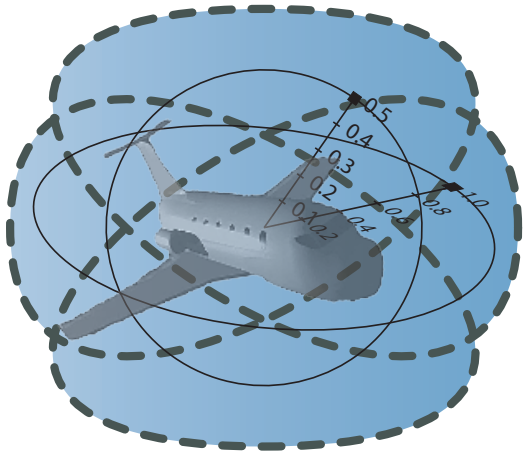
15-819/18-879: Logical Analysis of Hybrid Systems

27: Differential Temporal Dynamic Logic

André Platzer

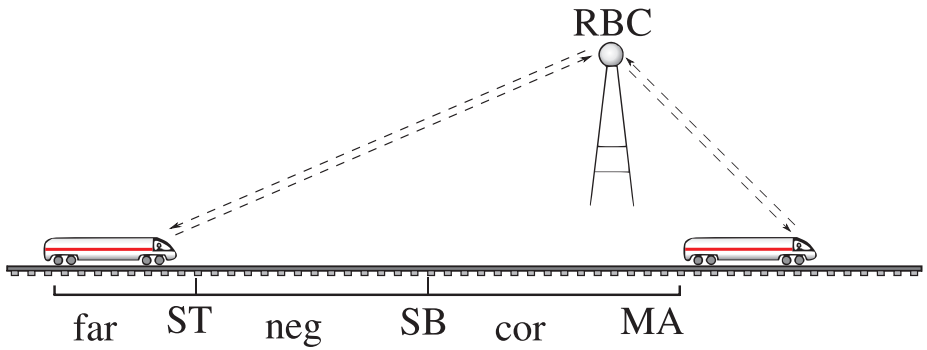
aplatzer@cs.cmu.edu
Carnegie Mellon University, Pittsburgh, PA



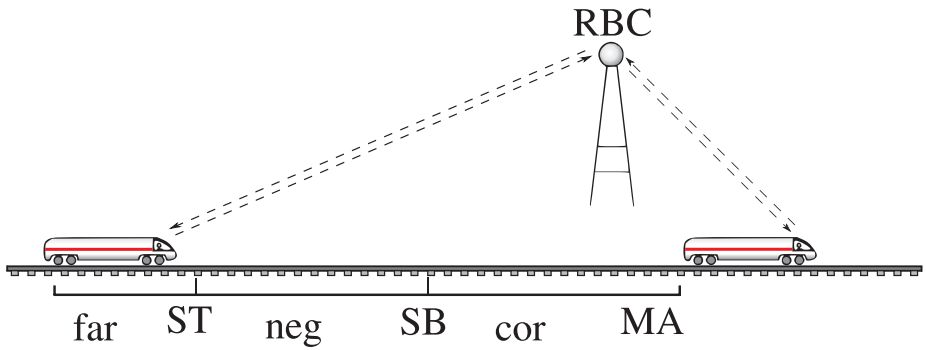
Outline

Outline

Verifying Hybrid Systems



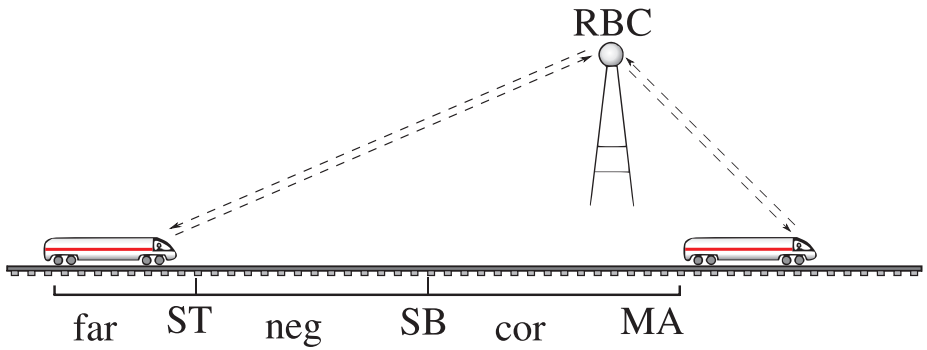
Verifying Hybrid Systems



Hybrid Systems

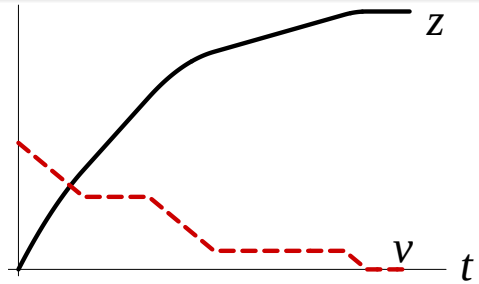
continuous evolution along differential equations + discrete change

Verifying Hybrid Systems

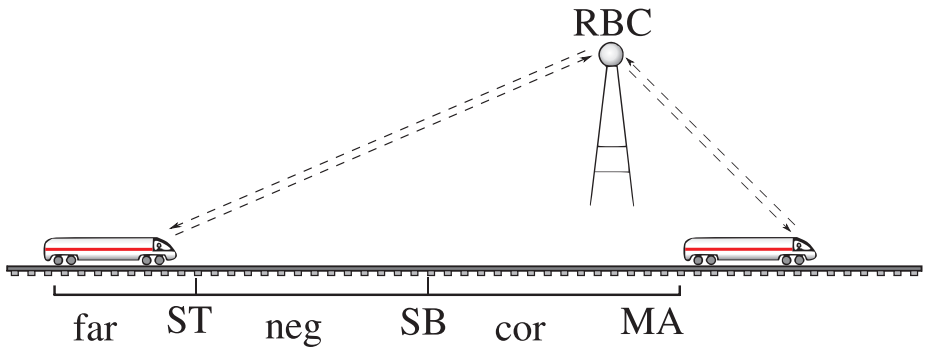


Hybrid Systems

continuous evolution along differential equations + discrete change

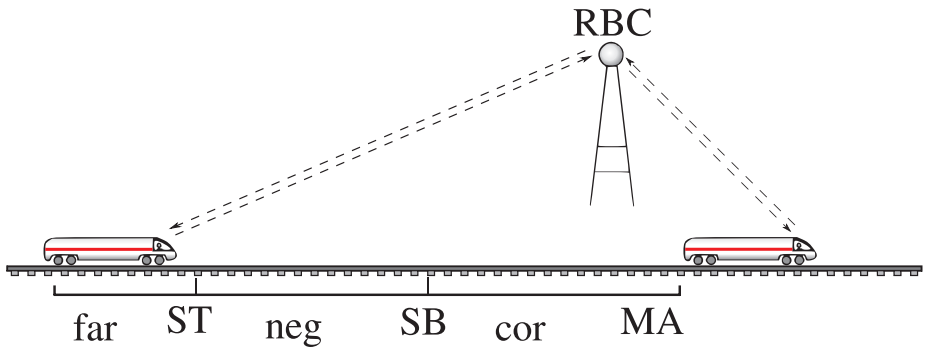


Verifying Hybrid Systems



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

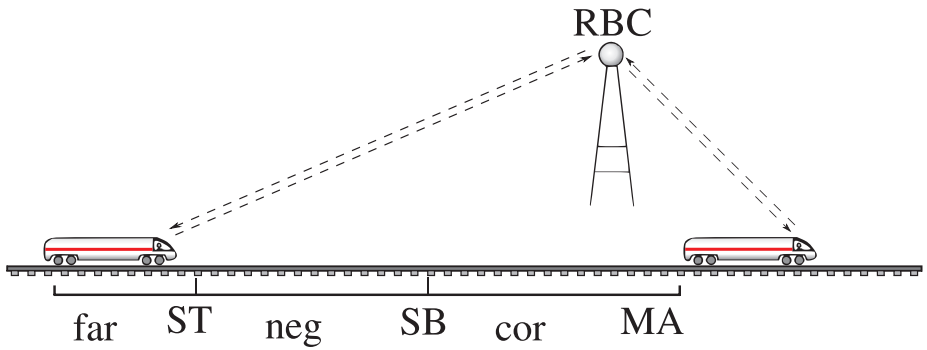
Verifying Hybrid Systems



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

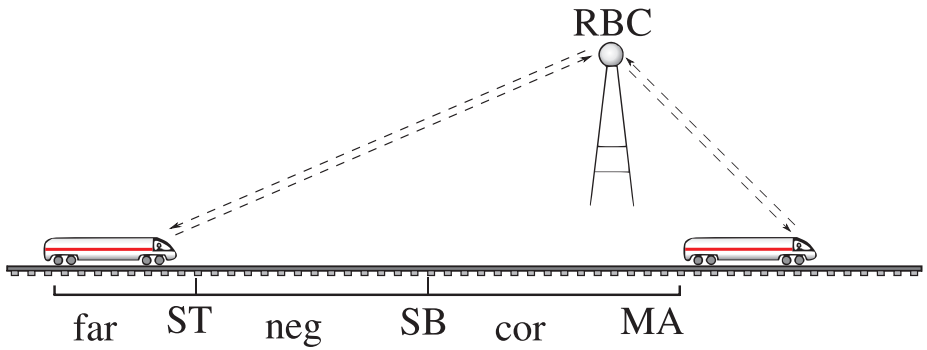
× no free parameters like ST, SB
× no finite-state bisimulation for HS

