A Temporal Dynamic Logic for Verifying Hybrid System Invariants

André Platzer[1,2]

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

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

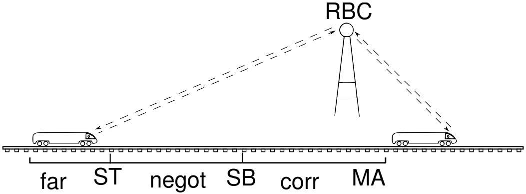
LFCS'07

Carl von Ossietzky universität Oldenburg
Albert-Ludwigs-Universität Freiburg
Universität des Saarlandes
Carnegie Mellon
DAAD Deutscher Akademischer Austausch Dienst
German Academic Exchange Service
Deutsche Forschungsgemeinschaft DFG

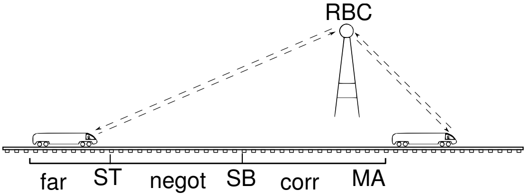
Outline

1. Motivation
2. Temporal Dynamic Logic dTL
    - Syntax
    - Trace Semantics
    - Conservative Extension
    - Safety Invariants in Train Control
3. Verification Calculus for dTL
    - Sequent Calculus
    - Verifying Safety Invariants in Train Control
    - Soundness
4. Conclusions & Future Work

Verifying Hybrid Systems



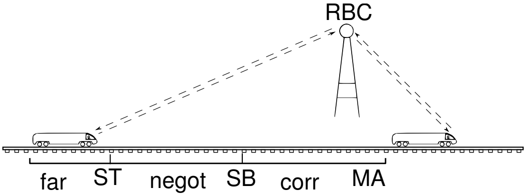
Verifying Hybrid Systems



Hybrid Systems

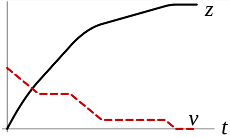
continuous evolution along differential equations + discrete change

Verifying Hybrid Systems

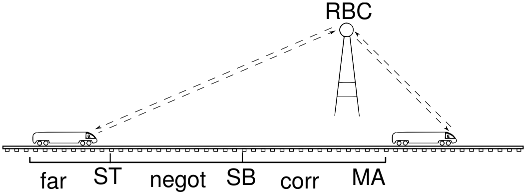


Hybrid Systems

continuous evolution along differential equations + discrete change

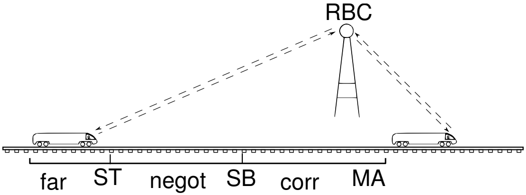


Verifying Hybrid Systems



problem	technique	OP	PAR	T	closed
$ETCS \models z < MA$	TL-MC	✓	×	✓	×

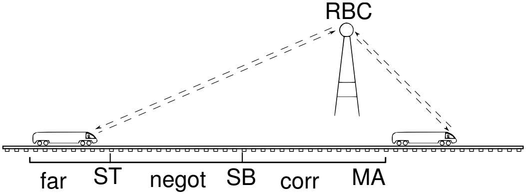
Verifying Hybrid Systems



problem	technique	OP	PAR	T	closed
$ETCS \models z < MA$	TL-MC	✓	×	✓	×

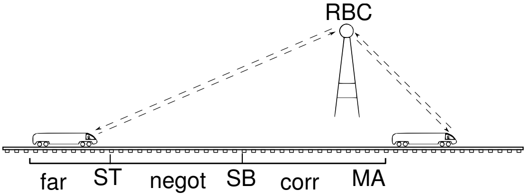
- × no free parameters like ST, SB
- × no finite-state bisimulation for HS

Verifying Hybrid Systems



problem	technique	OP	PAR	T	closed
$ETCS \models z < MA$	TL-MC	✓	×	✓	×
$\models (\mathrm{Ax}(ETCS) \rightarrow z < MA)$	TL-calculus	×	…	✓	…

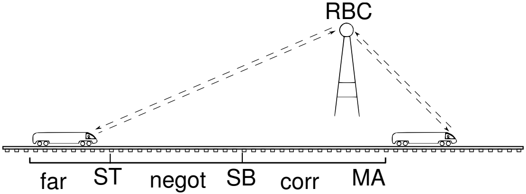
Verifying Hybrid Systems



problem	technique	OP	PAR	T	closed
$ETCS \models z < MA$	TL-MC	✓	×	✓	×
$\models (\mathrm{Ax}(ETCS) \rightarrow z < MA)$	TL-calculus	×	...	✓	...

