

Differential Dynamic Logic for Hybrid Systems

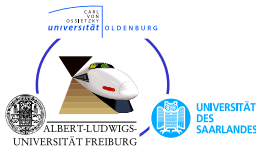
André Platzer^{1,2}

¹University of Oldenburg, Department of Computing Science, Germany

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

KeY'07

Carnegie Mellon.



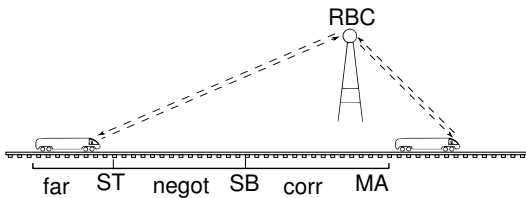
DAAD
Deutscher Akademischer Austausch Dienst
German Academic Exchange Service

Deutsche
Forschungsgemeinschaft
DFG

- 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

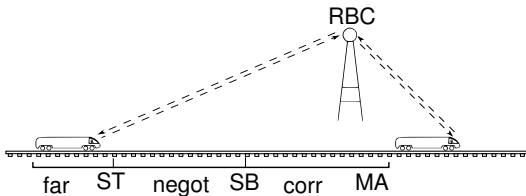


Verifying Parametric Hybrid Systems



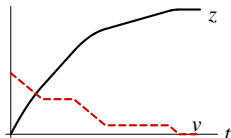


Verifying Parametric Hybrid Systems



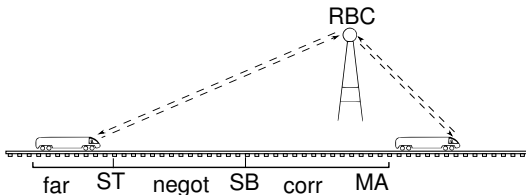
Hybrid Systems

continuous evolution along differential equations + discrete change





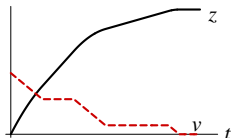
Verifying Parametric Hybrid Systems



Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

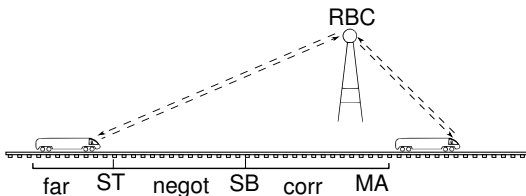
- Fix parameter $SB = 10000$ and hope?
- Handle SB as free symbolic parameter?
- Which constraints for SB ?



$$\forall MA \exists SB [Train]_{\text{safe}}$$



Verifying Parametric Hybrid Systems



Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

differential dynamic logic

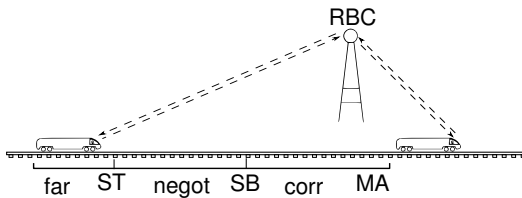
$$d\mathcal{L} = DL + HP$$

- 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

- 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

differential dynamic logic

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

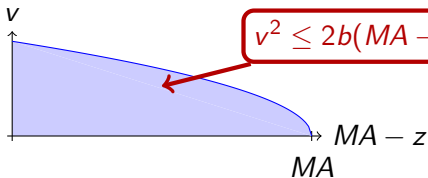
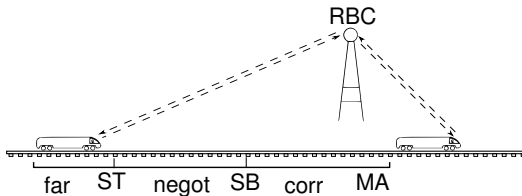