Verifying Hybrid Systems



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

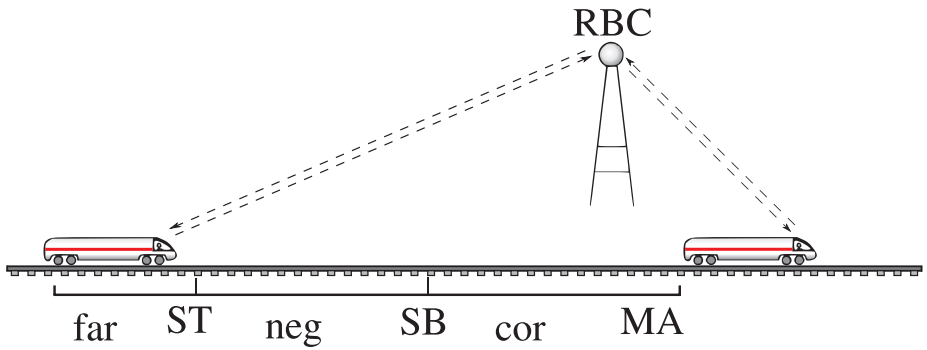
Verifying Hybrid Systems



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

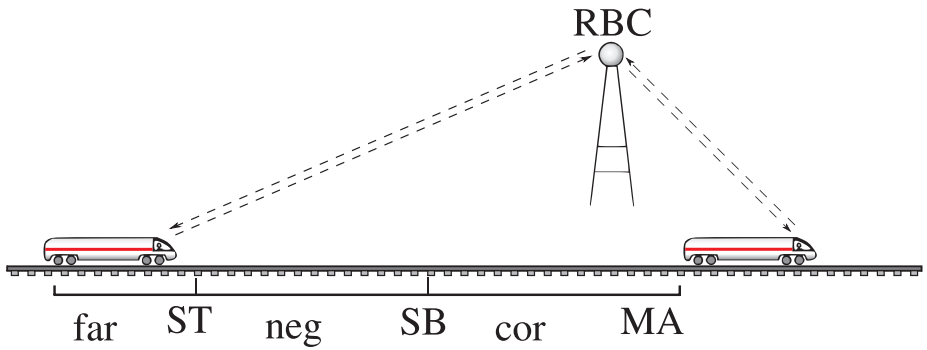
× declaratively axiomatise operational model

Verifying Hybrid Systems



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

Verifying Hybrid Systems

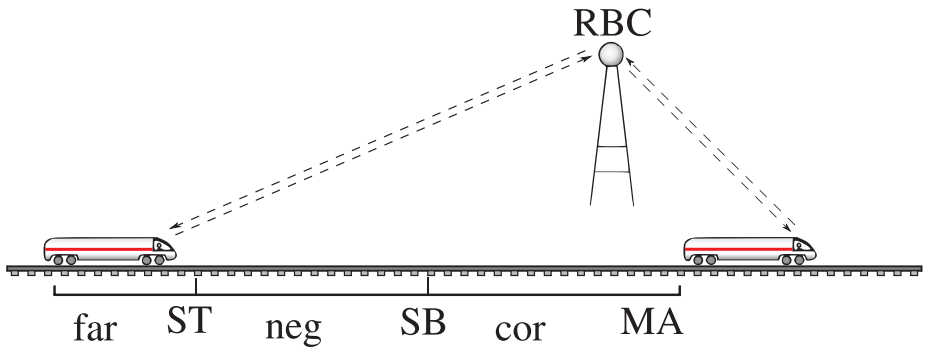


problem	technique	Op	Par	T	closed
$ETCS \models z < MA$	TL-MC	✓	×	✓	×
$\models (\mathrm{Ax}(ETCS) \rightarrow z < MA)$	TL-calculus	×	×	✓	...
$\models [ETCS]\, z < MA$	DL-calculus	✓	✓	×	✓

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

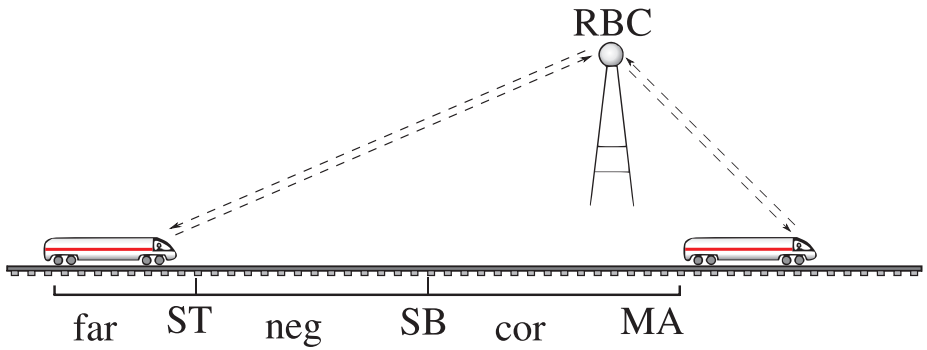
× no intermediate states

Verifying Hybrid Systems



problem	technique	Op	Par	T	closed
$ETCS \models z < MA$	TL-MC	✓	×	✓	×
$\models (\mathsf{Ax}(ETCS) \rightarrow z < MA)$	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

Temporal Dynamic Logic dTL: Syntax

Definition (Hybrid program α)

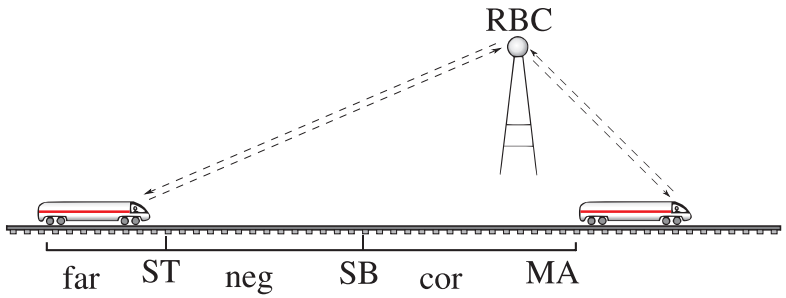
$x' = f(x)$	(continuous evolution)
$x := \theta$	(discrete jump)
$?\chi$	(conditional execution)
$\alpha; \beta$	(seq. composition)
$\alpha \cup \beta$	(nondet. choice)
α^*	(nondet. repetition)

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)

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



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

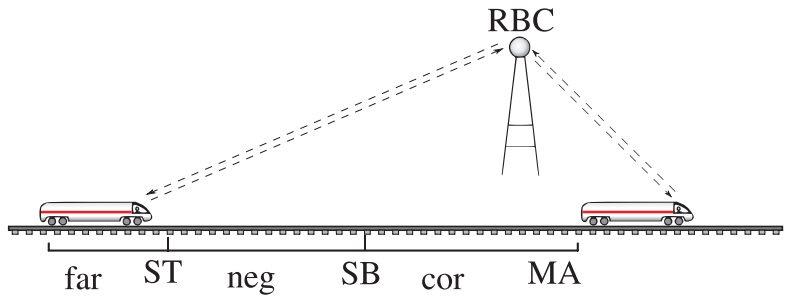
Definition (Formulas / state formulas ϕ)

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

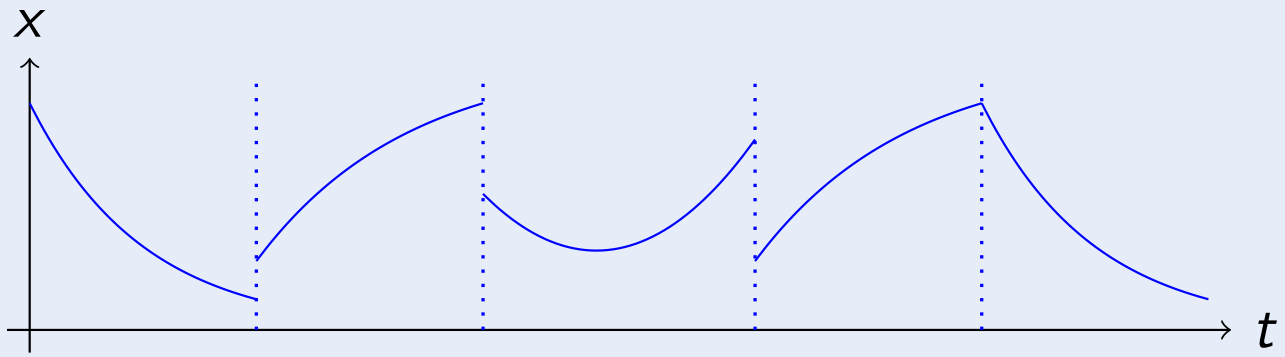
$$[ETCS]\Box(\ell \leq L \rightarrow z < MA)$$
$$ETCS \equiv neg; cor; z'' = a$$
$$neg \equiv z' = v, \ell' = 1$$



