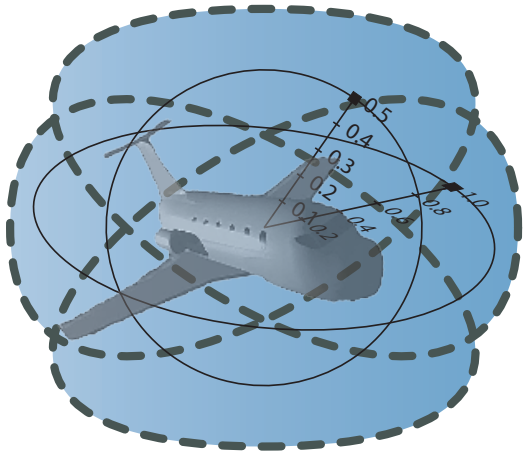
15-819/18-879: Logical Analysis of Hybrid Systems

15: Differential Dynamic Logic Proving

André Platzer

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



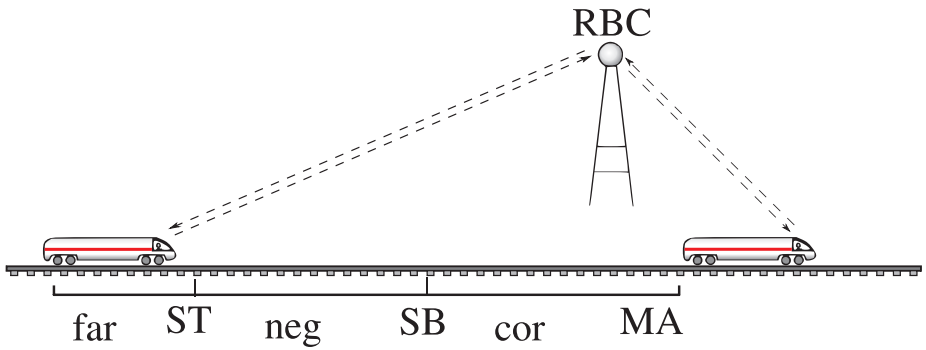
Outline

Outline

dℒ Design: The Logic of Hybrid Systems

differential dynamic logic

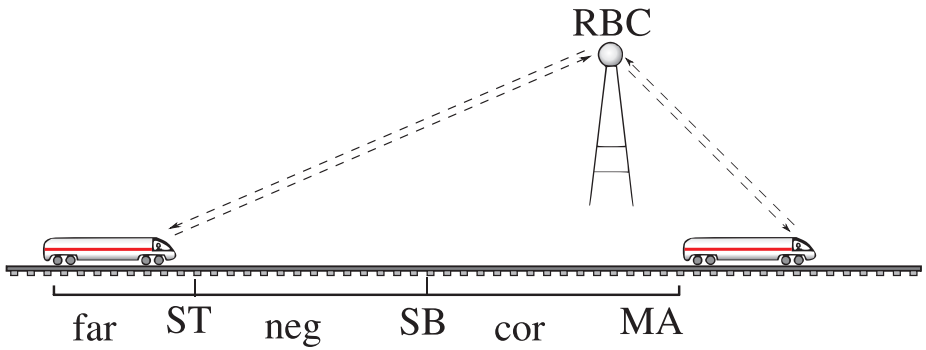
$$\mathsf{d}\mathcal{L} = \mathsf{DL} + \mathsf{HP}$$

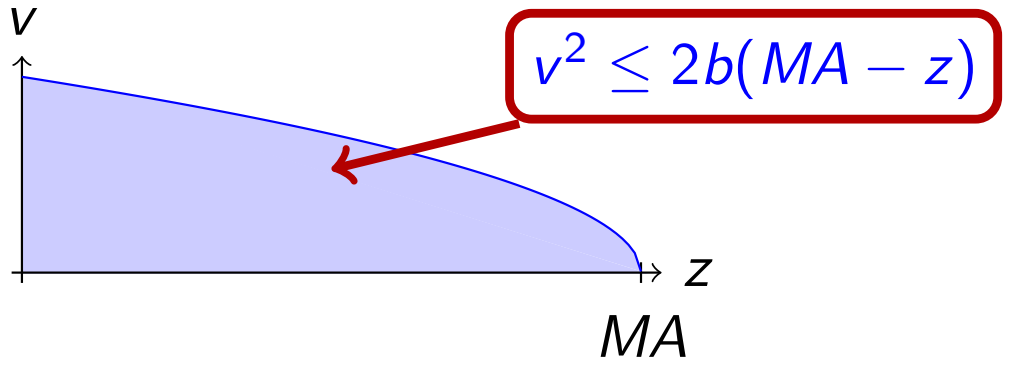


d$\mathcal{L}$ Design: Regions in First-Order Logic

differential dynamic logic

$\mathrm{d}\mathcal{L} = \mathrm{FOL}_{\mathbb{R}}$

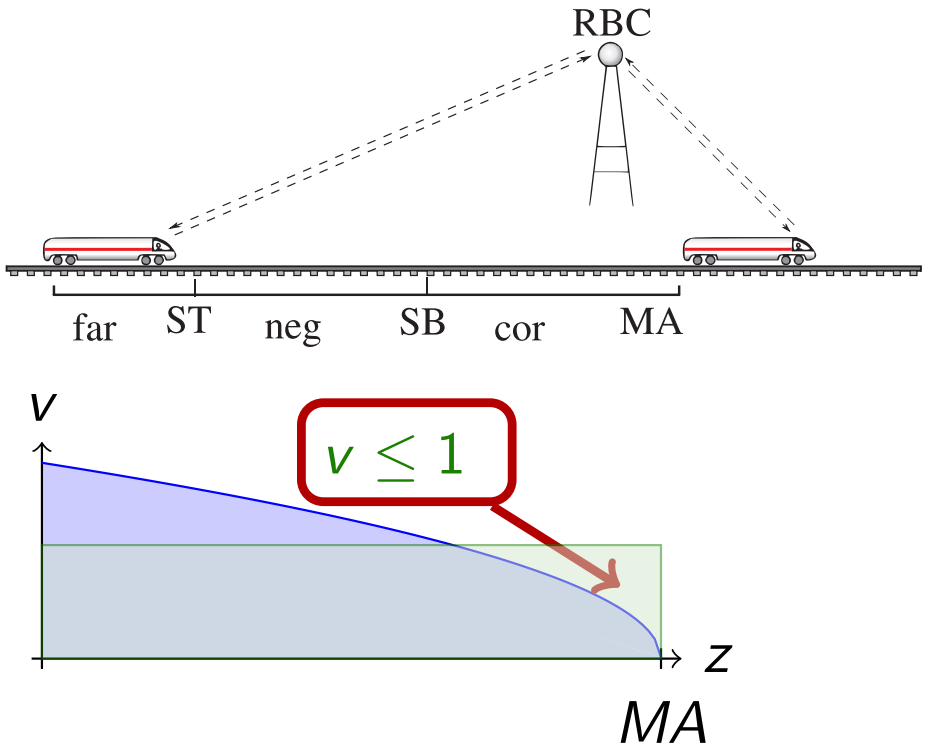




dℒ Design: Regions in First-Order Logic

differential dynamic logic

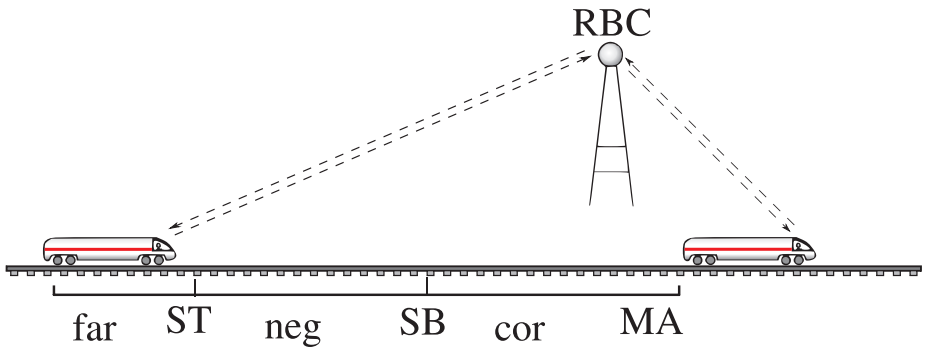
$$d\mathcal{L} = \text{FOL}_{\mathbb{R}}$$