dL Motives: Regions in First-order Logic

differential dynamic logic

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

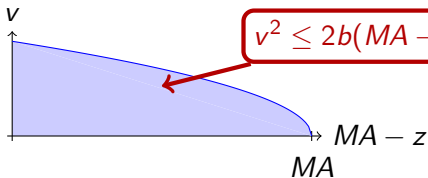
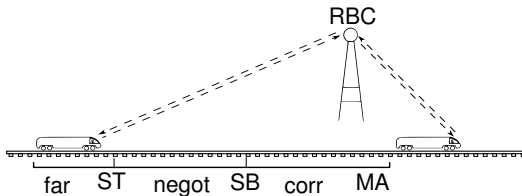




dL Motives: Regions in First-order Logic

differential dynamic logic

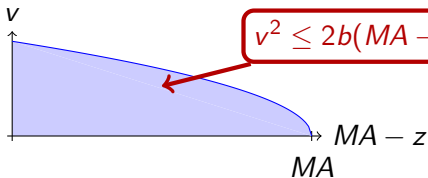
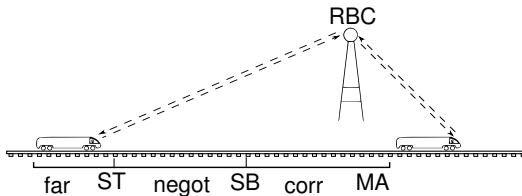
$$d\mathcal{L} = \text{FOL}$$



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

differential dynamic logic

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

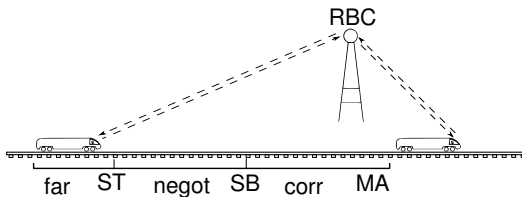


$$\forall t \text{ after}(\text{train-runs}(t))(v^2 \leq 2b(MA - z))$$

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

differential dynamic logic

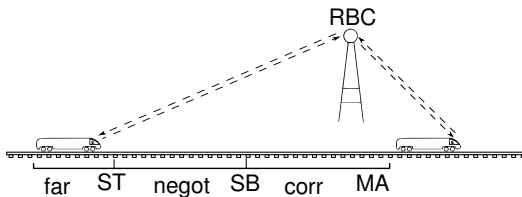
$$d\mathcal{L} = \text{FOL} + \text{DL} + \text{HP}$$



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

differential dynamic logic

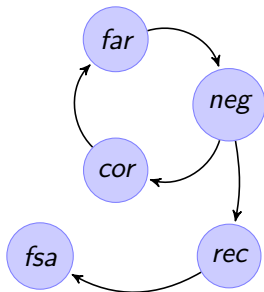
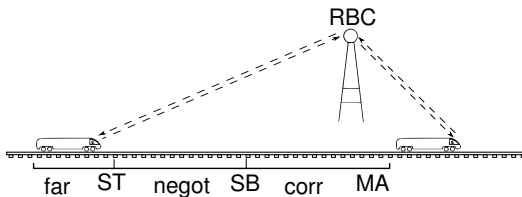
$$d\mathcal{L} = \text{FOL} + \text{DL} + \text{HP}$$



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

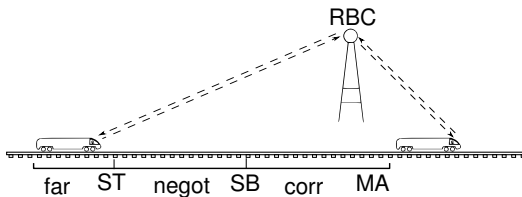
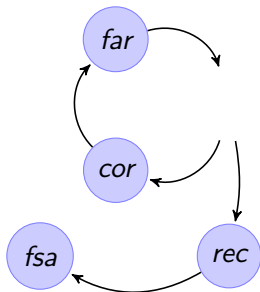
differential dynamic logic

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



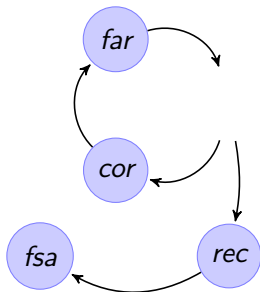
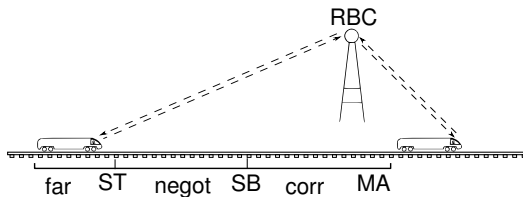
differential dynamic logic