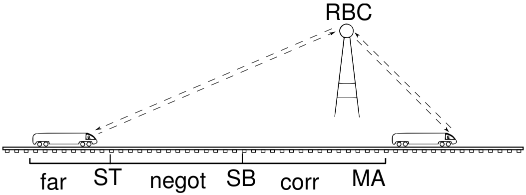
× declaratively axiomatise operational model

Verifying Hybrid Systems



problem	technique	OP	PAR	T	closed
$ETCS \models z < MA$	TL-MC	✓	×	✓	×
$\models (\mathrm{Ax}(ETCS) \rightarrow z < MA)$	TL-calculus	×	...	✓	...
$\models [ETCS]\, z < MA$	DL-calculus	✓	✓	×	✓

Verifying Hybrid Systems

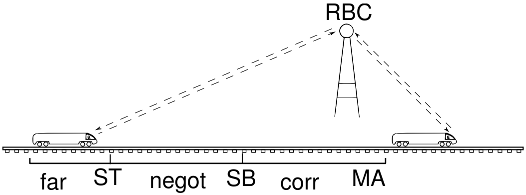


problem	technique	OP	PAR	T	closed
$ETCS \models z < MA$	TL-MC	✓	×	✓	×
$\models (\mathrm{Ax}(ETCS) \rightarrow z < MA)$	TL-calculus	×	...	✓	...
$\models [ETCS]\, z < MA$	DL-calculus	✓	✓	×	✓

✓ $[\mathrm{RBC}]\mathrm{partitioned} \rightarrow \langle \mathrm{Train} \rangle [\mathrm{RBC}]\mathrm{safe}$

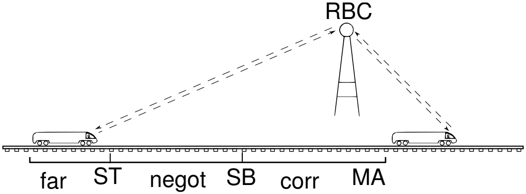
× no intermediate states

Verifying Hybrid Systems



problem	technique	OP	PAR	T	closed
$ETCS \models z < MA$	TL-MC	✓	×	✓	×
$\models (\mathrm{Ax}(ETCS) \rightarrow z < MA)$	TL-calculus	×	...	✓	...
$\models [ETCS]\, z < MA$	DL-calculus	✓	✓	×	✓
$\models [ETCS]\Box\, z < MA$	DTL-calculus	✓	✓	✓	✓

Verifying Hybrid Systems



problem	technique	OP	PAR	T	closed
$ETCS \models z < MA$	TL-MC	✓	×	✓	×
$\models (\mathrm{Ax}(ETCS) \rightarrow z < MA)$	TL-calculus	×	...	✓	...
$\models [ETCS]\, z < MA$	DL-calculus	✓	✓	×	✓
$\models [ETCS]\Box\, z < MA$	DTL-calculus	✓	✓	✓	✓

differential temporal dynamic logic

$$\mathrm{dTL} = \mathrm{TL} + \mathrm{DL} + \mathrm{HP}$$

Outline

1. Motivation
2. Temporal Dynamic Logic dTL
    - Syntax
    - Trace Semantics
    - Conservative Extension
    - Safety Invariants in Train Control
3. Verification Calculus for dTL
    - Sequent Calculus
    - Verifying Safety Invariants in Train Control
    - Soundness
4. Conclusions & Future Work

Outline

1. Motivation

2. Temporal Dynamic Logic dTL
   - Syntax
   - Trace Semantics
   - Conservative Extension
   - Safety Invariants in Train Control

3. Verification Calculus for dTL
   - Sequent Calculus
   - Verifying Safety Invariants in Train Control
   - Soundness

4. Conclusions & Future Work

Temporal Dynamic Logic dTL: Syntax

Definition (Hybrid program α)