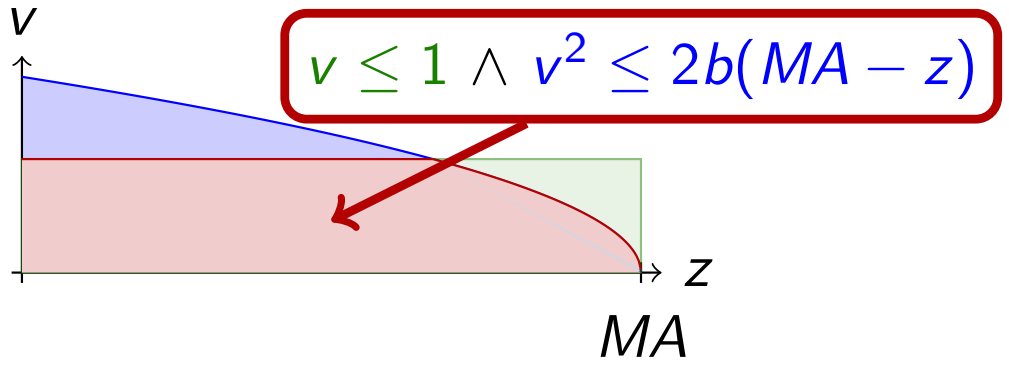


dℒ Design: Regions in First-Order Logic

differential dynamic logic

$d\mathcal{L} = \text{FOL}_{\mathbb{R}}$

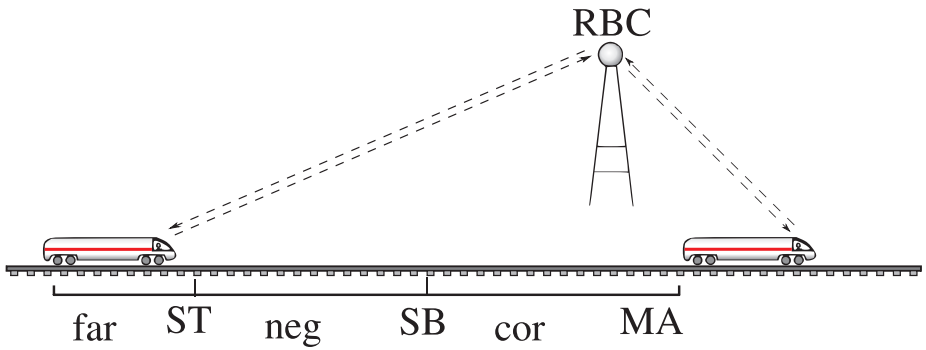


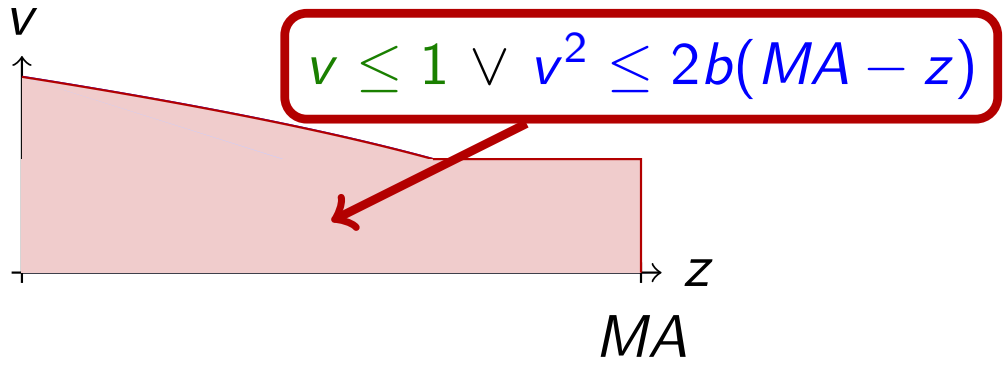


dℒ Design: Regions in First-Order Logic

differential dynamic logic

$d\mathcal{L} = \text{FOL}_{\mathbb{R}}$





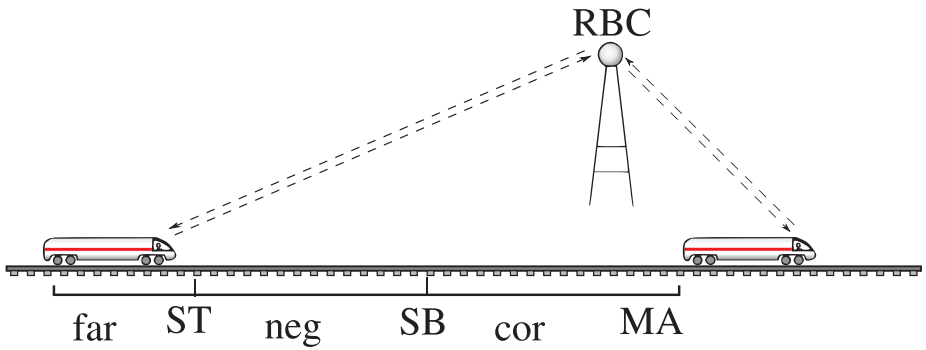
dℒ Design: Regions in First-Order Logic

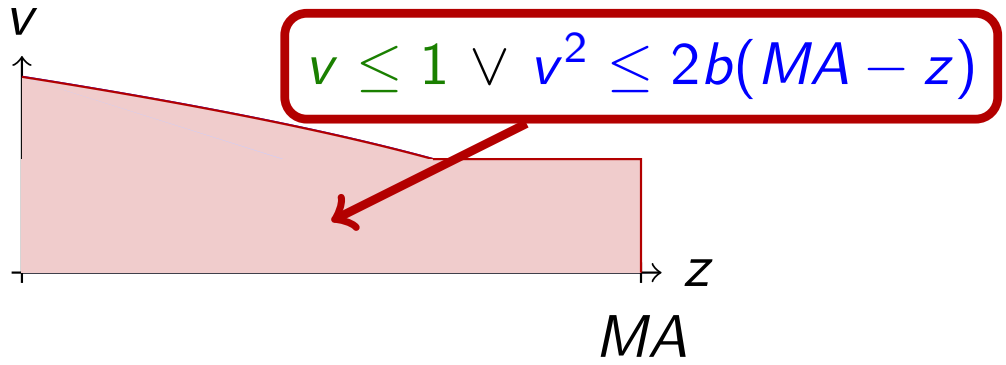
differential dynamic logic

$d\mathcal{L} = \text{FOL}_{\mathbb{R}}$

$\forall MA\, \exists SB\ \ldots$

$\forall t{\geq}0\ \ldots$

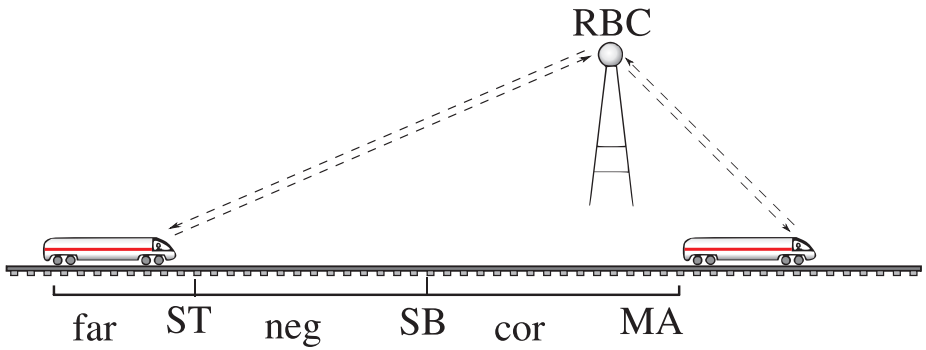


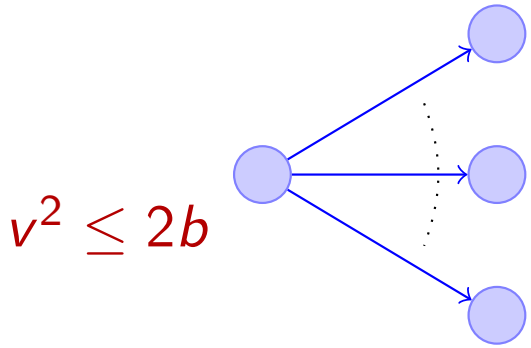


d$\mathcal{L}$ Design: State Transitions in Dynamic Logic

differential dynamic logic

$\mathsf{d}\mathcal{L} = \mathsf{FOL}_{\mathbb{R}} +$

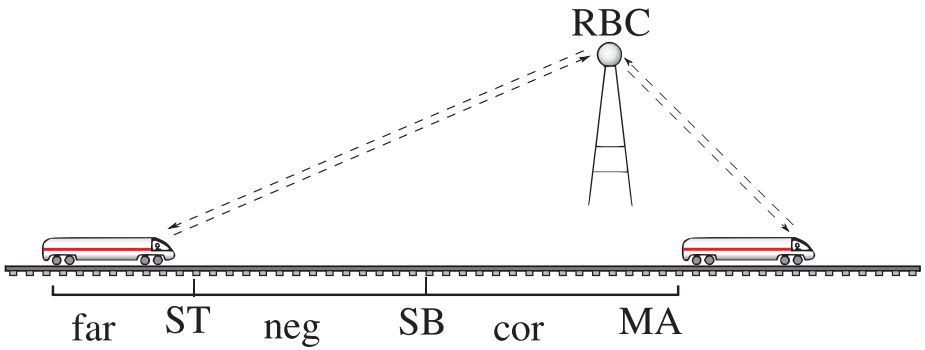


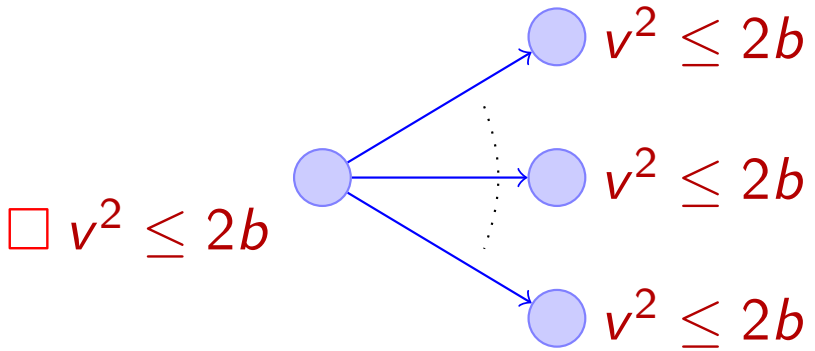


d$\mathcal{L}$ Design: State Transitions in Dynamic Logic

differential dynamic logic

$\mathsf{d}\mathcal{L} = \mathsf{FOL}_{\mathbb{R}} + \mathsf{ML}$

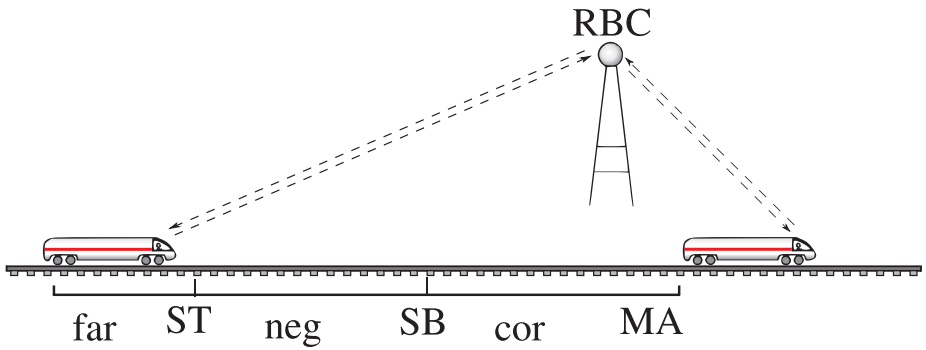


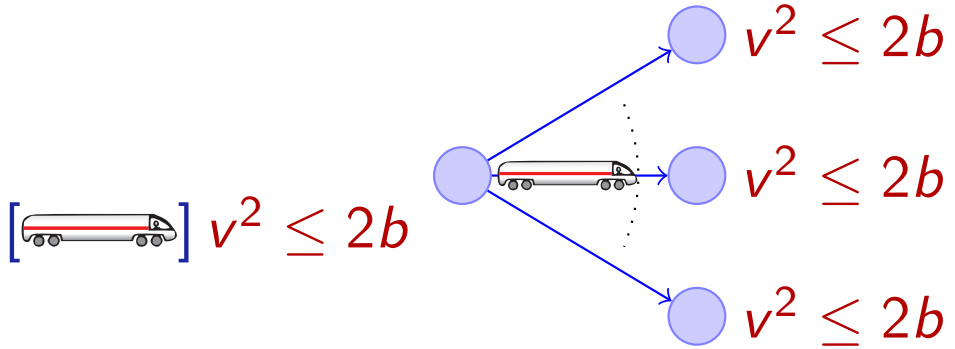


dℒ Design: State Transitions in Dynamic Logic

differential dynamic logic

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





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

Definition (d$\mathcal{L}$ Signature Σ)

Countable set of predicate or function symbols along with natural numbers as arities containing $0, 1, +, \cdot, /, =, \leq, >, \geq, <$ for reals

