Differential Dynamic Logic for Verifying Parametric Hybrid Systems
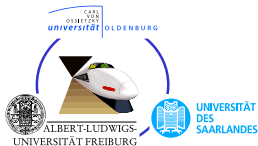
André Platzer[1,2]

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

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

Tableaux'07

Outline

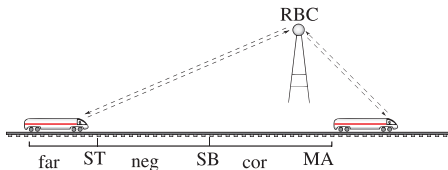# Verifying Parametric Hybrid Systems

Hybrid Systems

continuous evolution along differential equations + discrete change

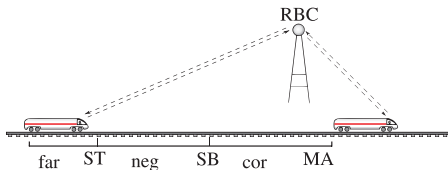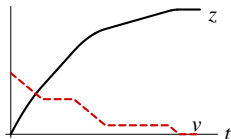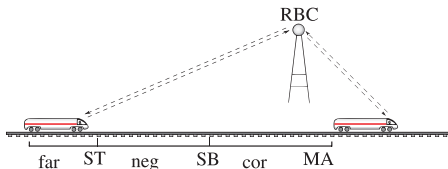# Verifying Parametric Hybrid Systems

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?

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

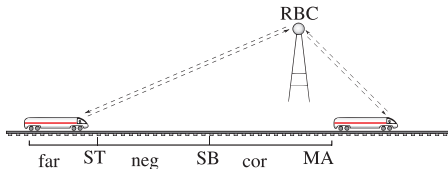**Parametric Hybrid Systems**

continuous evolution along differential equations + discrete change

differential dynamic logic

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

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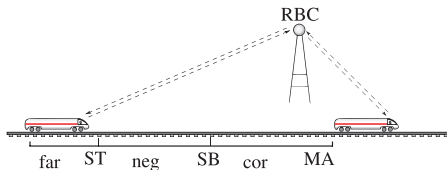An extended duration calculus for hybrid real-time systems.
In R. L. Grossman, A. Nerode, A. P. Ravn, and H. Rischel, editors, *Hybrid Systems*, volume 736 of *LNCS*, pages 36–59. Springer, 1992.

Outline

Outline

differential dynamic logic

dℒ = DL + HP

differential dynamic logic

$$d\mathcal{L} = FOL_{\mathbf{R}}$$

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

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

differential dynamic logic
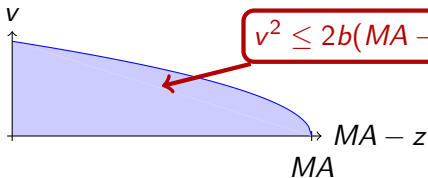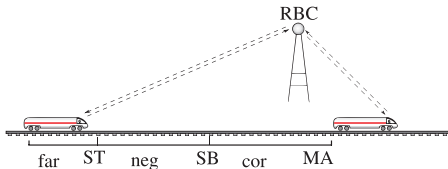
$$d\mathcal{L} = FOL_R + DL$$

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

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

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

differential dynamic logic

$d\mathcal{L} = FOL_{\mathbf{R}} + DL + HP$

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

differential dynamic logic

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

$$[\begin{smallmatrix}\fbox{}\end{smallmatrix}]v^2 \leq 2b(MA - z)$$

differential dynamic logic

$$d\mathcal{L} = FOL_{\mathbf{R}} + DL + HP$$

differential dynamic logic

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

differential dynamic logic

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

not compositional

far

cor

fsa

rec

neg

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)

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

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)

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

Definition (Hybrid program α)

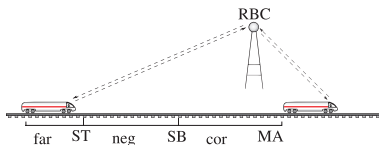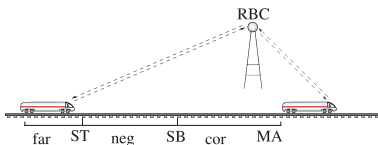|	
$x' = f(x)$	(continuous evolution)
$x := \theta$	(discrete jump)
$?\chi$	(conditional execution)
$\alpha; \beta$	(seq. composition)
$\alpha \cup \beta$	(nondet. choice)
α^*	(nondet. repetition)