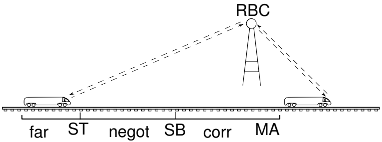
$x' = f(x)$	(continuous evolution)
$x := \theta$	(discrete jump)
$?\chi$	(conditional execution)
$\alpha; \beta$	(seq. composition)
$\alpha \cup \beta$	(nondet. choice)
α^*	(nondet. repetition)

Temporal Dynamic Logic dTL: 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)

$$\begin{aligned} ETCS &\equiv negot; corr; z'' = a \\ negot &\equiv z' = v, \ell' = 1 \\ corr &\equiv (?MA - z < SB;\ a := -b) \\ &\quad \cup (?MA - z \geq SB;\ a := \dots) \end{aligned}$$



Temporal Dynamic Logic dTL: Syntax

Definition (Formulas / state formulas ϕ)

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

Definition (Trace formulas π)

ϕ (non-temporal part)
$\Box\phi, \quad \Diamond\phi$ (temporal part)

Temporal Dynamic Logic dTL: Syntax

Definition (Formulas / state formulas ϕ)

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

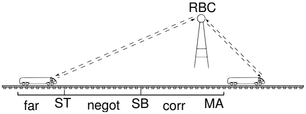
$[\alpha]\pi, \quad \langle\alpha\rangle\pi$ (dynamic part)

Definition (Trace formulas π)

ϕ (non-temporal part)

$\Box\phi, \quad \Diamond\phi$ (temporal part)

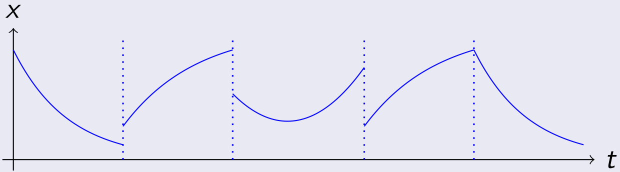
$$\begin{aligned} & [ETCS]\Box(\ell \leq L \rightarrow z < MA) \\ ETCS &\equiv negot; corr; z'' = a \\ negot &\equiv z' = v, \ell' = 1 \end{aligned}$$



Temporal Dynamic Logic dTL: Trace Semantics

Definition (Hybrid trace)

Hybrid trace is sequence of continuous functions $\sigma_i : [0, r_i] \to \text{Sta}\, V$

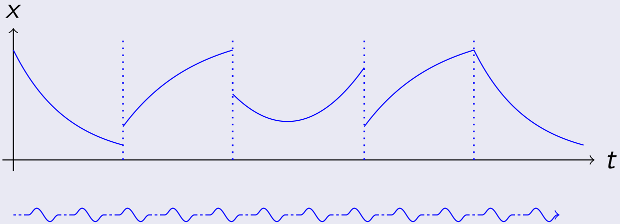


Semantics of hybrid program: set of all its hybrid traces σ

Temporal Dynamic Logic dTL: Trace Semantics

Definition (Hybrid trace)

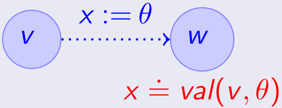
Hybrid trace is sequence of continuous functions $\sigma_i : [0, r_i] \to \mathrm{Sta}\ V$



Semantics of hybrid program: set of all its hybrid traces σ

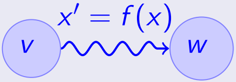
Temporal Dynamic Logic dTL: Trace Semantics

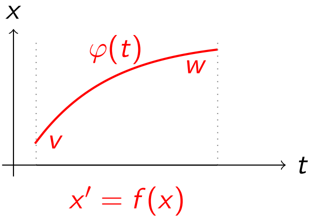
Definition (Hybrid programs α: trace semantics)



Temporal Dynamic Logic dTL: Trace Semantics

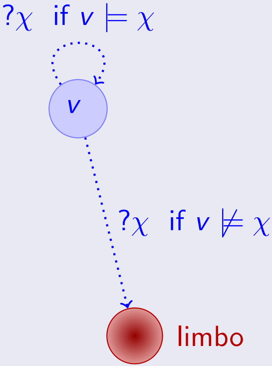
Definition (Hybrid programs α: trace semantics)