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

Definition (d$\mathcal{L}$ Signature Σ)

Countable set of predicate or function symbols along with natural numbers as arities containing $0, 1, +, \cdot, /, =, \leq, >, \geq, <$ for reals

Definition (d$\mathcal{L}$ Term t)

$t ::=$

x	for variable $x \in V$
$f(t_1, \ldots, t_n)$	for function $f/n \in \Sigma$ of arity $n \geq 0$

Differential Dynamic Logic dℒ: Syntax

Definition (dℒ Signature Σ)

Countable set of predicate or function symbols along with natural numbers as arities containing $0, 1, +, \cdot, /, =, \leq, >, \geq, <$ for reals

Definition (dℒ Formula ϕ, ψ)

$\phi ::=$

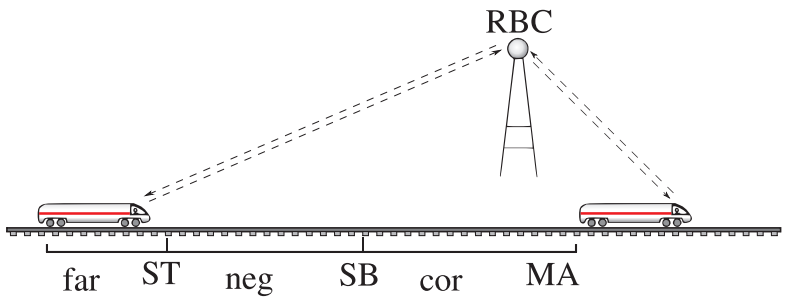
$[\alpha]\phi$	"all α reachables"
$\langle\alpha\rangle\phi$	"some α reachable"
$p(t_1, \ldots, t_n)$	for predicate $p/n \in \Sigma$ of arity $n \geq 0$
$\neg\phi$	"not"
$(\phi \wedge \psi)$	"and"
$(\phi \vee \psi)$	"or"
$(\phi \rightarrow \psi)$	"implies"
$\forall x\, \phi$	"universal quantifier/forall" for $x \in V$
$\exists x\, \phi$	"existential quantifier/exists" for $x \in V$

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

Definition (d$\mathcal{L}$ Formulas ϕ)

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

$$SB \geq \ldots \ \rightarrow\ [(ctrl\,;drive)^*]\, z \leq MA$$



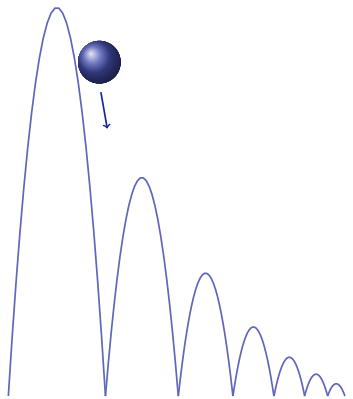
All trains respect *MA*
RBC partitions *MA*
$\Rightarrow$ system collision free