Temporal Dynamic Logic dTL: Trace Semantics

Definition (Hybrid trace)

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

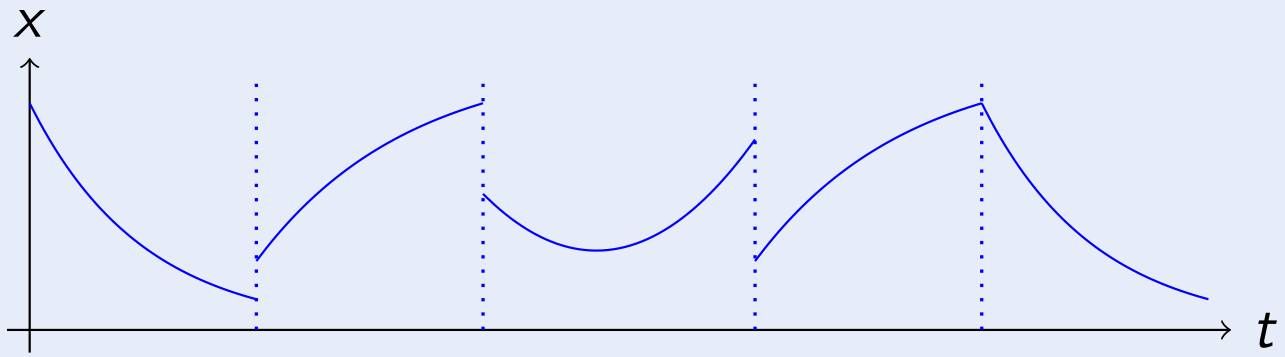


Trace semantics of hybrid program: set of all its hybrid traces σ

Temporal Dynamic Logic dTL: Trace Semantics

Definition (Hybrid trace)

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

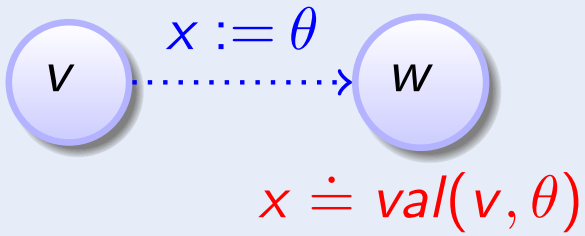


notation: 

Trace semantics of hybrid program: set of all its hybrid traces σ

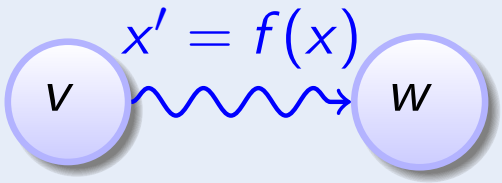
Temporal Dynamic Logic dTL: Trace Semantics

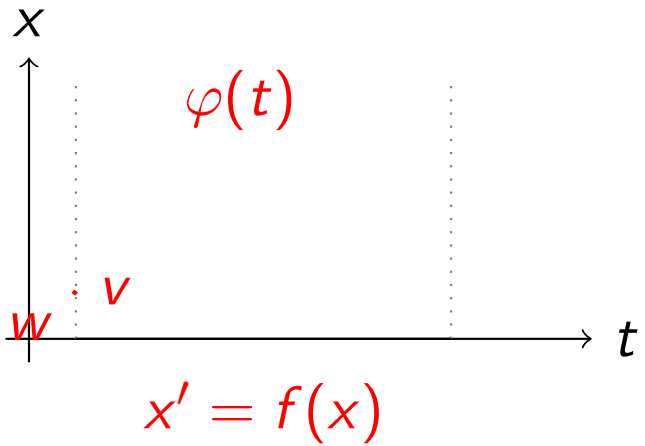
Definition (Hybrid programs α: trace semantics)



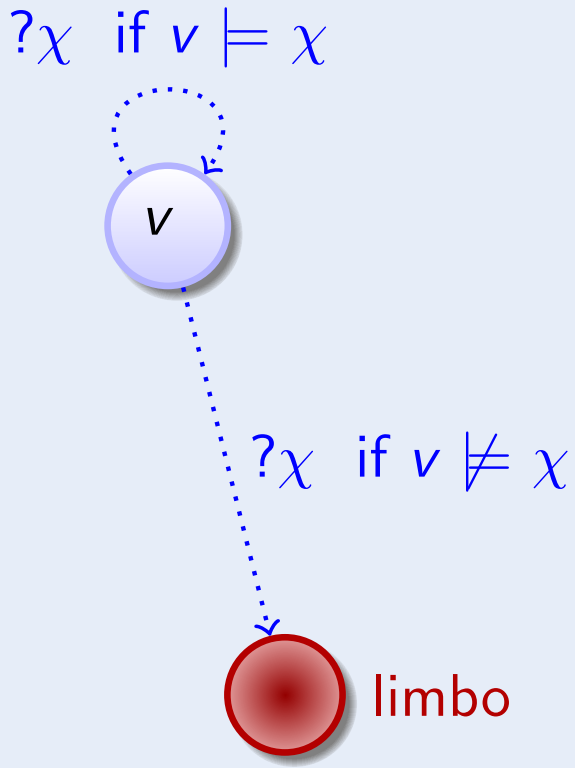
Temporal Dynamic Logic dTL: Trace Semantics

Definition (Hybrid programs α: trace semantics)

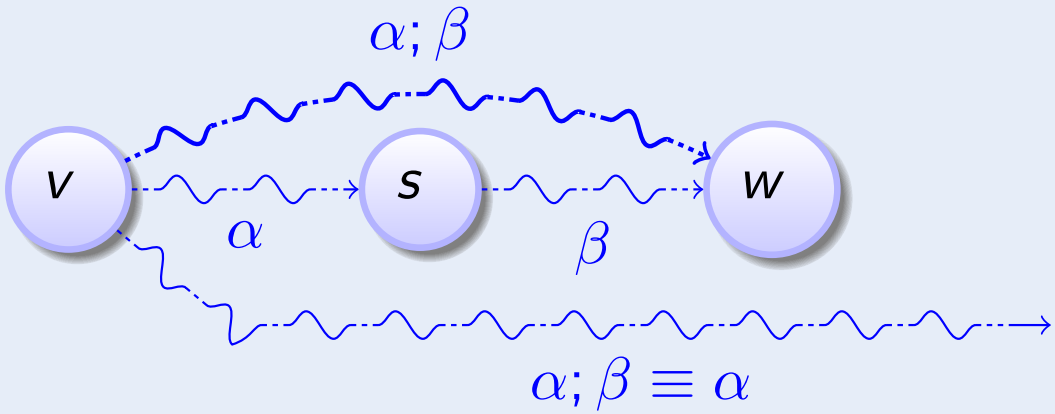




Definition (Hybrid programs α: trace semantics)

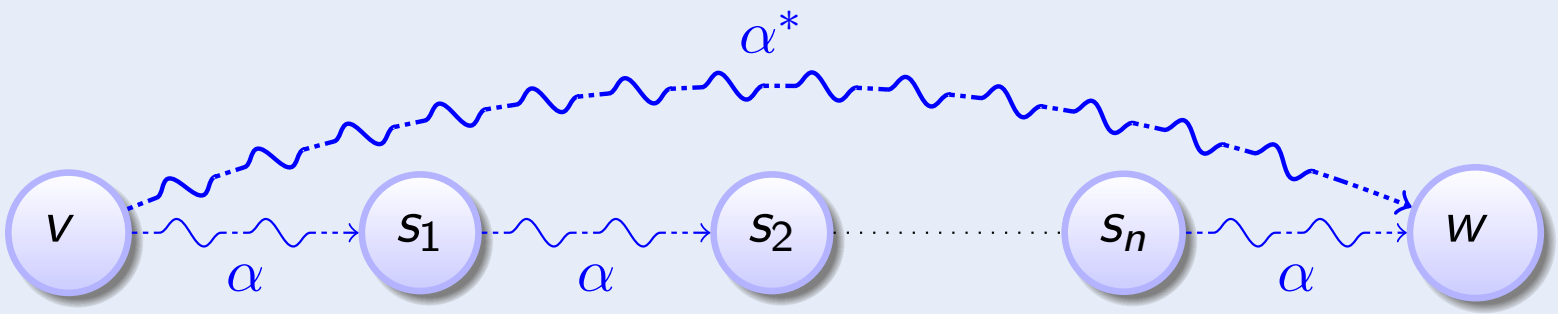


Definition (Hybrid programs α: trace semantics)