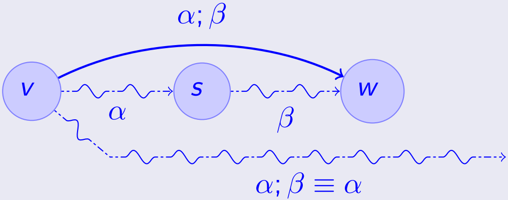
Temporal Dynamic Logic dTL: Trace Semantics

Definition (Hybrid programs α: trace semantics)



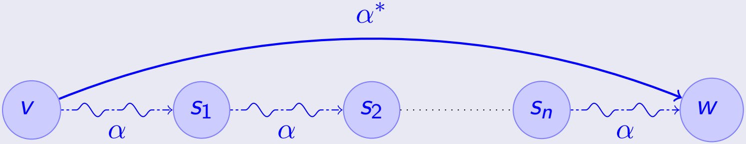
Temporal Dynamic Logic dTL: Trace Semantics

Definition (Hybrid programs α: trace semantics)



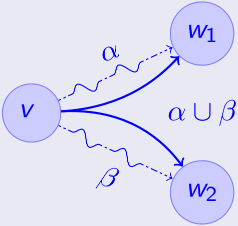
Temporal Dynamic Logic dTL: Trace Semantics

Definition (Hybrid programs α: trace semantics)



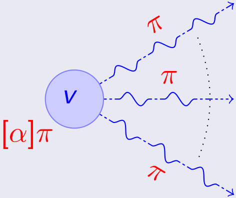
Temporal Dynamic Logic dTL: Trace Semantics

Definition (Hybrid programs α: trace semantics)



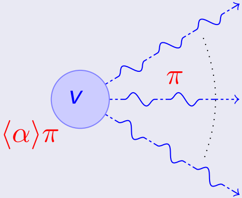
Temporal Dynamic Logic dTL: Trace Semantics

Definition (State formulas ϕ)



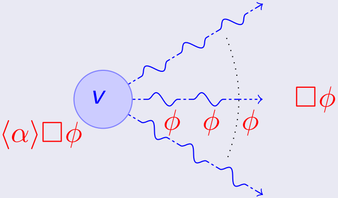
Temporal Dynamic Logic dTL: Trace Semantics

Definition (State formulas ϕ)



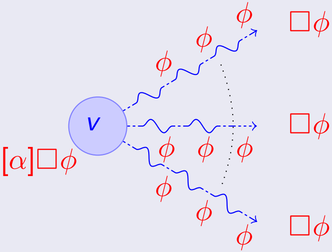
Temporal Dynamic Logic dTL: Trace Semantics

Definition (Trace formulas ϕ)



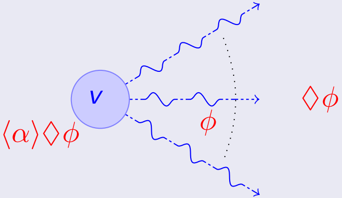
Temporal Dynamic Logic dTL: Trace Semantics

Definition (Trace formulas ϕ)



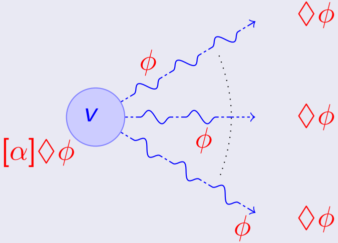
Temporal Dynamic Logic dTL: Trace Semantics

Definition (Trace formulas ϕ)



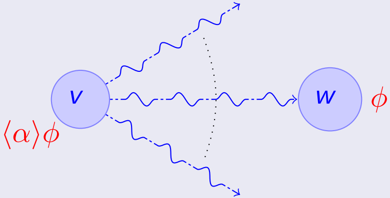
Temporal Dynamic Logic dTL: Trace Semantics

Definition (Trace formulas ϕ)



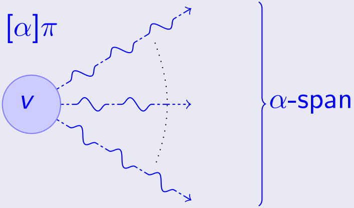
Temporal Dynamic Logic dTL: Trace Semantics

Definition (Trace formulas ϕ)