Differential Dynamic Logic dℒ: Ex. Moving Point

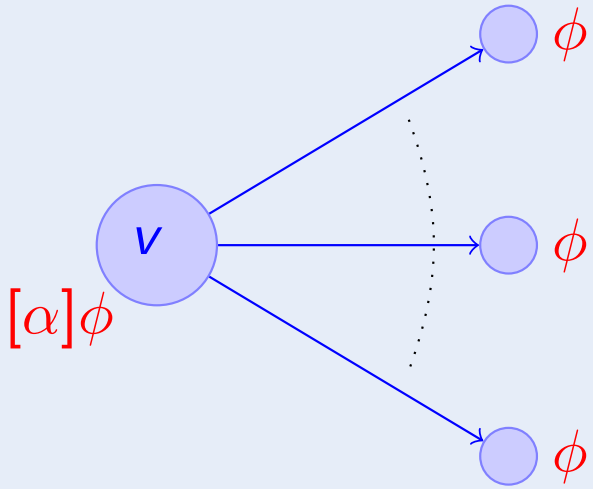
```
/* initial state characterization */
      x^2 < (4*c)^2 ->
[(
    if (x>0) then
        a := -4              /* move left */
    else
        a := 4               /* move right */
    fi;
    t := 0;                  /* reset clock variable t */
    {x'=a, t'=1, t<=c}       /* continuous evolution */
)*                           /* repeat these transitions */
] (x^2 <= (4*c)^2)           /* safety / postcondition */
```

Differential Dynamic Logic dℒ: Ex. Bouncing Ball

```
/* initial state characterization */
      g>0 & h>=0&t>=0 & v^2<=2*g*(H-h) & H>=0 ->
[(
    {h'=v,v'=-g,t'=1, h>=0}; /* falling/jumping */
    if (t>0 & h=0) then      /* if on ground */
        v := -c*v;           /* bounce back */
        t := 0
    fi
)*                           /* repeat these transitio
] (0<=h & h<=H)              /* safety / postcondition
```

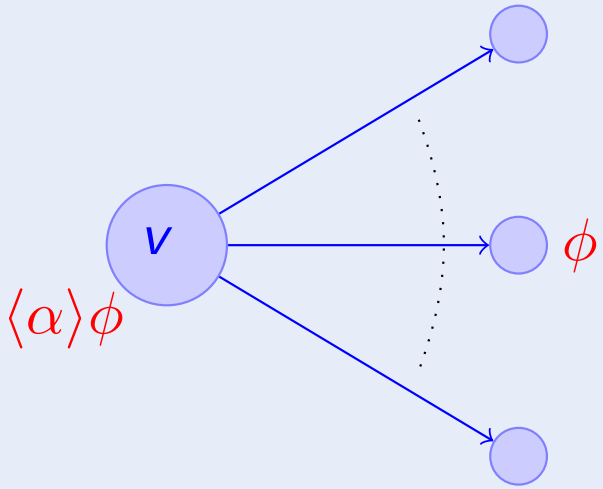


Definition (Formulas ϕ)



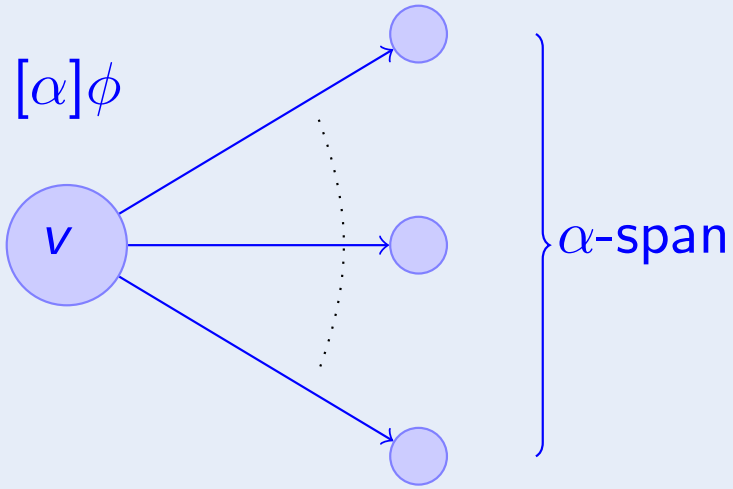
▸ Details ▸▸

Definition (Formulas ϕ)



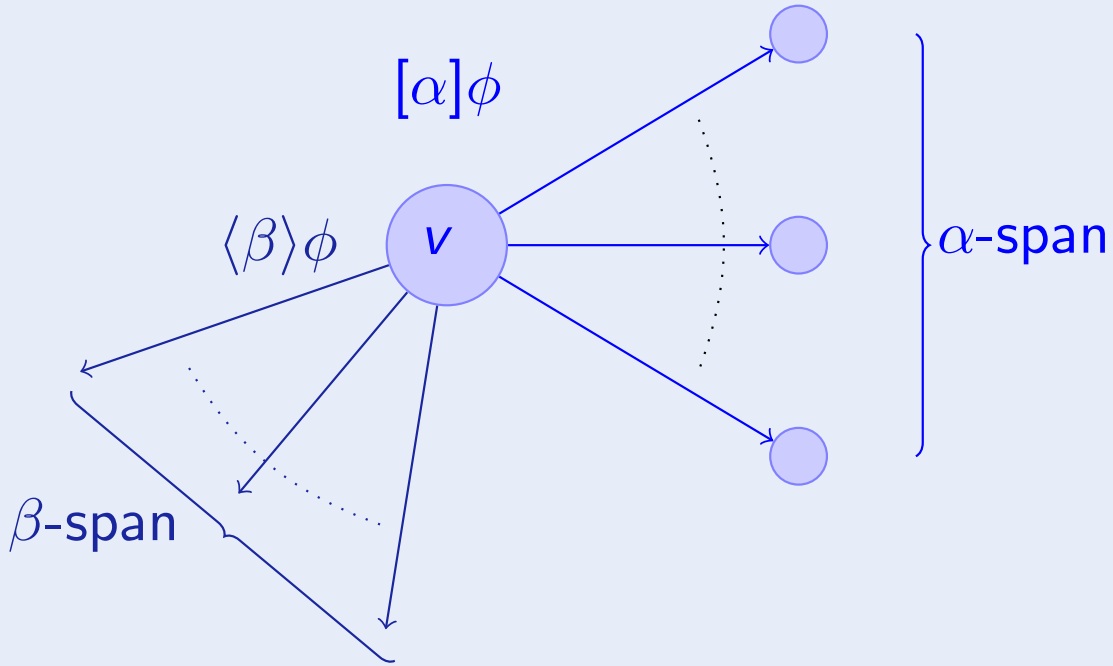
▸ Details ▸▸

Definition (Formulas ϕ)



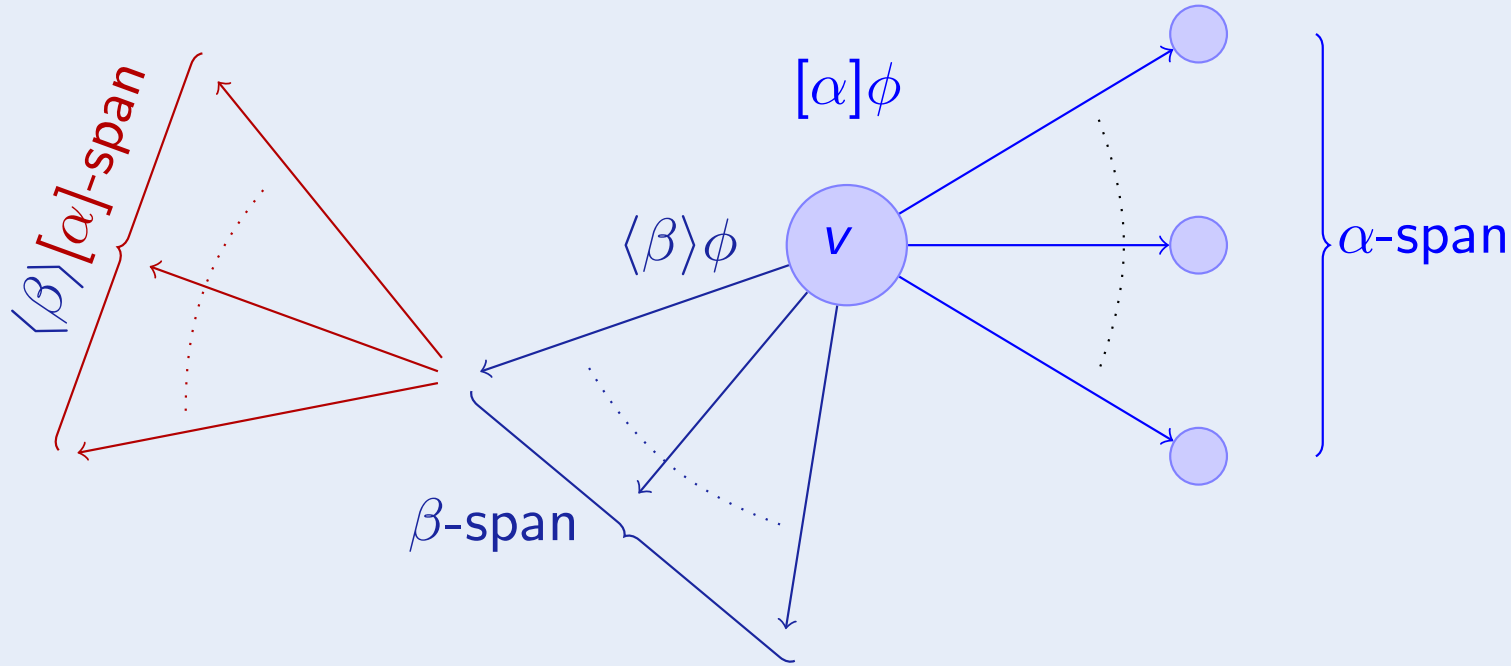
▸ Details ▸▸

Definition (Formulas ϕ)