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

Definition (Hybrid program α)

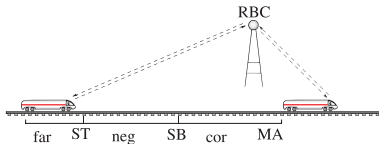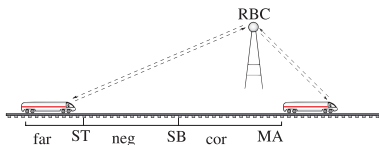|	
$x' = f(x) \,\&\, \chi$	(continuous evolution within invariant region)
$x := \theta$	(discrete jump)
$?\chi$	(conditional execution)
$\alpha; \beta$	(seq. composition)
$\alpha \cup \beta$	(nondet. choice)
α^*	(nondet. repetition)

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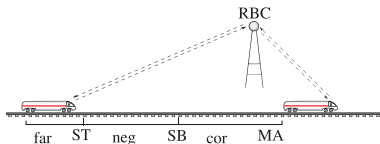$$\&\ v \geq 0 \wedge \tau \leq \varepsilon$$

Definition (Formulas ϕ)

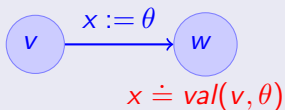|	
$\neg, \wedge, \vee, \rightarrow, \; \forall x, \exists x, \; =, \leq, +, \cdot$	(**R**-first-order part)
$[\alpha]\phi, \quad \langle\alpha\rangle\phi$	(dynamic part)

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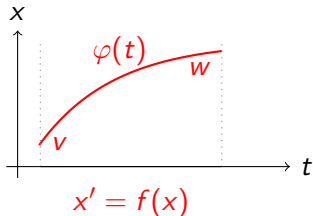

All trains respect MA
$\Rightarrow$ system safe
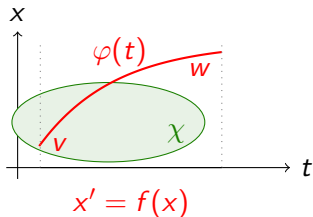
Differential Logic dℒ: Transition Semantics

Definition (Hybrid programs α: transition semantics)

Definition (Hybrid programs α: 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 dℒ: Transition Semantics

Definition (Hybrid programs α: 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)

Definition (Hybrid programs α: transition semantics)

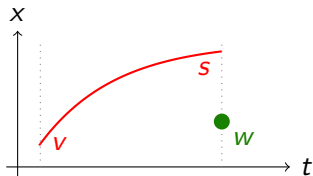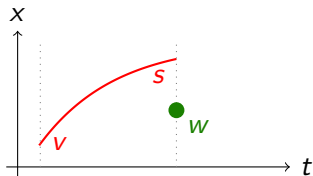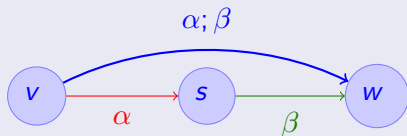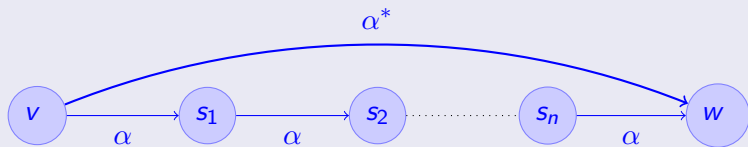# Differential Logic dℒ: Transition Semantics

Definition (Hybrid programs α: transition semantics)

Definition (Hybrid programs α: transition semantics)

$?\chi$

v

if $v \models \chi$

Definition (Formulas ϕ)

Definition (Formulas ϕ)

Definition (Formulas ϕ)

Differential Logic dℒ: Transition Semantics

Definition (Formulas ϕ)

Definition (Formulas ϕ)

Definition (Formulas ϕ)

compositional semantics!