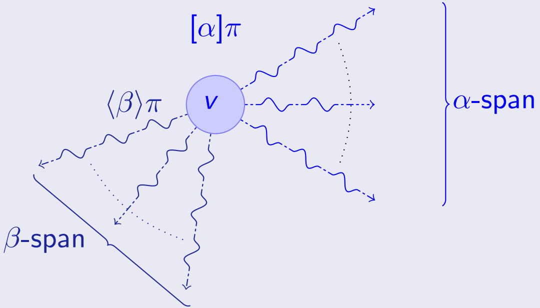
Temporal Dynamic Logic dTL: Trace Semantics

Definition (Trace formulas ϕ)



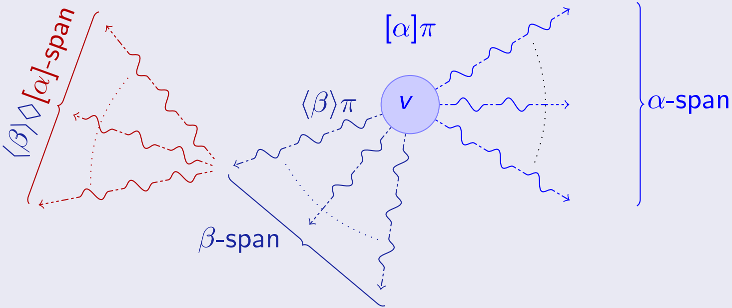
Temporal Dynamic Logic dTL: Trace Semantics

Definition (Trace formulas ϕ)



Temporal Dynamic Logic dTL: Trace Semantics

Definition (Trace formulas ϕ)

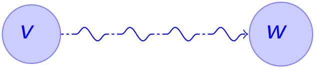


Conservative Extension dTL/d$\mathcal{L}$

Proposition

dTL *is conservative extension of non-temporal* d$\mathcal{L}$, *i.e.,*

$$\textit{trace semantics} \equiv \textit{transition semantics} \quad (\textit{without } \Box, \Diamond)$$

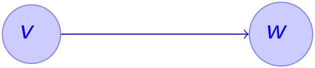


Conservative Extension dTL/d$\mathcal{L}$

Proposition

dTL *is conservative extension of non-temporal* d$\mathcal{L}$*, i.e.,*

$$\textit{trace semantics} \equiv \textit{transition semantics} \;\; (\textit{without}\ \Box, \Diamond)$$



Outline

1. Motivation

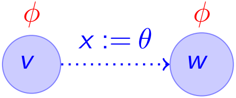
2. Temporal Dynamic Logic dTL
   - Syntax
   - Trace Semantics
   - Conservative Extension
   - Safety Invariants in Train Control

3. Verification Calculus for dTL
   - Sequent Calculus
   - Verifying Safety Invariants in Train Control
   - Soundness

4. Conclusions & Future Work

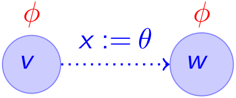
Verification Calculus for dTL

$$\frac{\phi \land [x := \theta]\phi}{[x := \theta]\Box\phi}$$

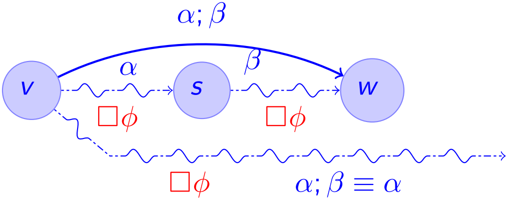


Verification Calculus for dTL

$$\frac{\phi \wedge [x := \theta]\phi}{[x := \theta]\Box\phi}$$

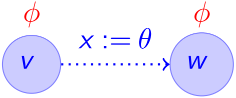


$$\frac{[\alpha]\Box\phi \wedge [\alpha][\beta]\Box\phi}{[\alpha; \beta]\Box\phi}$$

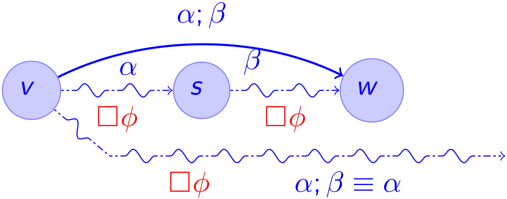


Verification Calculus for dTL

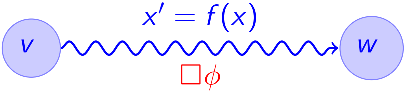
$$\frac{\phi \land [x := \theta]\phi}{[x := \theta]\Box\phi}$$