▸ Details ▸▸

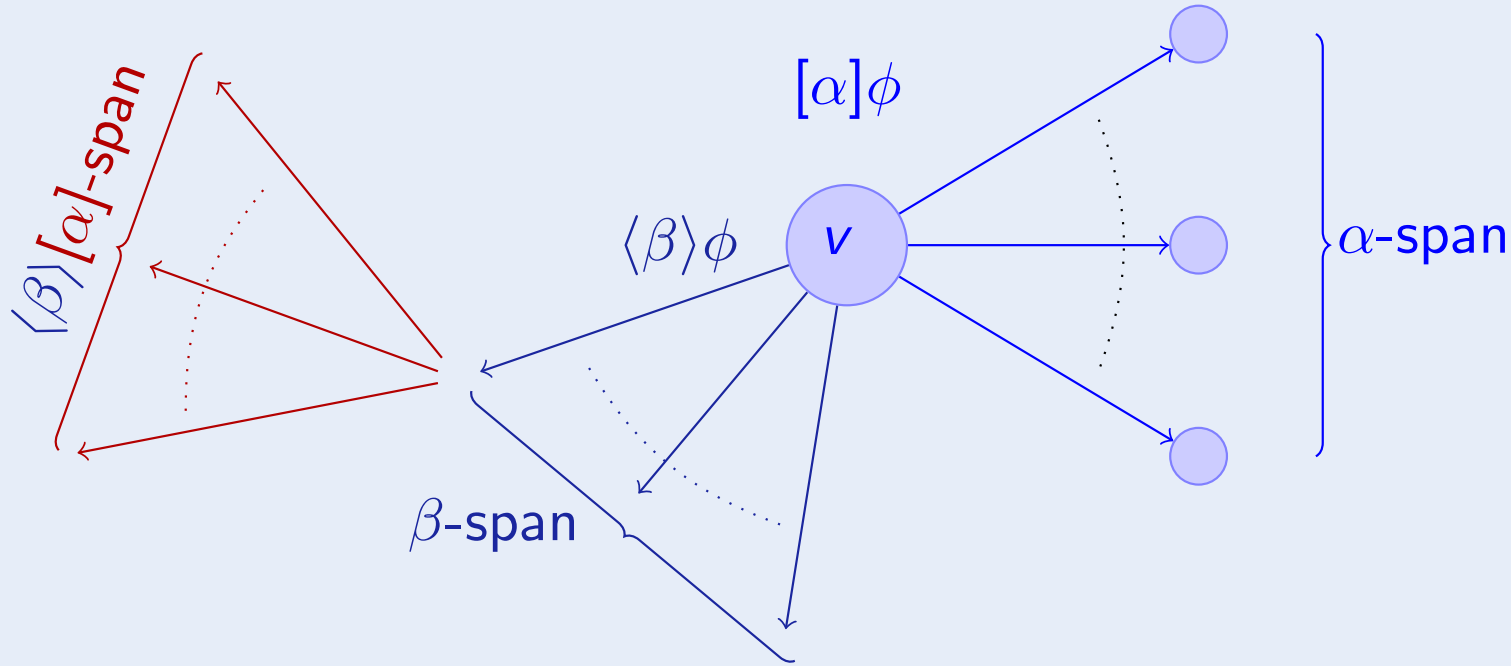
Definition (Formulas ϕ)



▸ Details ▸▸

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

Definition (Formulas ϕ)



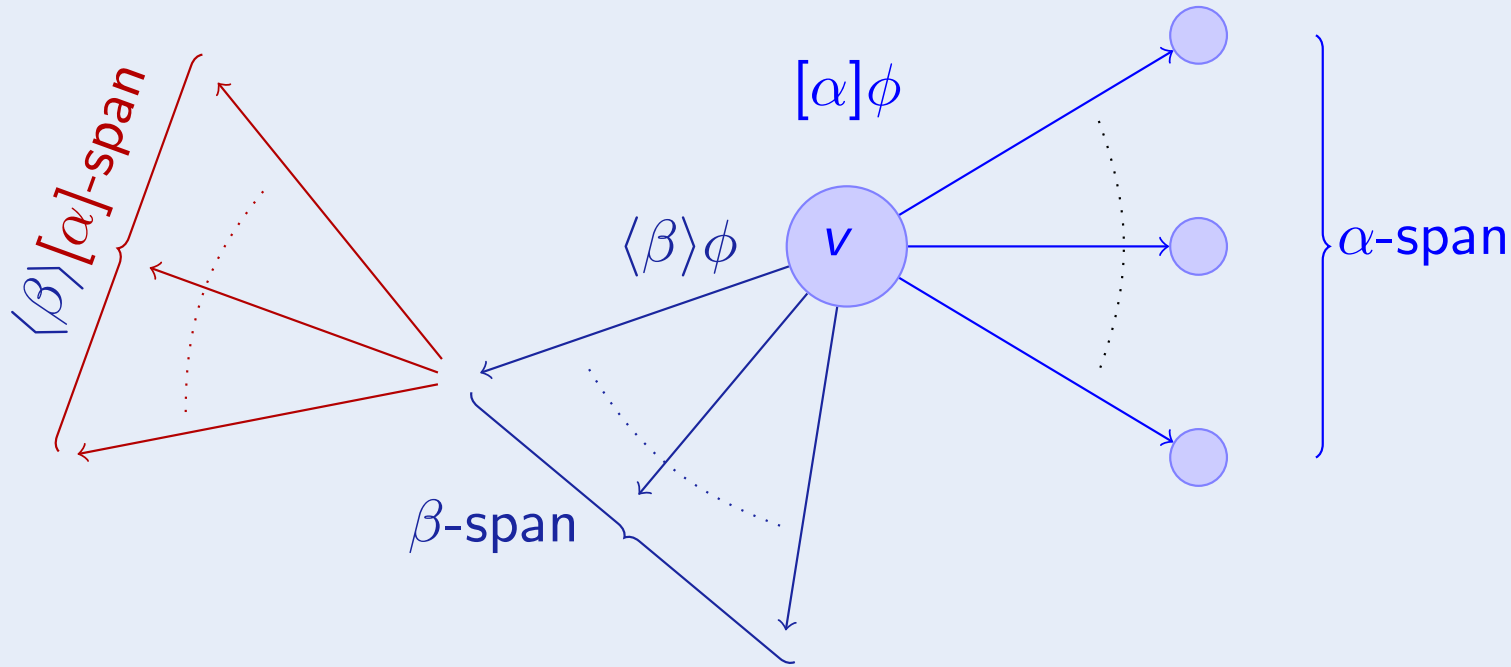
▸ Details ▸▸

compositional semantics $\Rightarrow$ compositional proofs!