Outline

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

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

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

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

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

Differential Analyser for Solving Differential Equations
invented 1876
built 1927

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

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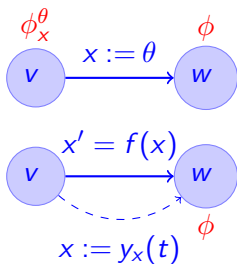
$$\frac{\phi_x^\theta}{\langle x := \theta \rangle \phi}$$

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

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

$$\bar{\chi} \;\equiv\; \forall 0 {\leq} s {\leq} t \, \langle x := y_x(s) \rangle \chi$$
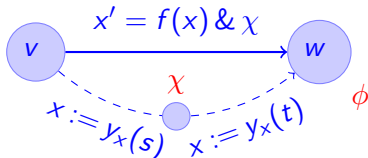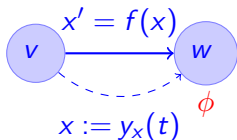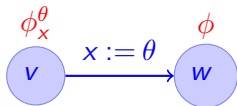
compositional semantics $\Rightarrow$ other rules as usual!
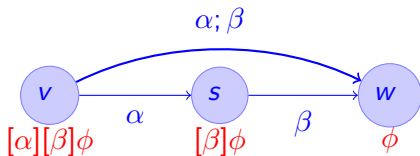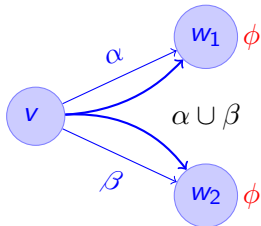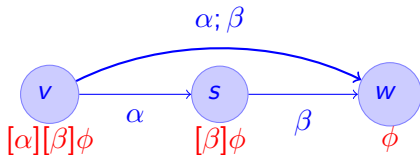
$$\frac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha \cup \beta]\phi}$$

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

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

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

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

$$\frac{\vdash p \quad \vdash (p \rightarrow [\alpha]p)}{\vdash [\alpha^*]p}$$
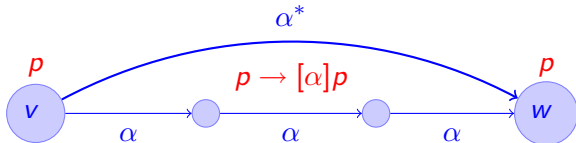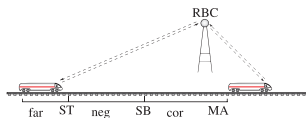
$$\vdash v > 0 \land z < MA \rightarrow \langle z' = v, v' = -b \rangle \ z \geq MA$$

Modular Combination by Side Deduction
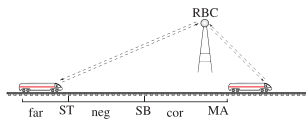
$$\frac{v > 0, z < MA \vdash \exists t{\geq}0 \; \langle z := -\frac{b}{2}t^2 + vt + z \rangle z \geq MA}{v > 0, z < MA \vdash \langle z' = v, v' = -b \rangle z \geq MA}$$
$$\overline{\qquad \vdash v > 0 \wedge z < MA \rightarrow \langle z' = v, v' = -b \rangle \; z \geq MA}$$

QE not applicable!

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

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

Modular Combination by Side Deduction

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

start side

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

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

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

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

start side

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

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

start
side

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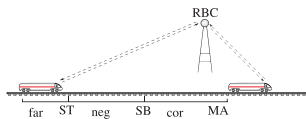{\vdash v > 0 \wedge z < MA \rightarrow \langle z' = v, v' = -b\rangle z \geq MA}
}{}$$

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

QE

start
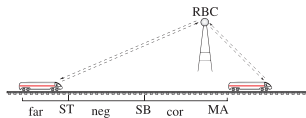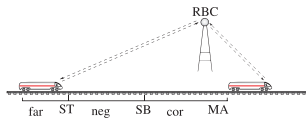side

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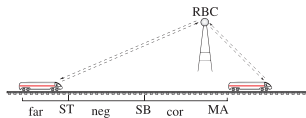 > 0, z < MA \vdash \langle z' = v, v' = -b \rangle z \geq MA}}{\vdash v > 0 \wedge z < MA \to \langle z' = v, v' = -b \rangle \, z \geq MA}$$