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

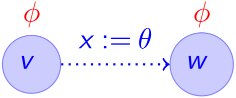


$$\frac{[x' = \theta]\phi}{[x' = \theta]\Box\phi}$$

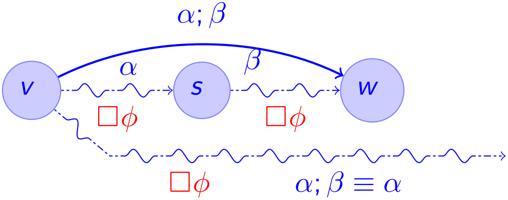


Verification Calculus for dTL

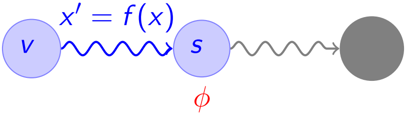
$$\frac{\phi \land [x := \theta]\phi}{[x := \theta]\Box\phi}$$



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



$$\frac{[x' = \theta]\phi}{[x' = \theta]\Box\phi}$$



Verification Calculus for dTL

Temporal Reduction Rules

10 temporal rules

$$\text{(T1)} \quad \frac{[\alpha]\Box\phi \land [\alpha][\beta]\Box\phi}{[\alpha;\beta]\Box\phi}$$

$$\text{(T2)} \quad \frac{\phi}{[?\chi]\Box\phi}$$

$$\text{(T3)} \quad \frac{\phi \land [x := \theta]\phi}{[x := \theta]\Box\phi}$$

$$\text{(T4)} \quad \frac{[x' = \theta]\phi}{[x' = \theta]\Box\phi}$$

$$\text{(T5)} \quad \frac{[\alpha;\alpha^*]\Box\phi}{[\alpha^*]\Box\phi}$$

$$\text{(T6)} \quad \frac{\langle\alpha\rangle\Diamond\phi \lor \langle\alpha\rangle\langle\beta\rangle\Diamond\phi}{\langle\alpha;\beta\rangle\Diamond\phi}$$

$$\text{(T7)} \quad \frac{\phi}{\langle ?\chi\rangle\Diamond\phi}$$

$$\text{(T8)} \quad \frac{\phi \lor \langle x := \theta\rangle\phi}{\langle x := \theta\rangle\Diamond\phi}$$

$$\text{(T9)} \quad \frac{\langle x' = \theta\rangle\phi}{\langle x' = \theta\rangle\Diamond\phi}$$

$$\text{(T10)} \quad \frac{\langle\alpha;\alpha^*\rangle\Diamond\phi}{\langle\alpha^*\rangle\Diamond\phi}$$

Verification Calculus for dTL

Non-temporal Rules

10 non-temporal rules

(D1) $$\frac{\langle\alpha\rangle\pi \lor \langle\beta\rangle\pi}{\langle\alpha \cup \beta\rangle\pi}$$

(D2) $$\frac{[\alpha]\pi \land [\beta]\pi}{[\alpha \cup \beta]\pi}$$

(D3) $$\frac{\langle\alpha\rangle\langle\beta\rangle\phi}{\langle\alpha; \beta\rangle\phi}$$

(D4) $$\frac{\chi \land \phi}{\langle ?\chi\rangle\phi}$$

(D5) $$\frac{\chi \to \phi}{[?\chi]\phi}$$

(D6) $$\frac{\phi \lor \langle\alpha; \alpha^*\rangle\phi}{\langle\alpha^*\rangle\phi}$$

(D7) $$\frac{\phi \land [\alpha; \alpha^*]\phi}{[\alpha^*]\phi}$$

(D8) $$\frac{F_x^\theta}{\langle x := \theta\rangle F}$$

(D9) $$\frac{\exists t{\geq}0\, \langle x := y_x(t)\rangle\phi}{\langle x' = \theta\rangle\phi}$$

(D10) $$\frac{\forall t{\geq}0\, [x := y_x(t)]\phi}{[x' = \theta]\phi}$$

Verification Calculus for dTL

Propositional/Quantifier Rules

10 propositional rules

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

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

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

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

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

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

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

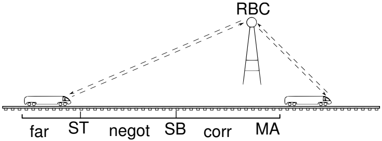
(P8) $$\frac{\vdash \phi, \psi}{\vdash \phi \lor \psi}$$