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



differential dynamic logic

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



not compositional



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)	

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)	

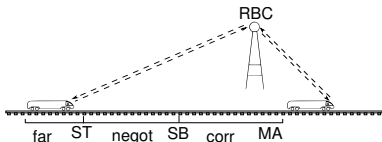
$$ETCS \equiv (cor, drive)^*$$

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

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

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

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



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)	

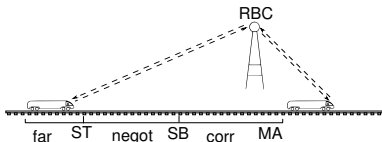
$ETCS \equiv (cor, drive)^*$

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

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

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

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



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)	

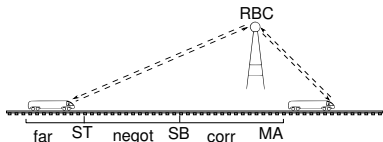
$ETCS \equiv (cor, drive)^*$

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

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

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

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



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)

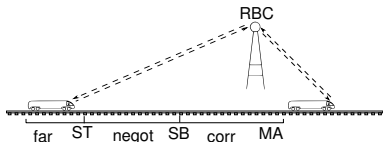
$ETCS \equiv (cor, drive)^*$

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

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

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

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



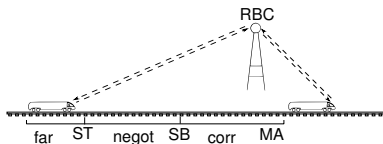
Definition (Formulas ϕ)

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

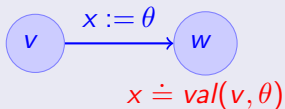
$$\psi \rightarrow [(cor; drive)^*] z \leq MA$$

All trains respect MA

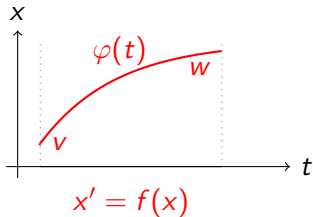
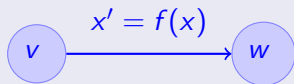
\Rightarrow system safe



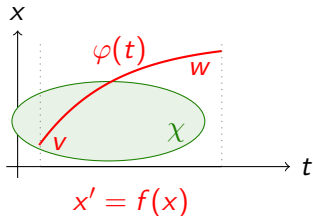
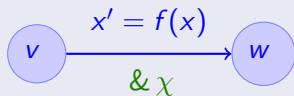
Definition (Hybrid programs α : transition semantics)



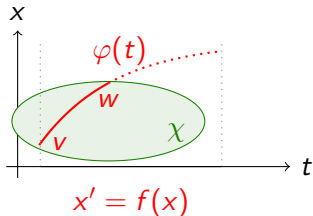
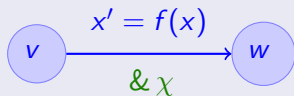
Definition (Hybrid programs α : transition semantics)



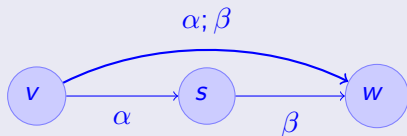
Definition (Hybrid programs α : transition semantics)



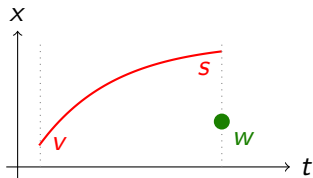
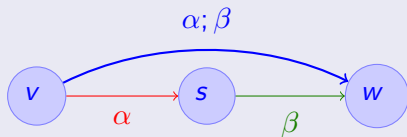
Definition (Hybrid programs α : transition semantics)