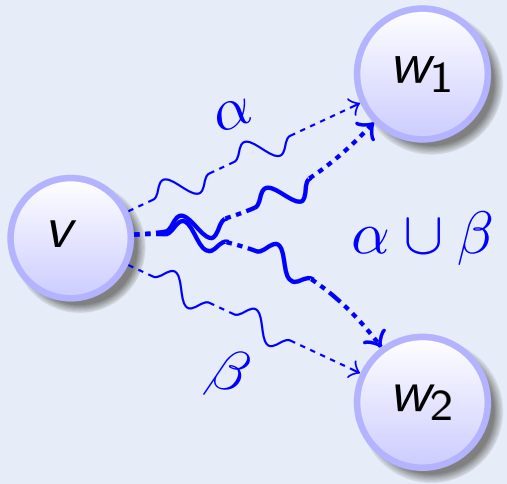


Temporal Dynamic Logic dTL: Trace Semantics

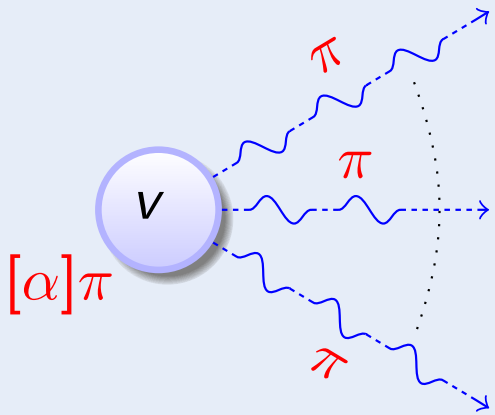
Definition (Hybrid programs α: trace semantics)



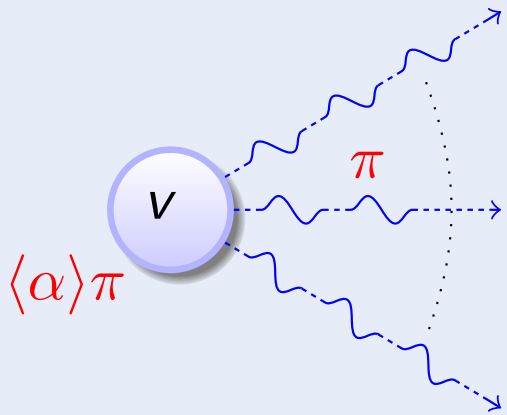
Definition (Hybrid programs α: trace semantics)



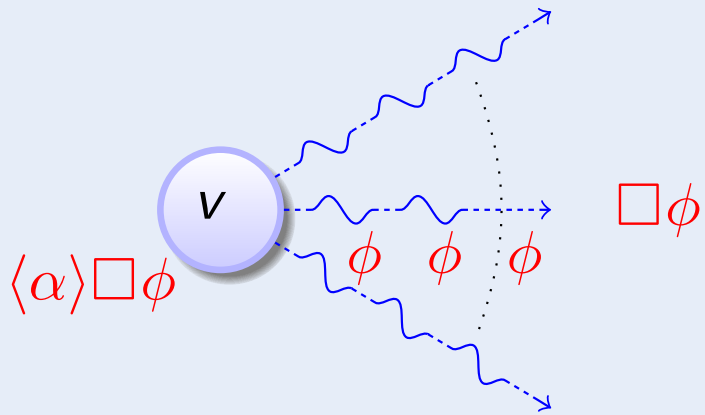
Definition (State formulas ϕ)



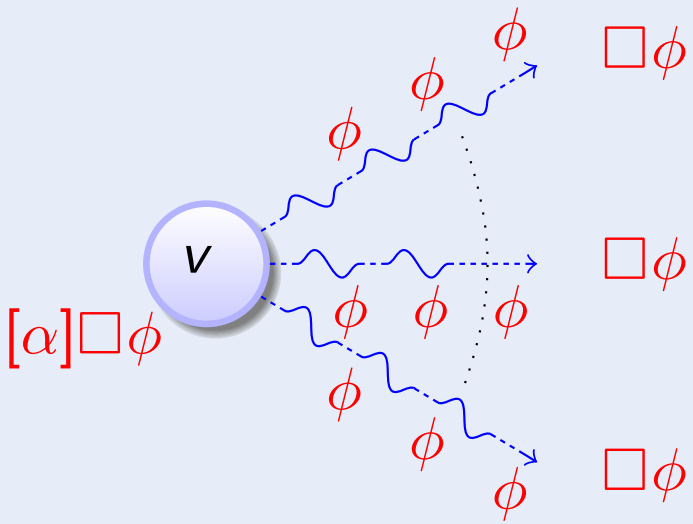
Definition (State formulas ϕ)



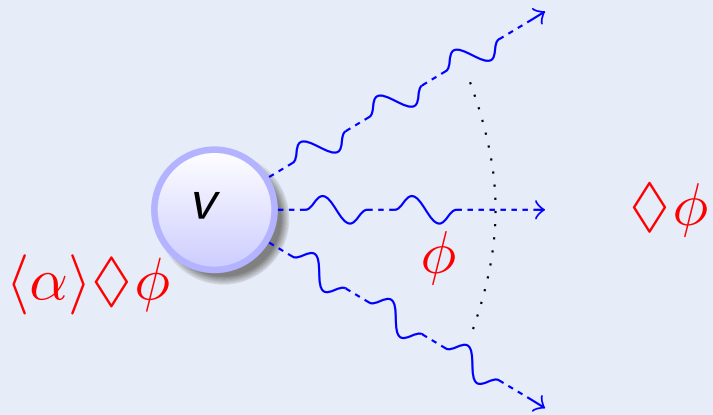
Definition (Trace formulas ϕ)



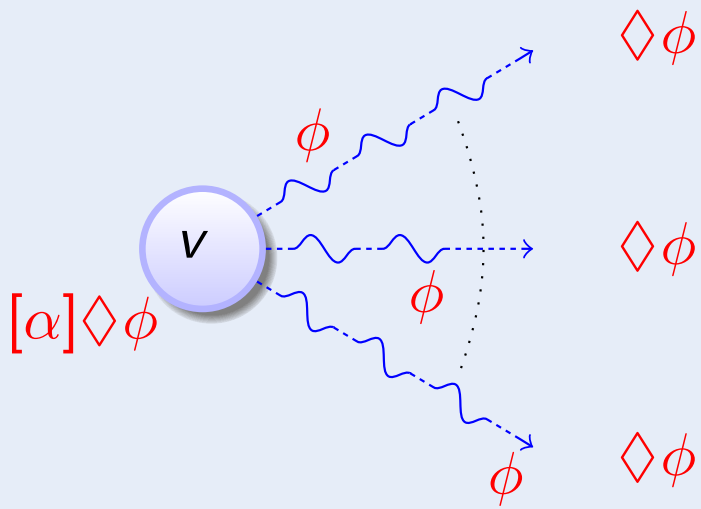
Definition (Trace formulas ϕ)



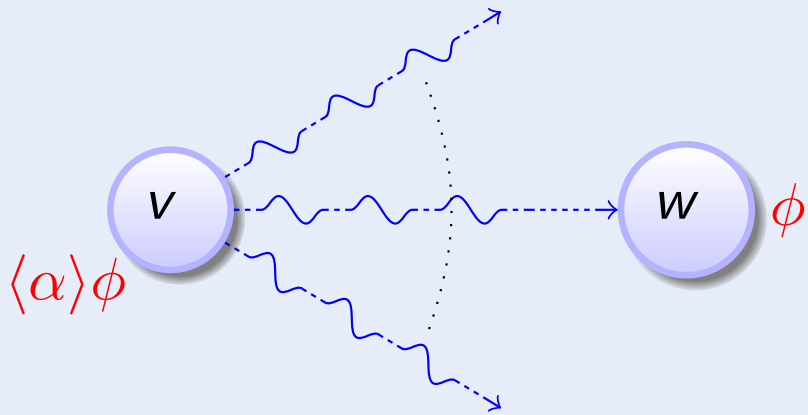
Definition (Trace formulas ϕ)



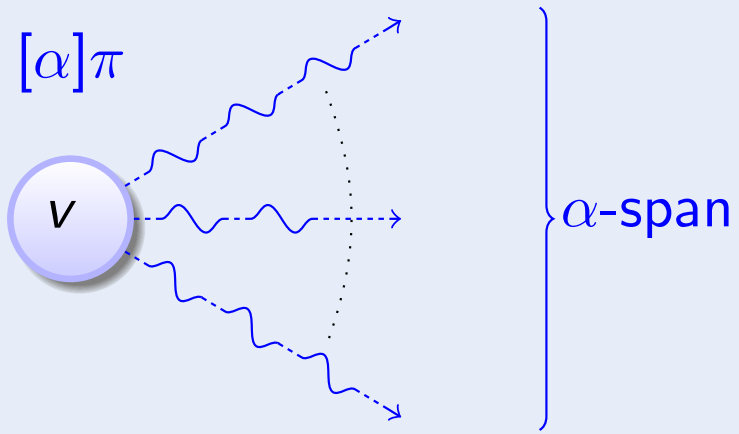
Definition (Trace formulas ϕ)