11 dynamic rules

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

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

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

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

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

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

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

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

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

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

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

9 propositional rules + 4 quantifier rules

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

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

(P3) $\dfrac{\phi \vdash \psi}{\vdash \phi \rightarrow \psi}$ (P6) $\dfrac{\vdash \phi \qquad \psi \vdash}{\phi \rightarrow \psi \vdash}$ (P9) $\dfrac{}{\phi \vdash \phi}$
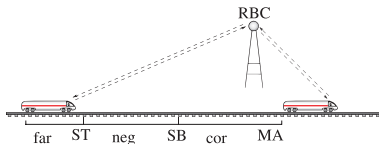
(F1) $\dfrac{\mathrm{QE}(\exists x \, \bigwedge_i (\Gamma_i \vdash \Delta_i))}{\Gamma \vdash \Delta, \exists x\, \phi}$ (F3) $\dfrac{\mathrm{QE}(\forall x \, \bigwedge_i (\Gamma_i \vdash \Delta_i))}{\Gamma \vdash \Delta, \forall x\, \phi}$

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

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

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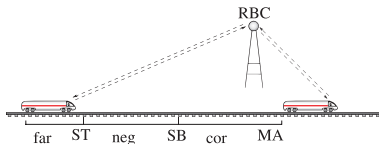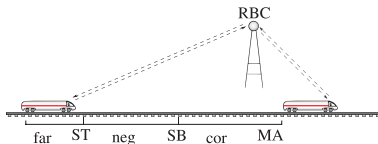$$\&\; v \ge 0 \wedge \tau \le \varepsilon$$

$$\frac{\cdots}{p,\,MA-z\ge SB \vdash v^2 \le 2b(MA - \varepsilon v - z)}$$
$$p,\,MA-z\ge SB \vdash \forall t\ge 0\,(\langle\tau := t\rangle \tau \le \varepsilon \rightarrow \langle z := vt\rangle$$
$$p,\,MA-z\ge SB \vdash \langle\tau := 0\rangle \forall t\ge 0\,(\langle\tau := t + \tau\rangle \tau \le \varepsilon$$
$$p,\,MA-z\ge SB \vdash \langle\tau := 0\rangle[z' = v, v' = 0, \tau' = 1\,\&$$

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

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

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

QE

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

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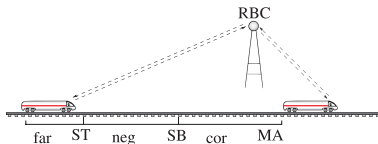\end{array}
$$

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

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

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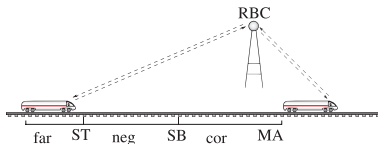
RBC

far ST neg SB cor MA

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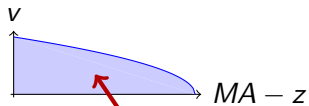$$p, MA-z \ge SB \vdash\; \langle a := 0\rangle [drive]p$$

$$*$$
$$\overline{p \vdash\; \forall t \ge 0\,(\langle v := -bt + v\rangle v \ge 0 \to \langle z := -\tfrac{b}{2} t^2 + vt + z;\, v := -bt + v\rangle p)}$$
$$p \vdash\; [z' = v,\, v' = -b\,\&\, v \ge 0]p$$
$$p \vdash\; \langle a := -b\rangle [drive]p$$
$$\qquad\qquad\qquad\qquad p \vdash\; [?MA-z \ge SB;\, a := 0][drive]p$$

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

Theorem (Soundness)

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

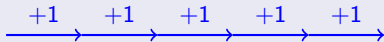- $x' = f(x)$
- Side deductions

Proposition (Incompleteness)

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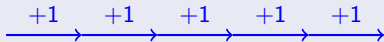(Yet, reachability in hybrid systems is undecidable)
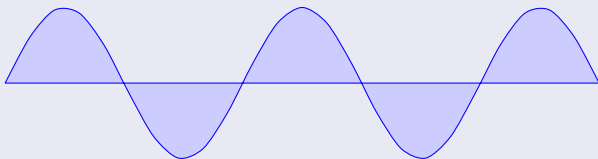
Proof

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

Proof

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

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

Verified ETCS Model

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

Outline

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

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