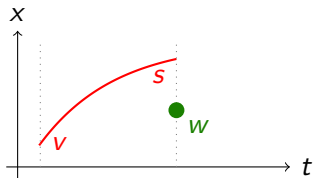
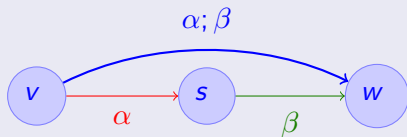
Definition (Hybrid programs α : transition semantics)



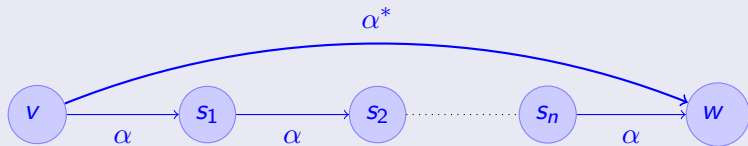
Definition (Hybrid programs $\alpha; \beta$: transition semantics)



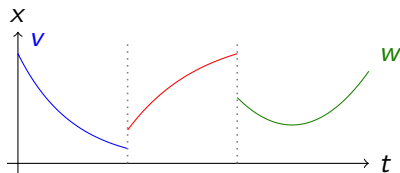
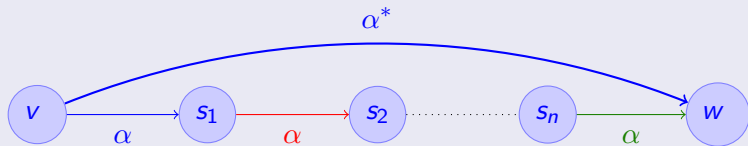
Definition (Hybrid programs $\alpha; \beta$: transition semantics)



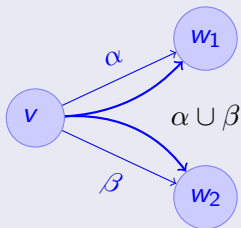
Definition (Hybrid programs α : transition semantics)



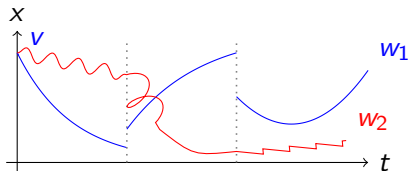
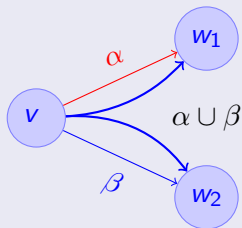
Definition (Hybrid programs α : transition semantics)



Definition (Hybrid programs α : transition semantics)



Definition (Hybrid programs α : transition semantics)

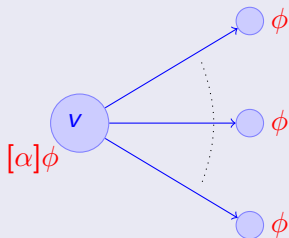


Definition (Hybrid programs α : transition semantics)

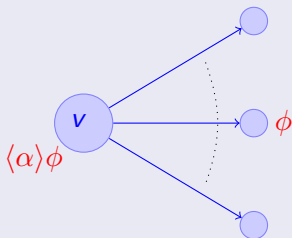


if $v \models \chi$

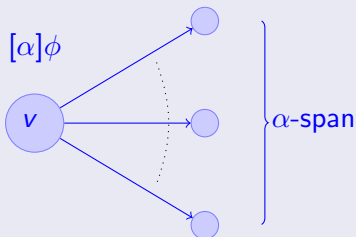
Definition (Formulas ϕ)



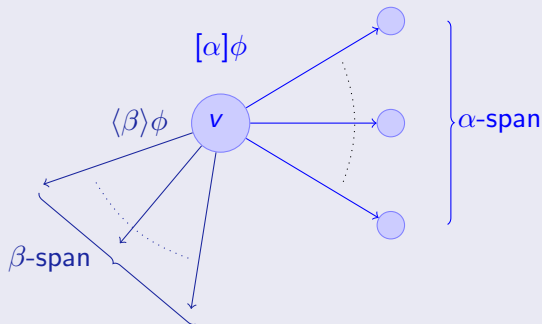
Definition (Formulas ϕ)