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

(P10) $$\frac{F_0 \vdash G_0}{F \vdash G}$$

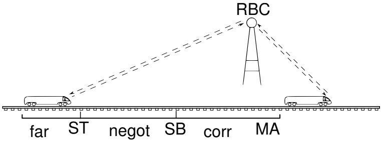
Verify Safety in Train Control

$$\begin{aligned}
ETCS &\equiv negot; corr; z'' = a \\
negot &\equiv z' = v, \ell' = 1 \\
corr &\equiv (?MA - z < ST;\ a := -b) \\
&\quad \cup (?MA - z \geq ST;\ a := \dots)
\end{aligned}$$



Verify Safety in Train Control

$$\begin{aligned}
ETCS &\equiv negot; corr; z'' = a\\
negot &\equiv z' = v, \ell' = 1\\
corr &\equiv (?MA - z < ST;\ a := -b)\\
&\quad \cup (?MA - z \geq ST;\ a := \dots)
\end{aligned}$$

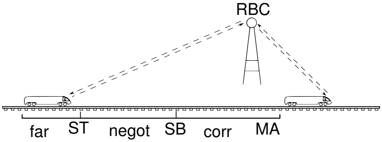


Proof

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\psi \vdash Lv + z < MA}{\psi \vdash \forall l{\geq}0\,(l \leq L \rightarrow lv + z < MA)}}{\psi \vdash \forall l{\geq}0\,\langle z := lv + z, \ell := l\rangle\phi}}{\psi \vdash [negot]\phi}}{\psi \vdash [negot]\Box\phi}
\quad
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\psi, \ell{\geq}0 \vdash v^2 < 2b(MA - Lv - z)}{\psi, \ell{\geq}0 \vdash \langle z := \ell v{+}z, a := \text{-}b\rangle \forall t{\geq}0\,(\ell{\leq}L \rightarrow \frac{a}{2}t^2{+}vt{+}z{<}MA)}}{\psi, \ell{\geq}0 \vdash \langle z := \ell v{+}z, a := \text{-}b\rangle \forall t{\geq}0\,\langle z := \frac{a}{2}t^2{+}vt{+}z\rangle\phi)}}{\psi, \ell{\geq}0 \vdash \langle z := \ell v{+}z, a := \text{-}b\rangle[z'' = a]\Box\phi \qquad \triangleright}}{\psi, \ell{\geq}0 \vdash \langle z := \ell v{+}z\rangle[corr][z'' = a]\Box\phi \qquad \triangleright}}{\psi, \ell{\geq}0 \vdash \langle z := \ell v{+}z\rangle[corr; z'' = a]\Box\phi}}{\psi \vdash \ell{\geq}0 \rightarrow \langle z := \ell v{+}z\rangle[corr; z'' = a]\Box\phi}}{\psi \vdash \forall\ell{\geq}0\,\langle z := \ell v{+}z\rangle[corr; z'' = a]\Box\phi}}{\psi \vdash [negot][corr; z'' = a]\Box\phi}}{\psi \vdash [negot; corr; z'' = a]\Box\phi}}{\vdash \psi \rightarrow [negot; corr; z'' = a]\Box\phi}$$