Definition (Trace formulas ϕ)

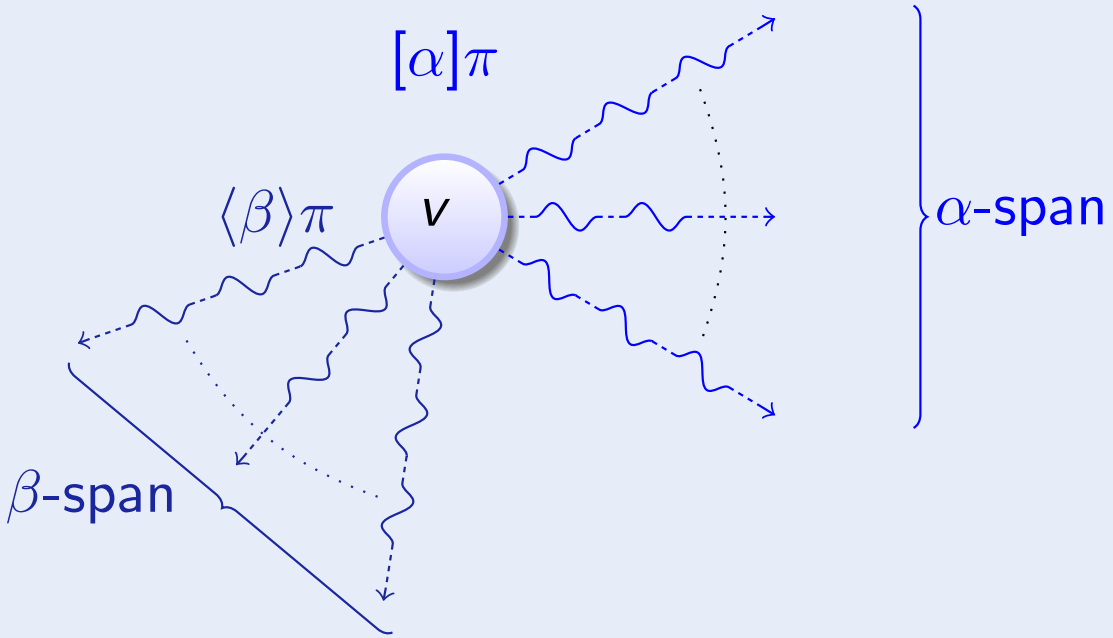


Definition (Trace formulas ϕ)



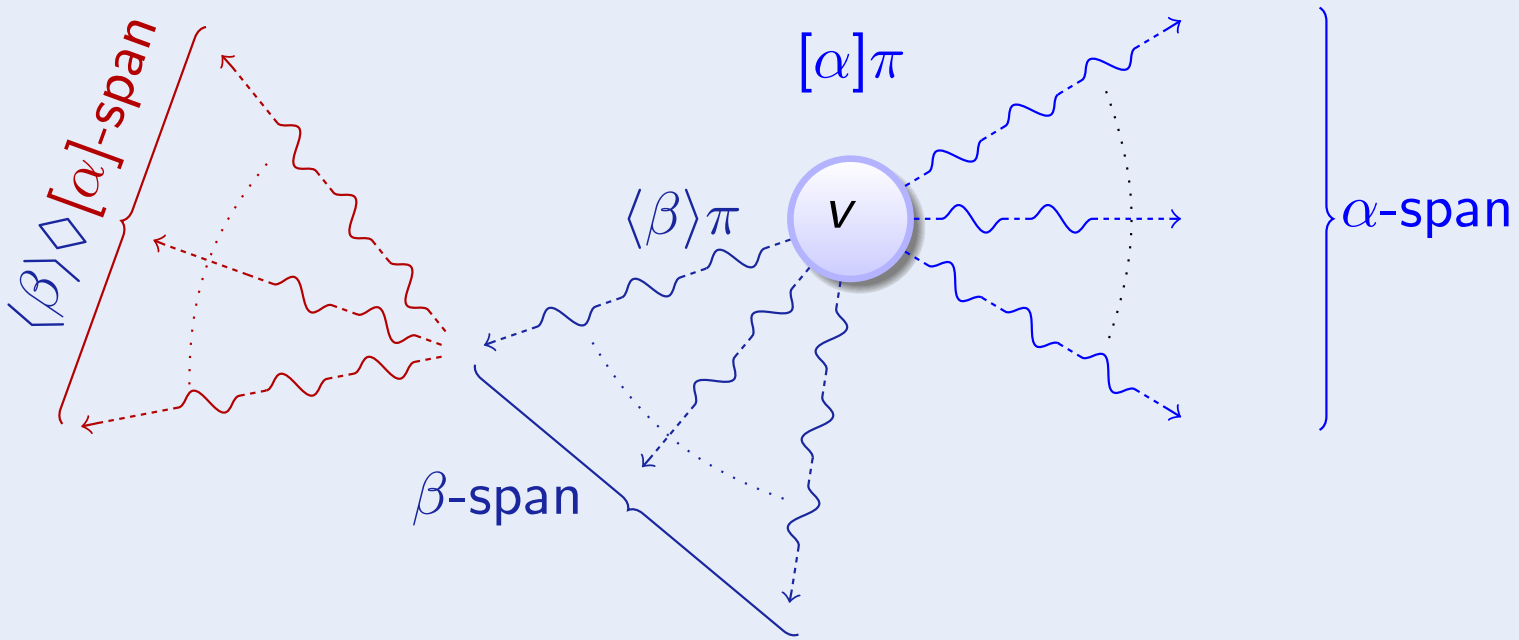
Temporal Dynamic Logic dTL: Trace Semantics

Definition (Trace formulas ϕ)



Temporal Dynamic Logic dTL: Trace Semantics

Definition (Trace formulas ϕ)

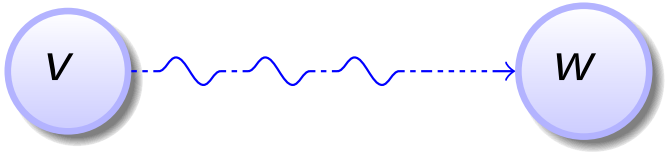


Conservative Extension dTL/d$\mathcal{L}$

Proposition

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

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

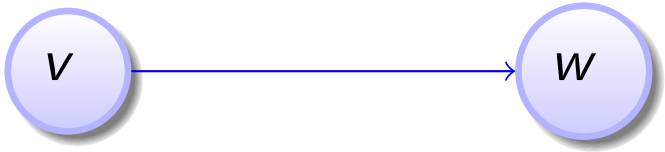


Conservative Extension dTL/d$\mathcal{L}$

Proposition

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

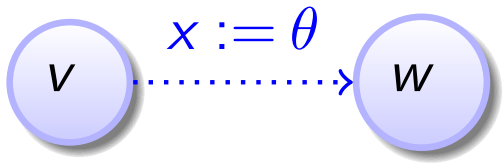
$$\textit{trace semantics} \equiv \textit{transition semantics} \quad (\textit{without } \Box, \Diamond)$$



Outline

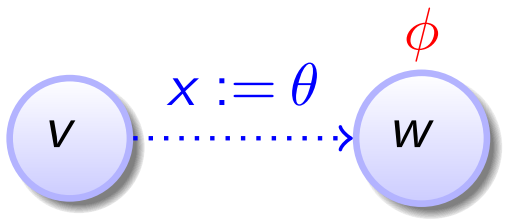
Modular Proof Calculus for Temporal dTL

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



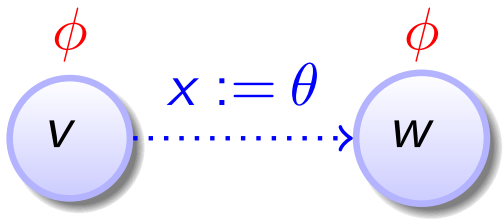
Modular Proof Calculus for Temporal dTL

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



Modular Proof Calculus for Temporal dTL

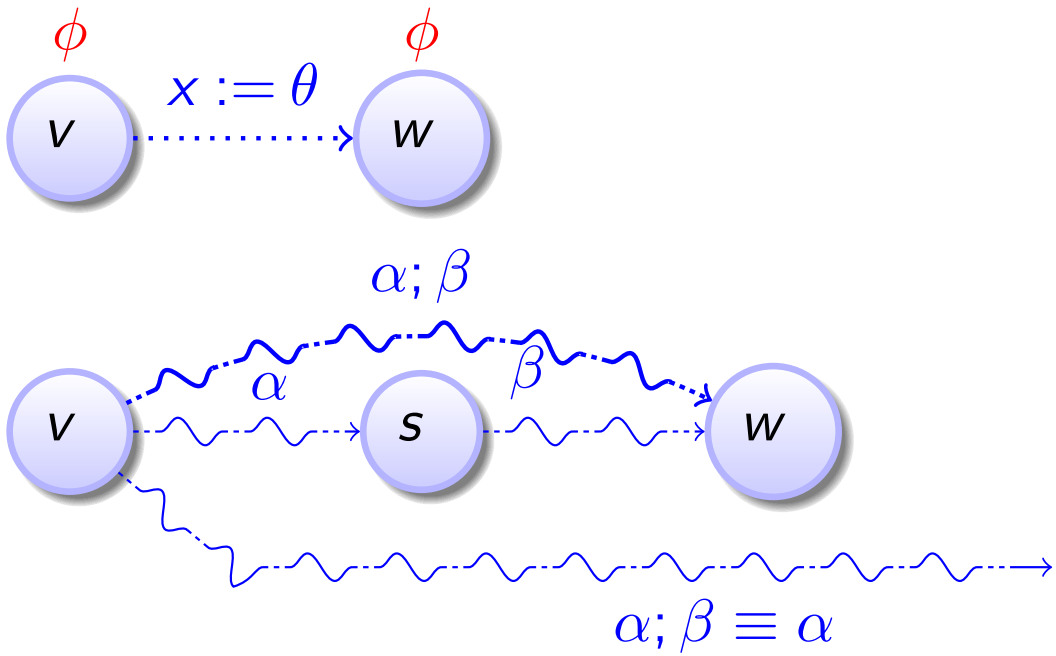
$$\frac{\phi \wedge [x := \theta]\phi}{[x := \theta]\Box\phi}$$