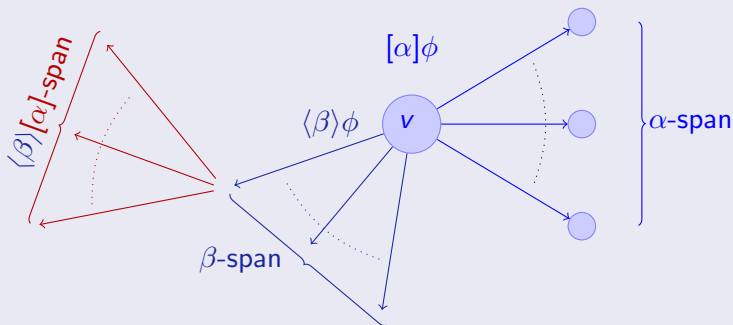
Definition (Formulas ϕ)



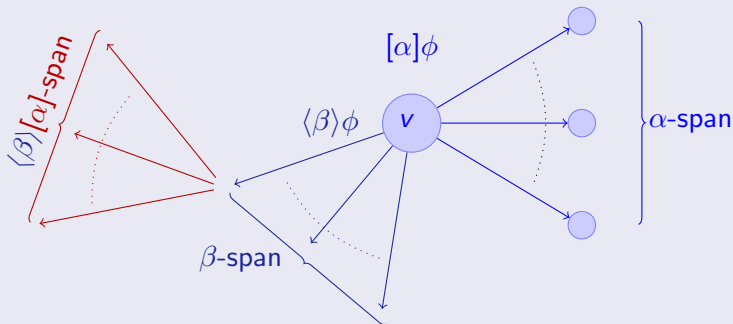
Definition (Formulas ϕ)



Definition (Formulas ϕ)



Definition (Formulas ϕ)

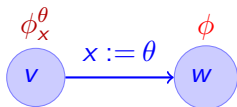


compositional semantics!

- 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



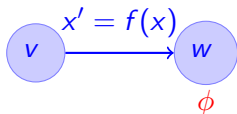
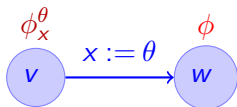
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$





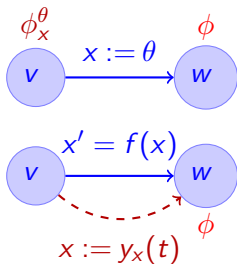
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$

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



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

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

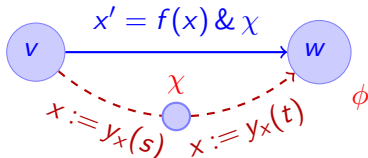
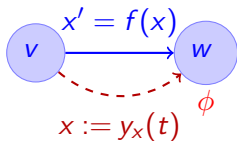
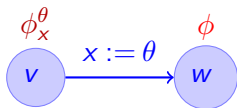


$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$

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

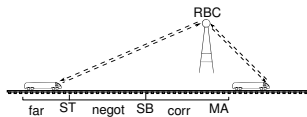
$$\frac{\exists t \geq 0 (\bar{\chi} \wedge \langle x := y_x(t) \rangle \phi)}{\langle x' = f(x) \& \chi \rangle \phi}$$

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





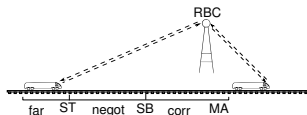
Modular Combination by Side Deduction



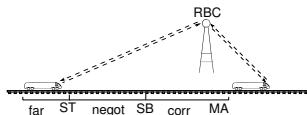
$$\vdash v > 0 \wedge z < MA \rightarrow \langle z' = v, v' = -b \rangle z \geq MA$$



Modular Combination by Side Deduction

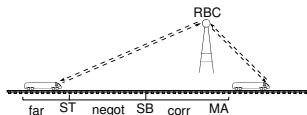


$$\frac{\frac{v > 0, z < MA \vdash \exists t \geq 0 \langle z := -\frac{b}{2}t^2 + vt + z \rangle z \geq MA}{v > 0, z < MA \vdash \langle z' = v, v' = -b \rangle z \geq MA}}{\vdash v > 0 \wedge z < MA \rightarrow \langle z' = v, v' = -b \rangle z \geq MA}$$