Definition (Formulas ϕ)

$$
\begin{array}{lcl}
I,\eta,v \models \theta_1 \geq \theta_2 & :\Longleftrightarrow & [\![\theta_1]\!]_{I,v,\eta} \geq [\![\theta_2]\!]_{I,v,\eta} \\
I,\eta,v \models \phi \wedge \psi & :\Longleftrightarrow & I,\eta,v \models \phi \text{ and } I,\eta,v \models \psi \\
I,\eta,v \models \neg\phi & :\Longleftrightarrow & I,\eta,v \models \phi \text{ does not hold} \\
I,\eta,v \models \forall x\, \phi & :\Longleftrightarrow & I,\eta,w \models \phi \text{ for all } w \text{ that agree with } v \\
 & & \quad \text{except for the value of } x \\
I,\eta,v \models \exists x\, \phi & :\Longleftrightarrow & I,\eta,w \models \phi \text{ for some } w \text{ that agrees with } v \\
 & & \quad \text{except for the value of } x \\
I,\eta,v \models [\alpha]\phi & :\Longleftrightarrow & I,\eta,w \models \phi \quad \text{for all } w \text{ with } (v,w) \in \rho_I(\alpha) \\
I,\eta,v \models \langle\alpha\rangle\phi & :\Longleftrightarrow & I,\eta,w \models \phi \quad \text{for some } w \text{ with } (v,w) \in \rho_I(\alpha)
\end{array}
$$

Definition (Formulas ϕ)



▸ Details ▸▸

Nested Modalities

- $[RBC]\text{partitioned} \rightarrow \exists SB \langle \text{Train} \rangle [RBC]\text{safe}$

Nested Modalities

- $[RBC]\text{partitioned} \rightarrow \exists SB\, \langle \text{Train} \rangle [RBC]\text{safe}$
- $([\text{Train}]\text{safe}) \leftrightarrow \frac{v^2}{2b} \leq m - z \ldots$

Nested Modalities

- $[RBC]\text{partitioned} \rightarrow \exists SB\, \langle \text{Train} \rangle [RBC]\text{safe}$
- $([\text{Train}]\text{safe}) \leftrightarrow \frac{v^2}{2b} \leq m - z \ldots$
- $[\text{rbc}](M \rightarrow [\text{spd}]\langle SB := * \rangle [\text{atp}; \text{drive}]\text{safe})$

Nested Modalities

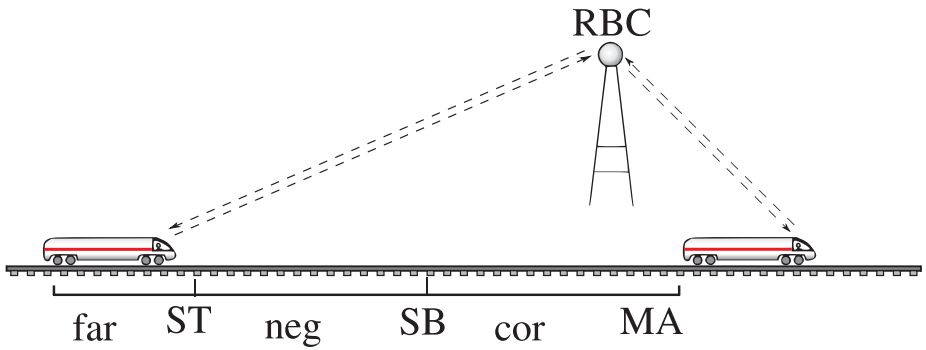
- $[RBC]\text{partitioned} \rightarrow \exists SB\, \langle \text{Train} \rangle [RBC]\text{safe}$
- $([\text{Train}]\text{safe}) \leftrightarrow \frac{v^2}{2b} \leq m - z \ldots$
- $[\text{rbc}](M \rightarrow [\text{spd}]\langle SB := * \rangle [\text{atp}; \text{drive}]\text{safe})$
- $[\text{aircraft}_1]\langle \text{aircraft}_2 \rangle \text{separate}$

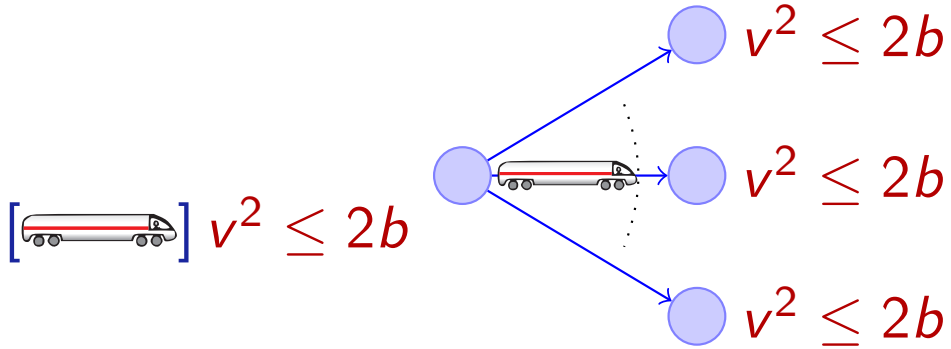
Outline

dℒ Design: State Transitions in Dynamic Logic

differential dynamic logic

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

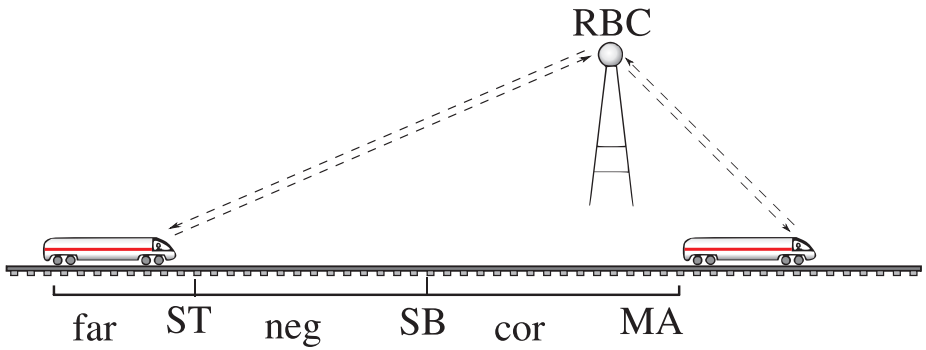




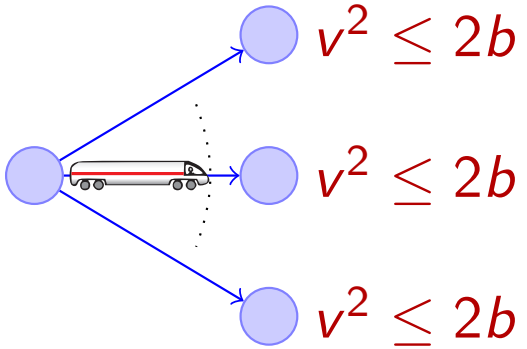
dℒ Design: Hybrid Programs as Uniform Model

differential dynamic logic

$$\mathsf{d}\mathcal{L} = \mathsf{FOL}_{\mathbb{R}} + \mathsf{DL} + \mathsf{HP}$$



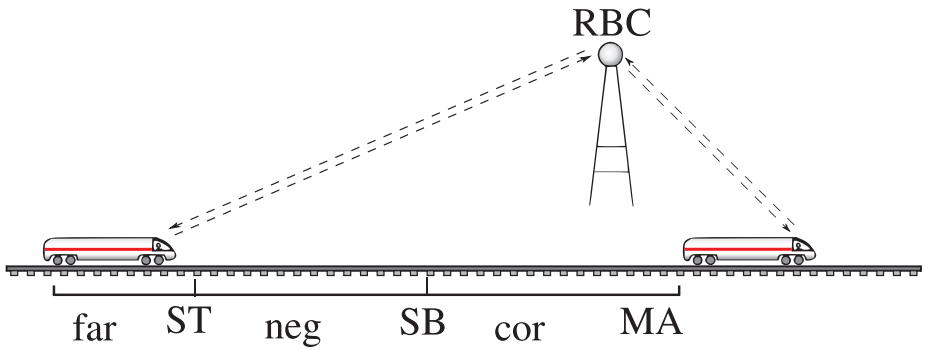
$[z'' = a]\, v^2 \leq 2b$



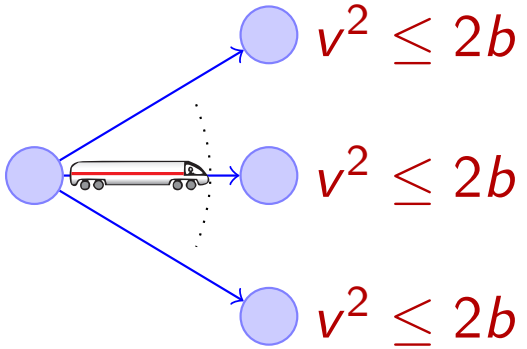
dℒ Design: Hybrid Programs as Uniform Model