Verify Safety in Train Control

$$v^2 < 2b(MA - Lv - z)$$
$$Lv + z < MA$$

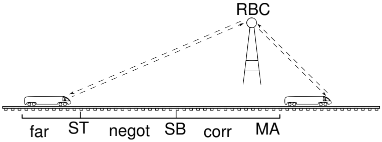


Proof

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\psi \vdash Lv + z < MA}{\psi \vdash \forall l{\ge}0\,(l \le L \to lv + z < MA)}}{\psi \vdash \forall l{\ge}0\,\langle z := lv + z, \ell := l\rangle \phi}}{\psi \vdash [negot]\phi}}{\psi \vdash [negot]\Box\phi} \quad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\psi, \ell{\ge}0 \vdash v^2 < 2b(MA - Lv - z)}{\psi, \ell{\ge}0 \vdash \langle z := \ell v{+}z, a := \text{-}b\rangle \forall t{\ge}0\,(\ell{\le}L \to \frac{a}{2}t^2{+}vt{+}z{<}MA)}}{\psi, \ell{\ge}0 \vdash \langle z := \ell v{+}z, a := \text{-}b\rangle \forall t{\ge}0\,\langle z := \frac{a}{2}t^2{+}vt{+}z\rangle \phi)}}{\psi, \ell{\ge}0 \vdash \langle z := \ell v{+}z, a := \text{-}b\rangle [z'' = a]\Box\phi \quad \triangleright}}{\psi, \ell{\ge}0 \vdash \langle z := \ell v{+}z\rangle [corr][z'' = a]\Box\phi \quad \triangleright}}{\psi, \ell{\ge}0 \vdash \langle z := \ell v{+}z\rangle [corr; z'' = a]\Box\phi}}{\psi \vdash \ell{\ge}0 \to \langle z := \ell v{+}z\rangle [corr; z'' = a]\Box\phi}}{\psi \vdash \forall \ell{\ge}0\,\langle z := \ell v{+}z\rangle [corr; z'' = a]\Box\phi}}{\psi \vdash [negot][corr; z'' = a]\Box\phi}}{\dfrac{\psi \vdash [negot; corr; z'' = a]\Box\phi}{\vdash \psi \to [negot; corr; z'' = a]\Box\phi}}$$

Verify Safety in Train Control

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



$$\boxed{ST \geq Lv + \frac{v^2}{2b}}$$

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

Soundness

Theorem (Soundness)

dTL *calculus is sound.*

Proposition (Incompleteness)

"All" discrete or continuous fragments of dTL *are inherently incomplete.*

fragment	discrete	continuous
FOL		✓
$[\alpha]\Box\phi$	×	×
$[\alpha]\Diamond\phi$	×	×
$[\alpha]\phi$	×	×

(Yet, reachability in hybrid systems is not semidecidable)

Outline

1. Motivation
2. Temporal Dynamic Logic dTL
    - Syntax
    - Trace Semantics
    - Conservative Extension
    - Safety Invariants in Train Control
3. Verification Calculus for dTL
    - Sequent Calculus
    - Verifying Safety Invariants in Train Control
    - Soundness
4. Conclusions & Future Work

Future Work

- Prove dTL/d$\mathcal{L}$ relatively complete
- “Temporal” induction
- Improve alternating “liveness” quantifiers $[\alpha]\Diamond\phi$
- dTL*

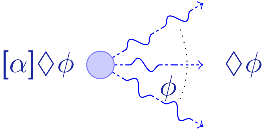
$$[\mathit{ETCS}](\Box\Diamond \mathit{sensor} \rightarrow \Diamond\Box \mathit{stable})$$

Conclusions (I)

Deductively verify temporal properties of operational hybrid systems

differential temporal dynamic logic

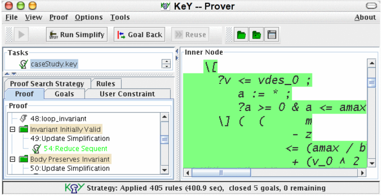
$$\mathrm{dTL} = \mathrm{TL} + \mathrm{DL} + \mathrm{HP}$$



problem	technique	OP	PAR	T	closed
$ETCS \models z < MA$	TL-MC	✓	×	✓	×
$\models (\mathrm{Ax}(ETCS) \rightarrow z < MA)$	TL-calculus	×	...	✓	...
$\models [ETCS]\, z < MA$	DL-calculus	✓	✓	×	✓
$\models [ETCS]\Box\, z < MA$	dTL-calculus	✓	✓	✓	✓

Conclusions (II)

- Train control (ETCS) verification
- Modular temporal/non-temporal calculus
- Constructive deduction modulo
- Verification tool HyKeY
- Parameter discovery



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

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

- B. Beckert and S. Schlager.
  A sequent calculus for first-order dynamic logic with trace modalities.
  In R. Goré, A. Leitsch, and T. Nipkow, editors, *IJCAR*, volume 2083 of *LNCS*, pages 626–641. Springer, 2001.

- J. M. Davoren, V. Coulthard, N. Markey, and T. Moor.
  Non-deterministic temporal logics for general flow systems.
  In R. Alur and G. J. Pappas, editors, *HSCC*, volume 2993 of *LNCS*, pages 280–295. Springer, 2004.

- V. Mysore, C. Piazza, and B. Mishra.
  Algorithmic algebraic model checking II: Decidability of semi-algebraic model checking and its applications to systems biology.
  In D. Peled and Y.-K. Tsay, editors, *ATVA*, volume 3707 of *LNCS*, pages 217–233. Springer, 2005.

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