QE not applicable!

$$\begin{array}{c}
 \hline
 v > 0, z < MA \vdash \exists t \geq 0 \langle z := -\frac{b}{2}t^2 + vt + z \rangle z \geq MA \\
 \hline
 v > 0, z < MA \vdash \langle z' = v, v' = -b \rangle z \geq MA \\
 \hline
 \vdash v > 0 \wedge z < MA \rightarrow \langle z' = v, v' = -b \rangle z \geq MA
 \end{array}$$



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

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

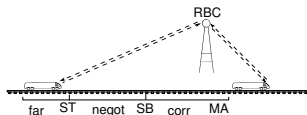
$$\frac{}{v > 0, z < MA \vdash \langle z' = v, v' = -b \rangle z \geq MA}$$

$$\frac{}{\vdash v > 0 \wedge z < MA \rightarrow \langle z' = v, v' = -b \rangle z \geq MA}$$

↑
start
side



Modular Combination by Side Deduction



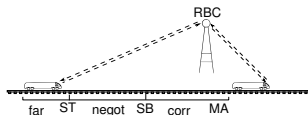
$$\frac{v > 0, z < MA \vdash t \geq 0 \quad \frac{v > 0, z < MA \vdash -\frac{b}{2}t^2 + vt + z \geq MA}{v > 0, z < MA \vdash \langle z := -\frac{b}{2}t^2 + vt + z \rangle z \geq MA}}{v > 0, z < MA \vdash t \geq 0 \wedge \langle z := -\frac{b}{2}t^2 + vt + z \rangle z \geq MA}$$

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

start
side



Modular Combination by Side Deduction



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

$$v > 0, z < MA \vdash v^2 \geq 2b(MA - z)$$

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

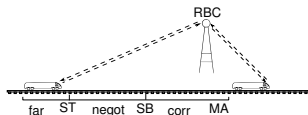
$$v > 0, z < MA \vdash \langle z' = v, v' = -b \rangle z \geq MA$$

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

start
side



Modular Combination by Side Deduction



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

$$v > 0, z < MA \vdash v^2 \geq 2b(MA - z)$$

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

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

$$\frac{v > 0, z < MA \vdash \langle z' = v, v' = -b \rangle z \geq MA}{\vdash v > 0 \wedge z < MA \rightarrow \langle z' = v, v' = -b \rangle z \geq MA}$$

start
side

11 dynamic rules

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

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

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

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

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

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

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

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

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

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

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

9 propositional rules + 4 quantifier rules

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

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

$$(P7) \quad \frac{\phi \vdash \quad \psi \vdash}{\phi \vee \psi \vdash}$$

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

$$(P5) \quad \frac{\vdash \phi \quad \vdash \psi}{\vdash \phi \wedge \psi}$$

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

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

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

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

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

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

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

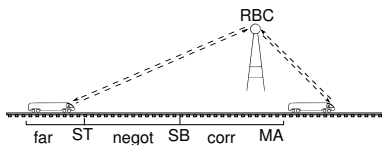
$$(F4) \quad \frac{\text{QE}(\exists x \bigwedge_i (\Gamma_i \vdash \Delta_i))}{\Gamma, \forall x \phi \vdash \Delta}$$

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

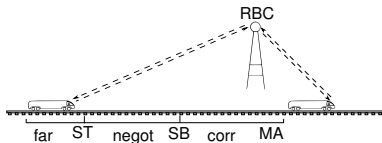
$$cor \equiv (?MA - z < SB; a := -b)$$

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

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

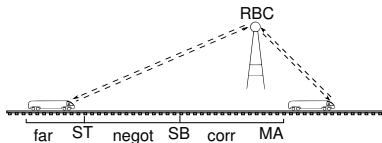
$$\& v \geq 0 \wedge \tau \leq \varepsilon$$