differential dynamic logic

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



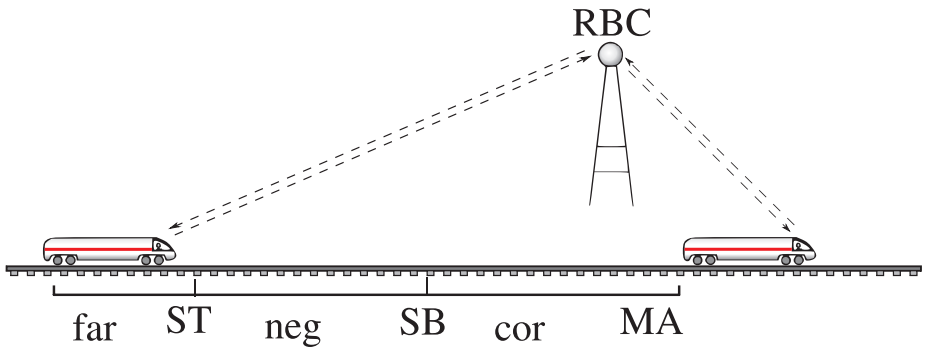
$$[\texttt{if}(z > SB)\, a := -b;\ z'' = a]\, v^2 \leq 2b$$



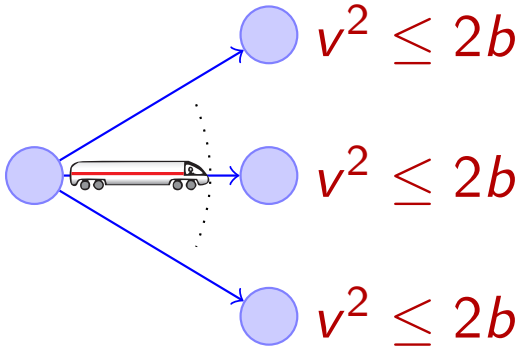
dℒ Design: Hybrid Programs as Uniform Model

differential dynamic logic

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



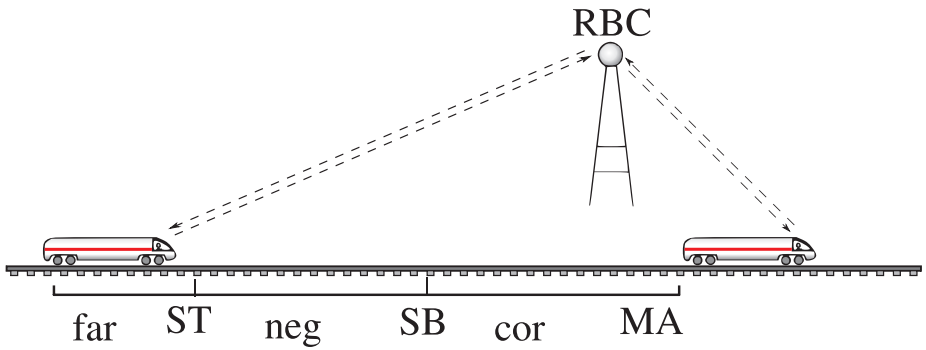
$$[\underbrace{\texttt{if}(z > SB)\, a := -b;\ z'' = a}_{\text{hybrid program}}]\, v^2 \leq 2b$$

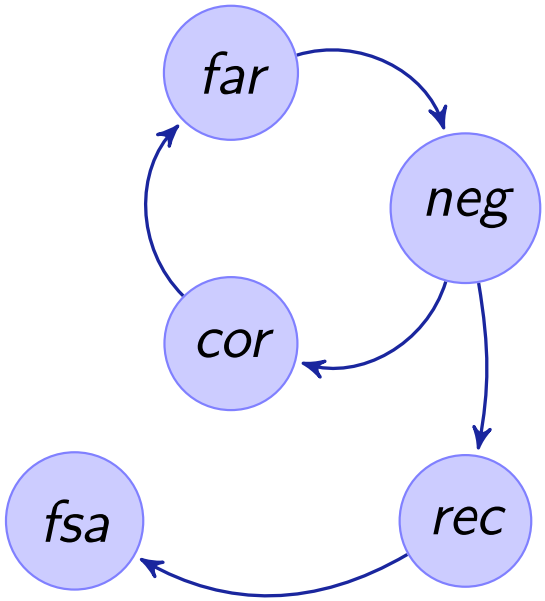


dℒ Design: What about Hybrid Automata?

differential dynamic logic

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



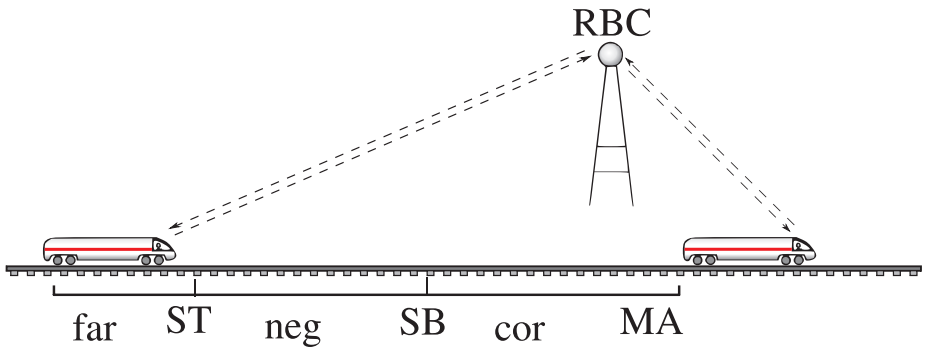


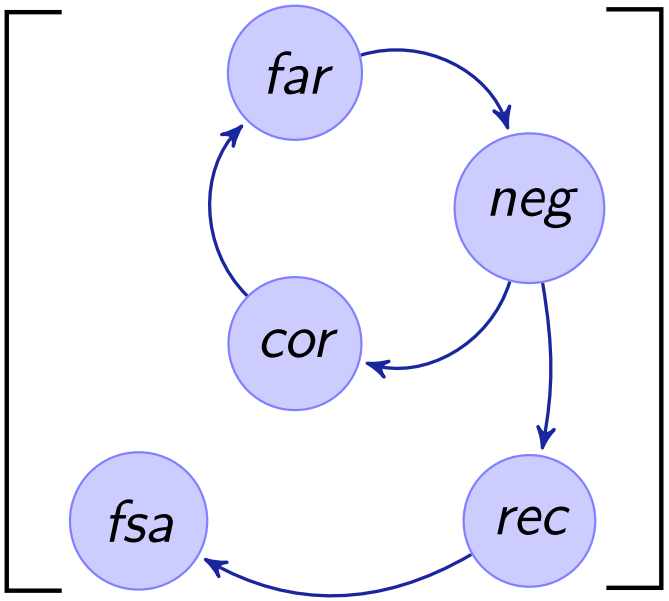
How about hybrid automata?

dℒ Design: What about Hybrid Automata?

