdash [?MA{-}z{\geq}SB; a := 0][drive]p$

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

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

Verify Safety in Train Control

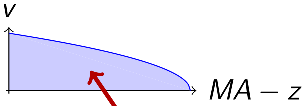
$$\boxed{\text{inv} \;\equiv\; v^2 \le 2b(MA - z)}$$



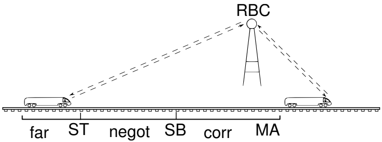
$$
\begin{array}{l}
*\\
\hline
p\vdash\ \forall t{\ge}0\,(\langle v := -bt + v\rangle v \ge 0 \to \langle z := -\tfrac{b}{2}t^2 + vt + z; v := -bt + v\rangle p)\\
\hline
p\vdash\ [z' = v, v' = -b \,\&\, v \ge 0]p\\
\hline
p\vdash\ \langle a := -b\rangle[drive]p
\end{array}
\qquad
\begin{array}{l}
\quad\dots\\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

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

Verify Safety in Train Control



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



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

$$\cdots$$

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

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

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

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

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

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

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

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

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

Verified ETCS Model

system : $\big(\mathrm{poll};\ (\mathrm{negot} \cup (\mathrm{speedControl};\ \mathrm{atp};\ \mathrm{move}))\big)^*$

init : $drive := 0;\ brake := 1$

poll : $SB := \frac{v^2-d^2}{2b} + \left(\frac{a_{max}}{b} + 1\right)\left(\frac{a_{max}}{2}\varepsilon^2 + \varepsilon v\right);\ ST := *$

negot : $(?m - z > ST) \cup (?m - z \leq ST;\ \mathrm{rbc})$

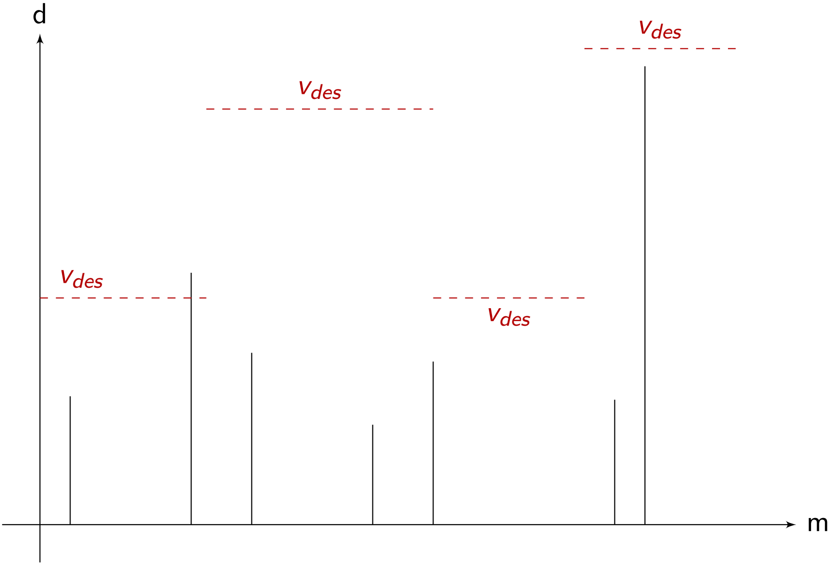
rbc : $(vdes := *;\ ?vdes > 0) \cup (state := brake)$
$\cup\ \big(d_{old} := d;\ m_{old} := m;\ m := *;\ d := *;$
$?d \geq 0 \wedge d_{old}^2 - d^2 \leq 2b(m - m_{old})\big)$

speedCtrl : $(?state = brake;\ a := -b)$
$\cup\Big(?state = drive;$
$\big((?v \leq v_{des};\ a := *;\ ? - b \leq a \leq a_{max})$
$\cup(?v \geq v_{des};\ a := *;\ ?0 > a \geq\ - b)\big)\Big)$

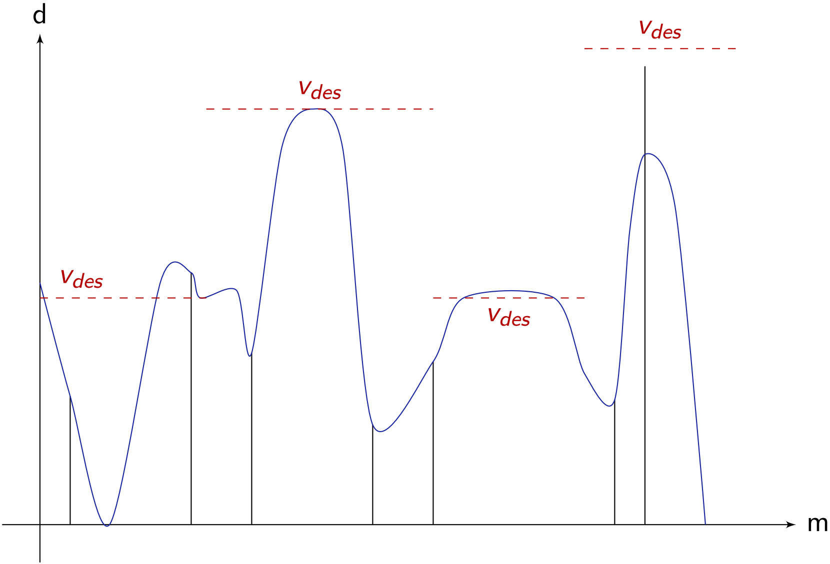
atp : $(?m - z \leq SB;\ a := -b) \cup (?m - z > SB)$

move : $t := 0;\ \{\dot{z} = v, \dot{v} = a, \dot{t} = 1, (v \geq 0 \wedge t \leq \varepsilon)\}$

Distance Profile



Distance Profile



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 not semidecidable)

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

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

Outline

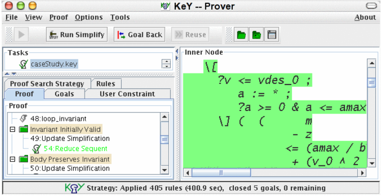
1. Motivation
2. Differential Logic d$\mathcal{L}$
   - Design Motives
   - Syntax
   - Transition Semantics
   - Speed Supervision in Train Control
3. Verification Calculus for d$\mathcal{L}$
   - Sequent Calculus
   - Modular Combination by Side Deduction
   - Verifying Speed Supervision in Train Control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

Conclusions

differential dynamic logic

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

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



48:loop_invariant
Invariant Initially Valid
49:Update Simplification
54:Reduce Sequent
Body Preserves Invariant
50:Update Simplification

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

Strategy: Applied 405 rules (400.9 sec), closed 5 goals, 0 remaining

Future Work

- Prove relative completeness of $\mathrm{d}\mathcal{L}/(\mathsf{ODE}+\mathsf{Inv})$
- Dynamic reconfiguration of system structures

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.