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



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

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

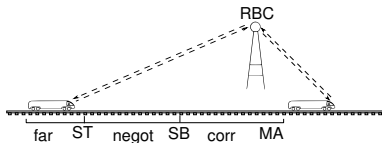


*	$p \vdash \forall t \geq 0 (\langle v := -bt + v \rangle v \geq 0 \rightarrow \langle z := -\frac{b}{2}t^2 + vt + z; v := -bt + v \rangle p)$...
$p \vdash [z' = v, v' = -b \ \& \ v \geq 0] p$	$p, MA - z \geq SB \vdash \langle \tau := 0 \rangle \forall t \geq 0 (\langle \tau := t \rangle \tau \leq \varepsilon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

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

↑ QE

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



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

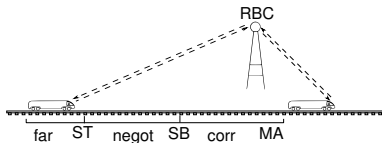


Verify Safety in Train Control

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

QE

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

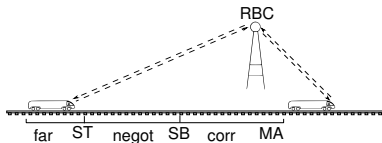


$p, MA - z \geq SB \vdash \tau \leq 2b(MA - \varepsilon v - z)$
$p, MA - z \geq SB \vdash \forall t \geq 0 ((\tau := t) \tau \leq \varepsilon \Rightarrow \langle z := vt \rangle p)$
$p, MA - z \geq SB \vdash \langle \tau := 0 \rangle \forall t \geq 0 ((\tau := t + \tau) \tau \leq \varepsilon \Rightarrow p)$
$p, MA - z \geq SB \vdash \langle \tau := 0 \rangle \langle z' = v, v' = 0, \tau' = 1 \& \tau \leq \varepsilon \rangle p$
$p, MA - z \geq SB \vdash \langle a := 0 \rangle \langle \tau := 0 \rangle \langle z' = v, v' = a, \tau \leq \varepsilon \rangle p$
$p, MA - z \geq SB \vdash \langle a := 0 \rangle [drive] p$
$p \vdash [?MA - z \geq SB; a := 0] [drive] p$
$p \vdash [cor] [drive] p$
$p \vdash [cor; drive] p$

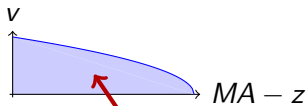
*

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

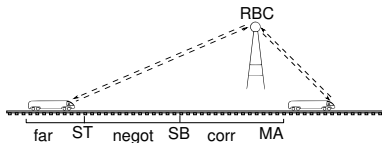
$$\text{inv} \equiv v^2 \leq 2b(MA - z)$$



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



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

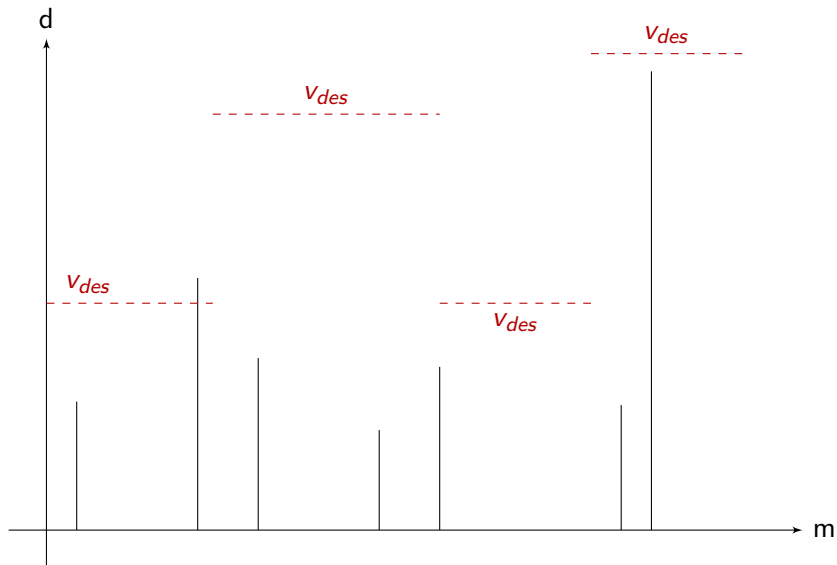


*	$p \vdash \forall t \geq 0 (\langle v := -bt + v \rangle v \geq 0 \rightarrow \langle z := -\frac{b}{2}t^2 + vt + z; v := -bt + v \rangle p)$...
$p \vdash [z' = v, v' = -b \ \& \ v \geq 0] p$	$p, MA - z \geq SB \vdash \forall t \geq 0 (\langle \tau := t \rangle \tau \leq \epsilon \rightarrow \langle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