Modular Proof Calculus for Temporal dTL

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

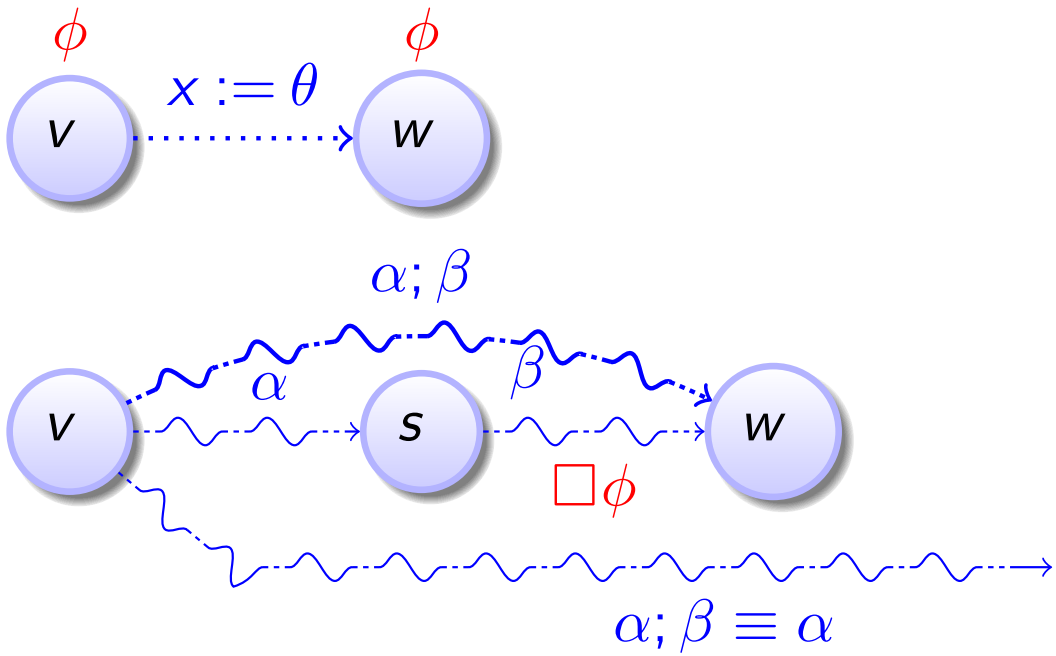
$$\frac{}{[\alpha;\beta]\Box\phi}$$



Modular Proof Calculus for Temporal dTL

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

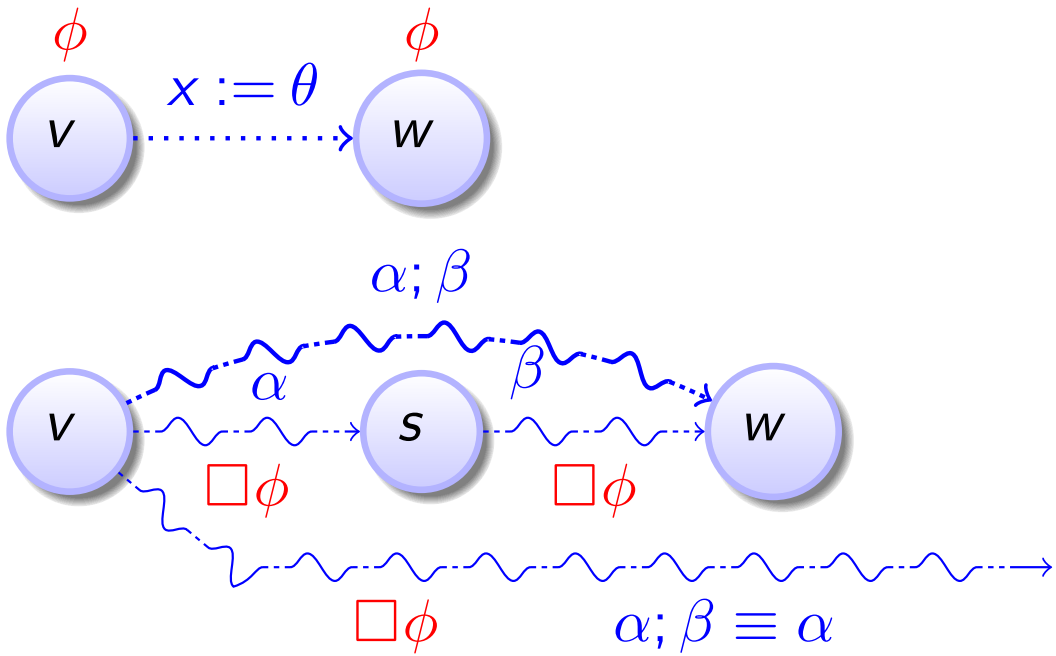
$$\frac{[\alpha][\beta]\Box\phi}{[\alpha;\beta]\Box\phi}$$



Modular Proof Calculus for Temporal dTL

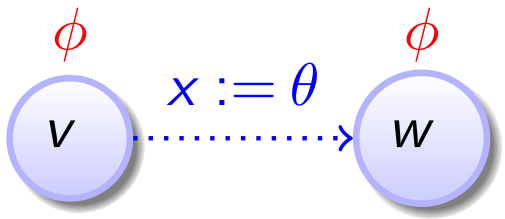
$$\frac{\phi \wedge [x := \theta]\phi}{[x := \theta]\Box\phi}$$

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

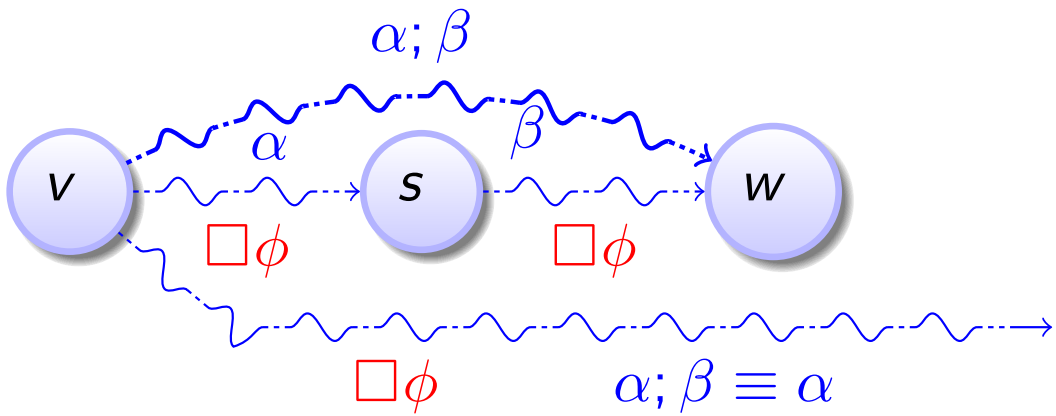


Modular Proof Calculus for Temporal dTL

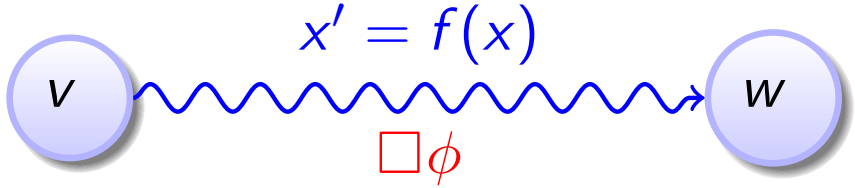
$$\frac{\phi \wedge [x := \theta]\phi}{[x := \theta]\Box\phi}$$