system : $(\text{poll}; (\text{negot} \cup (\text{speedControl}; \text{atp}; \text{move})))^*$
 init : $\text{drive} := 0; \text{brake} := 1$
 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 : $(?m - z > ST) \cup (?m - z \leq ST; \text{rbc})$
 rbc : $(v_{des} := *; ?v_{des} > 0) \cup (\text{state} := \text{brake})$
 $\cup (d_{old} := d; m_{old} := m; m := *; d := *;$
 $?d \geq 0 \wedge d_{old}^2 - d^2 \leq 2b(m - m_{old}))$
 speedCtrl : $(?state = \text{brake}; a := -b)$
 $\cup \left(?state = \text{drive}; \right.$
 $\left. \left((?v \leq v_{des}; a := *; ?-b \leq a \leq a_{\max}) \right. \right.$
 $\left. \left. \cup (?v \geq v_{des}; a := *; ?0 > a \geq -b) \right) \right)$
 atp : $(?m - z \leq SB; a := -b) \cup (?m - z > SB)$
 move : $t := 0; \{\dot{z} = v, \dot{v} = a, \dot{t} = 1, (v \geq 0 \wedge t \leq \varepsilon)\}$

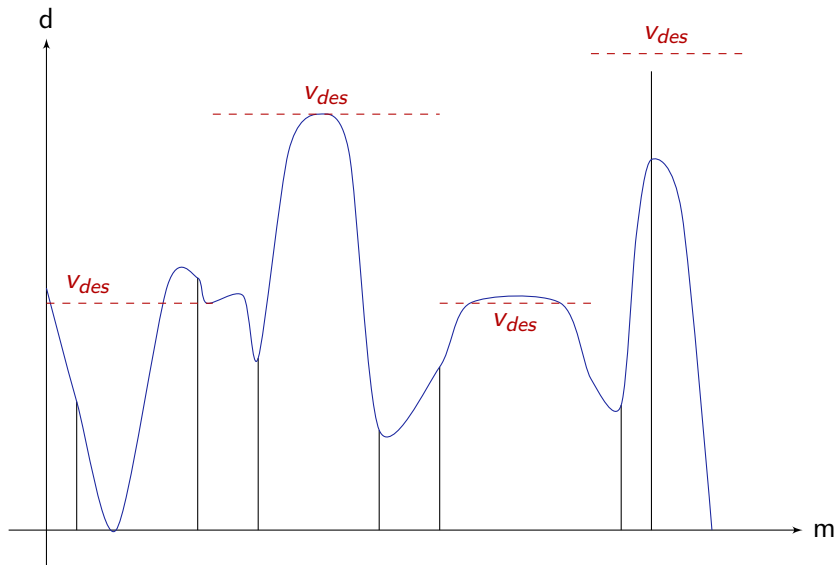


Distance Profile





Distance Profile



Theorem (Soundness)

dL calculus is sound.

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

Proposition (Incompleteness)

*The discrete or continuous fragments of dL are inherently incomplete.
(Yet, reachability in hybrid systems is not semidecidable)*

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

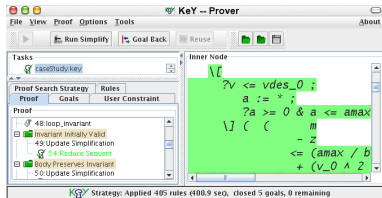
$$\langle s'' = -s, \tau' = 1 \rangle (s = 0 \wedge \tau = n) \quad \rightsquigarrow s = \sin$$

- 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

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



- Prove relative completeness of $d\mathcal{L}/(\text{ODE} + \text{Inv})$
- 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.