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

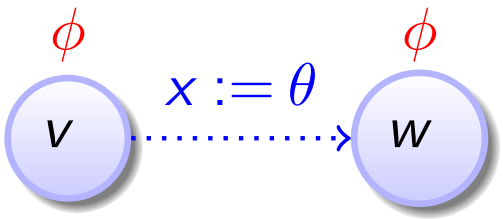


$$\frac{}{[x' = \theta]\Box\phi}$$

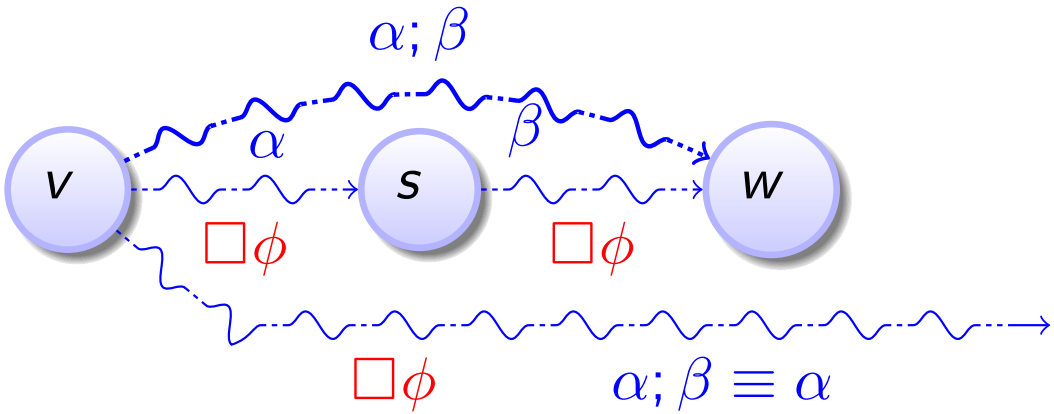


Modular Proof Calculus for Temporal dTL

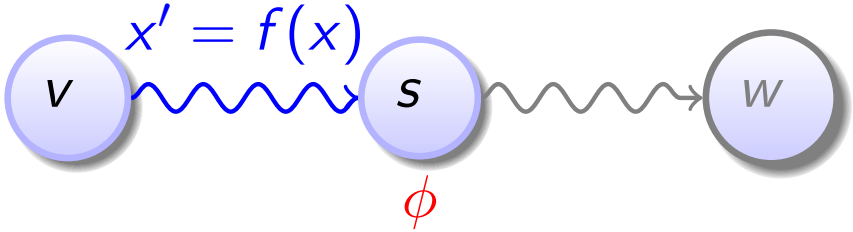
$$\frac{\phi \wedge [x := \theta]\phi}{[x := \theta]\Box\phi}$$



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

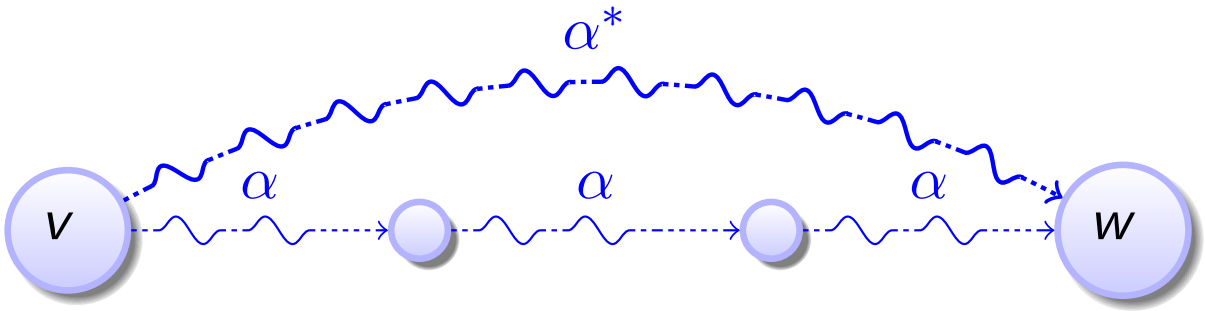


$$\frac{[x' = \theta]\phi}{[x' = \theta]\Box\phi}$$



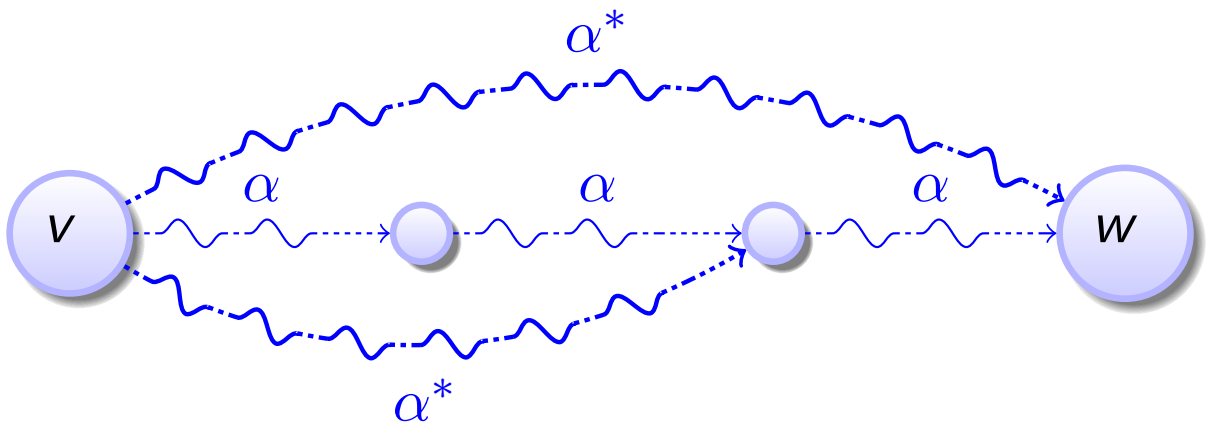
Modular Proof Calculus for Temporal dTL

$$\frac{}{[\alpha^*]\Box\phi}$$



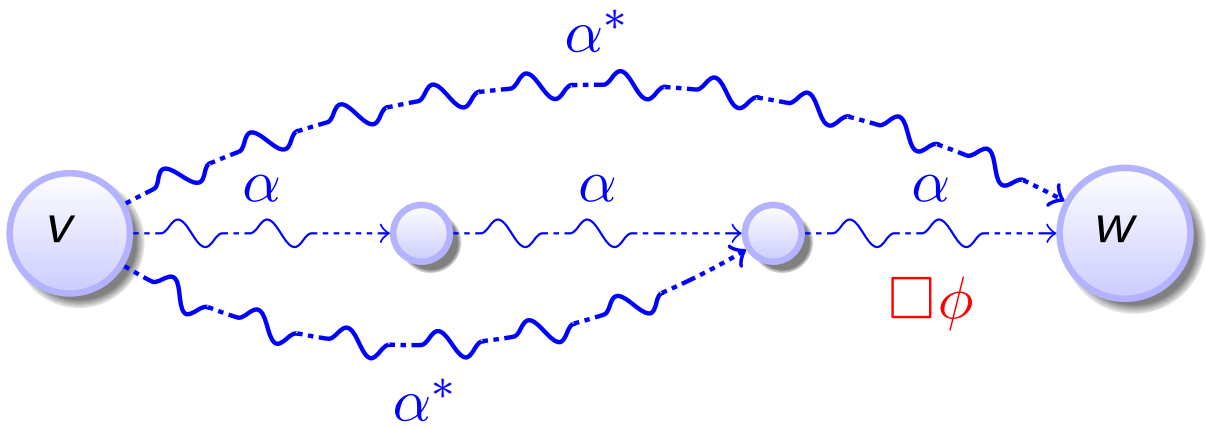
Modular Proof Calculus for Temporal dTL

$$\frac{[\alpha^*]}{[\alpha^*]\Box\phi}$$



Modular Proof Calculus for Temporal dTL

$$\frac{[\alpha^*][\alpha]\Box\phi}{[\alpha^*]\Box\phi}$$



10 temporal rules

(T1) $\dfrac{[\alpha]\Box\phi \land [\alpha][\beta]\Box\phi}{[\alpha;\beta]\Box\phi}$

(T2) $\dfrac{\phi}{[?\chi]\Box\phi}$

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

(T4) $\dfrac{[x' = \theta]\phi}{[x' = \theta]\Box\phi}$

(T5) $\dfrac{[\alpha;\alpha^*]\Box\phi}{[\alpha^*]\Box\phi}$

(T6) $\dfrac{\langle\alpha\rangle\Diamond\phi \lor \langle\alpha\rangle\langle\beta\rangle\Diamond\phi}{\langle\alpha;\beta\rangle\Diamond\phi}$

(T7) $\dfrac{\phi}{\langle?\chi\rangle\Diamond\phi}$

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

(T9) $\dfrac{\langle x' = \theta\rangle\phi}{\langle x' = \theta\rangle\Diamond\phi}$

(T10) $\dfrac{\langle\alpha;\alpha^*\rangle\Diamond\phi}{\langle\alpha^*\rangle\Diamond\phi}$

10 non-temporal rules

(D1) $\dfrac{\langle\alpha\rangle\pi \vee \langle\beta\rangle\pi}{\langle\alpha \cup \beta\rangle\pi}$

(D2) $\dfrac{[\alpha]\pi \wedge [\beta]\pi}{[\alpha \cup \beta]\pi}$

(D3) $\dfrac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$

(D4) $\dfrac{\chi \wedge \phi}{\langle ?\chi\rangle\phi}$

(D5) $\dfrac{\chi \rightarrow \phi}{[?\chi]\phi}$

(D6) $\dfrac{\phi \vee \langle\alpha;\alpha^*\rangle\phi}{\langle\alpha^*\rangle\phi}$

(D7) $\dfrac{\phi \wedge [\alpha;\alpha^*]\phi}{[\alpha^*]\phi}$

(D8) $\dfrac{F_x^\theta}{[x := \theta]F}$

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

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

10 propositional rules

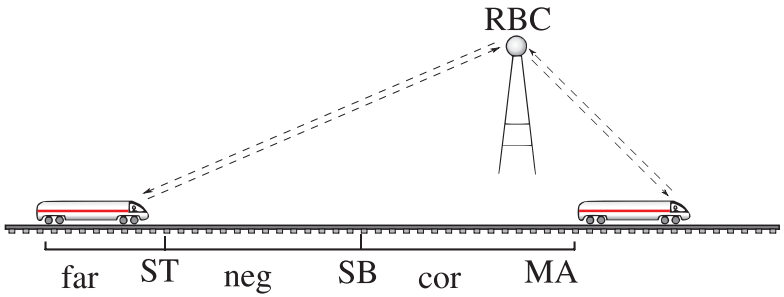
(P1) $\dfrac{\vdash \phi}{\neg\phi \vdash}$ (P4) $\dfrac{\phi, \psi \vdash}{\phi \wedge \psi \vdash}$ (P7) $\dfrac{\phi \vdash \quad \psi \vdash}{\phi \vee \psi \vdash}$

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

(P3) $\dfrac{\phi \vdash \psi}{\vdash \phi \rightarrow \psi}$ (P6) $\dfrac{\vdash \phi \quad \psi \vdash}{\phi \rightarrow \psi \vdash}$ (P9) $\dfrac{}{\phi \vdash \phi}$

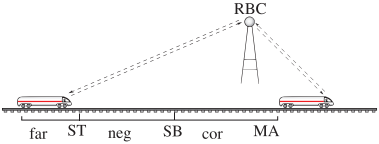
Verify Safety in Train Control

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



Verify Safety in Train Control

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



Proof

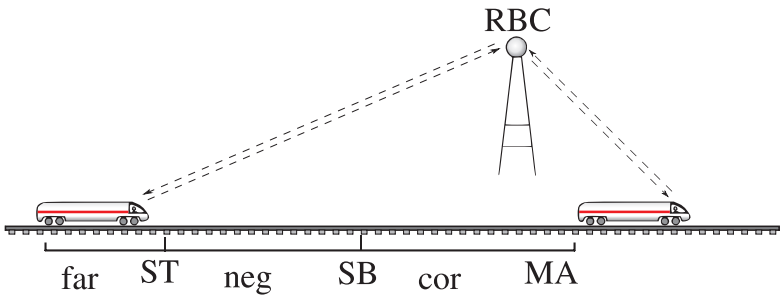
$$\psi \vdash Lv + z < MA$$
$$\psi \vdash \forall l{\geq}0\,(l \leq L \rightarrow lv + z < MA)$$
$$\psi \vdash \forall l{\geq}0\,[z := lv + z, \ell := l]\phi$$
$$\psi \vdash [neg]\phi$$
$$\psi \vdash [neg]\Box\phi$$

$$\psi, \ell{\geq}0 \vdash v^2 < 2b(MA - Lv - z)$$
$$\psi, \ell{\geq}0 \vdash [z := \ell v{+}z, a := \text{-}b]\forall t{\geq}0\,(\ell{\leq}L \rightarrow \tfrac{a}{2}t^2{+}vt{+}z{<}MA)$$
$$\psi, \ell{\geq}0 \vdash [z := \ell v{+}z, a := \text{-}b]\forall t{\geq}0\,[z := \tfrac{a}{2}t^2{+}vt{+}z]\phi)$$
$$\psi, \ell{\geq}0 \vdash [z := \ell v{+}z, a := \text{-}b][z'' = a]\Box\phi \qquad \triangleright$$
$$\psi, \ell{\geq}0 \vdash [z := \ell v{+}z][cor][z'' = a]\Box\phi \qquad \triangleright$$
$$\psi, \ell{\geq}0 \vdash [z := \ell v{+}z][cor; z'' = a]\Box\phi$$
$$\psi \vdash \ell{\geq}0 \rightarrow [z := \ell v{+}z][cor; z'' = a]\Box\phi$$
$$\psi \vdash \forall \ell{\geq}0\,[z := \ell v{+}z][cor; z'' = a]\Box\phi$$
$$\psi \vdash [neg][cor; z'' = a]\Box\phi$$

$$\psi \vdash [neg; cor; z'' = a]\Box\phi$$
$$\vdash \psi \rightarrow [neg; cor; z'' = a]\Box\phi$$

Verify Safety in Train Control

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



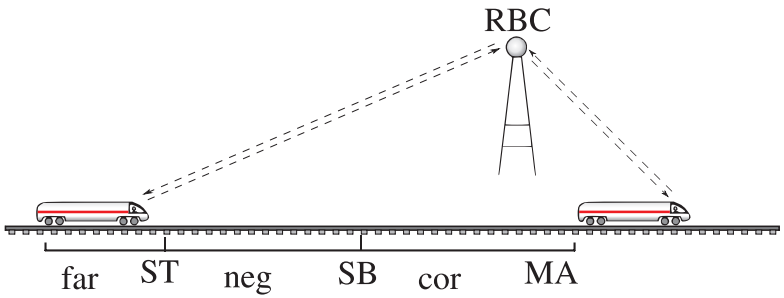
Proof

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

$$\dfrac{\psi \vdash [neg; cor; z'' = a]\Box\phi}{\vdash \psi \rightarrow [neg; cor; z'' = a]\Box\phi}$$

Verify Safety in Train Control

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



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

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

Soundness

Theorem (Soundness)

dTL *calculus is sound.*

Proposition (Incompleteness)

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

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

(Yet, reachability in hybrid systems is not semidecidable)

Completeness

Theorem (Relative completeness)

dTL *calculus is a sound & complete axiomatization of temporal properties of hybrid systems relative to (non-temporal)* d$\mathcal{L}$.

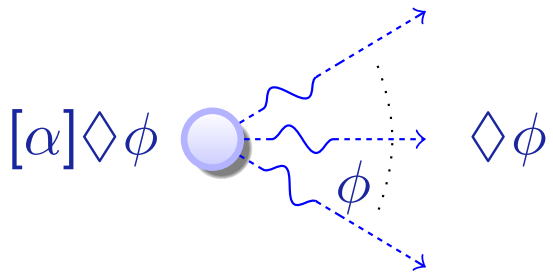
Outline

Conclusions (I)

Deductively verify temporal properties of operational hybrid systems

differential temporal dynamic logic

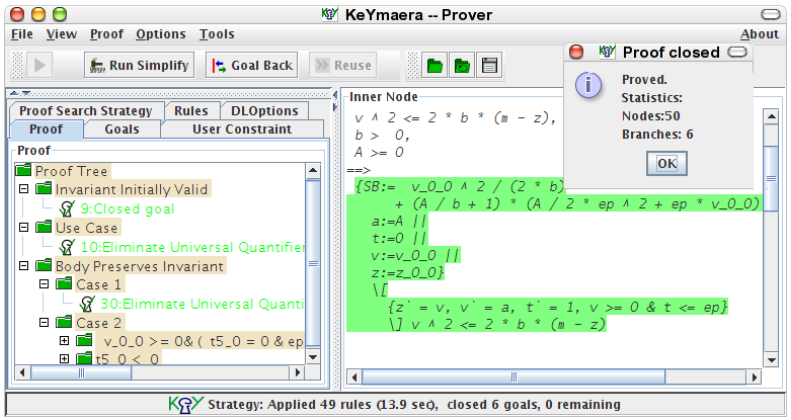
$$\text{dTL} = \text{TL} + \text{DL} + \text{HP}$$



problem	technique	OP	PAR	T	closed
$ETCS \models z < MA$	TL-MC	✓	×	✓	×
$\models (\text{Ax}(ETCS) \rightarrow z < MA)$	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 KeYmaera
- Parameter discovery



Landscape


Logical Analysis of Hybrid Systems
Logic
Proof Calculus
Theorem Proving
Model Checking
Algebra
Computer Algebra
Algebraic Geometry
Differential Algebra
Algorithms
Fixedpoint Loops
Proof Strategies
Decision Procedures
Analysis
Differential Equations
Dynamical Systems
Differen-tiation


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.


A. Platzer.
A temporal dynamic logic for verifying hybrid system invariants.
In S. N. Artëmov and A. Nerode, editors, *LFCS*, volume 4514 of *LNCS*, pages 457–471. Springer, 2007.