differential dynamic logic

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



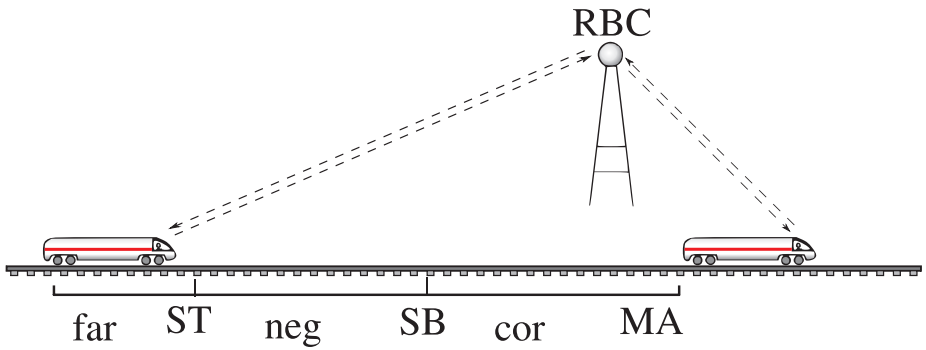


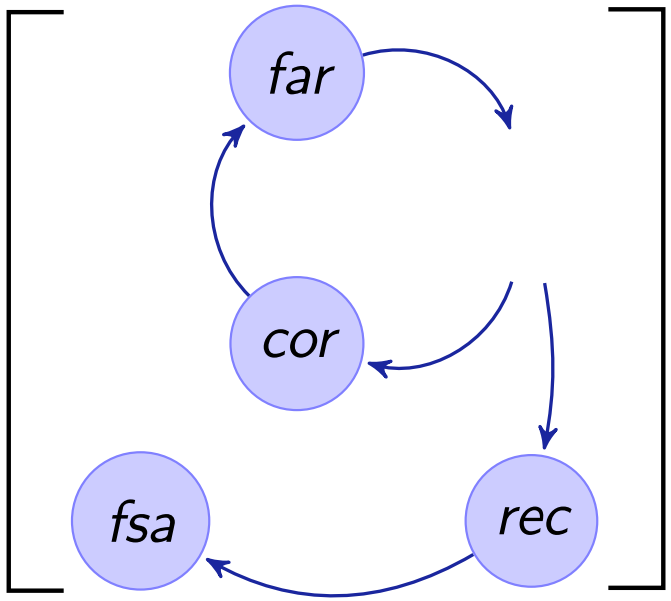
$v^2 \leq 2b\,..$

dℒ Design: What about Hybrid Automata?

differential dynamic logic

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



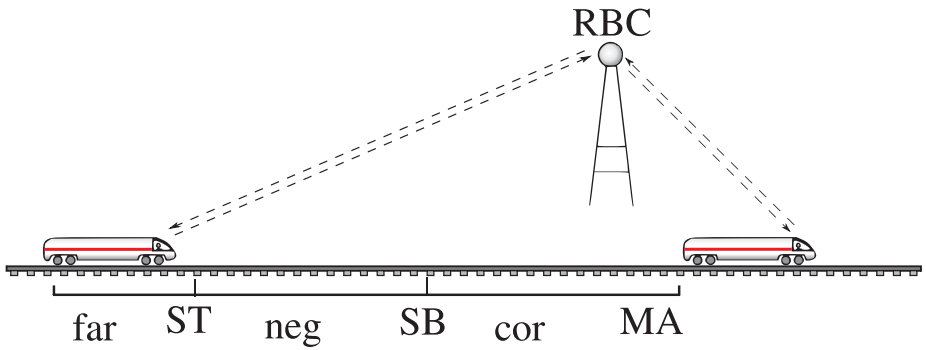


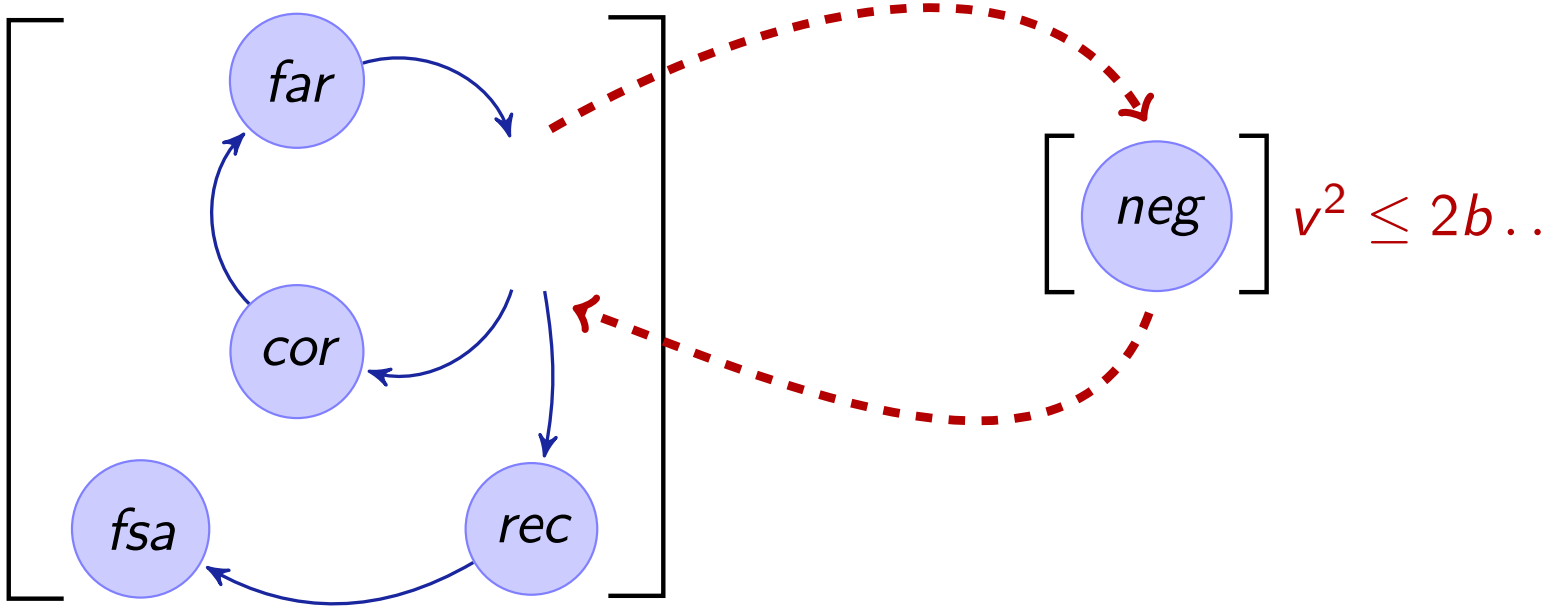
$$[\ \textit{neg}\ ]\ v^2 \leq 2b\,..$$

dℒ Design: What about Hybrid Automata?

differential dynamic logic

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

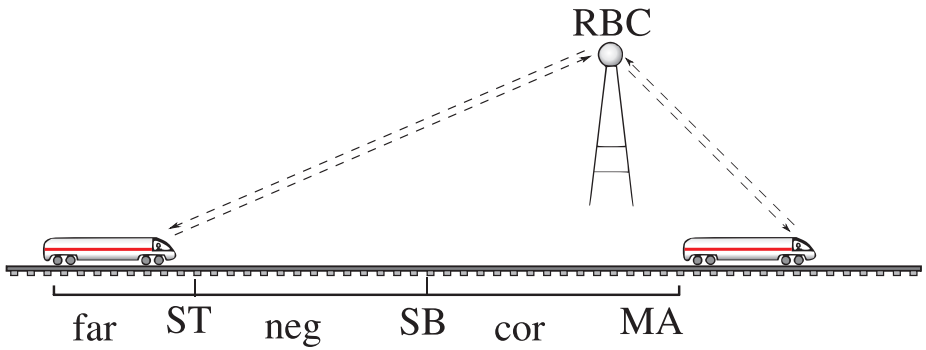


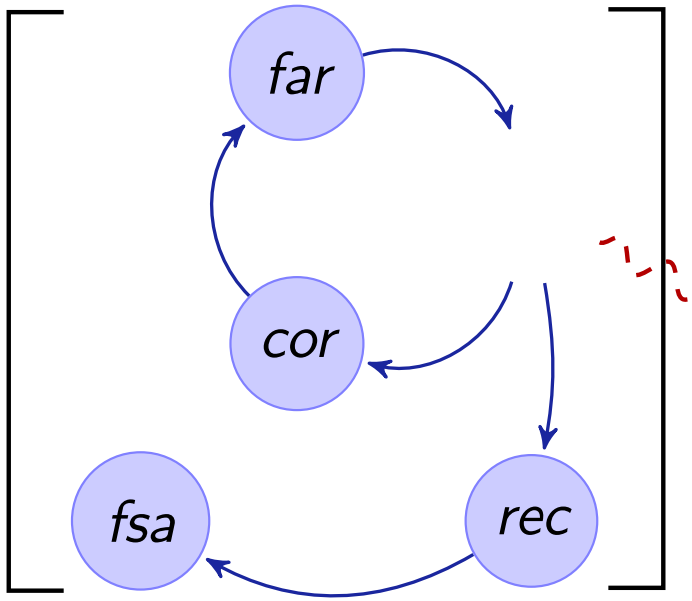


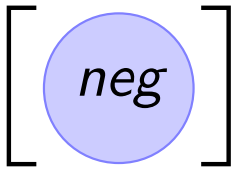
dℒ Design: What about Hybrid Automata?

differential dynamic logic

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



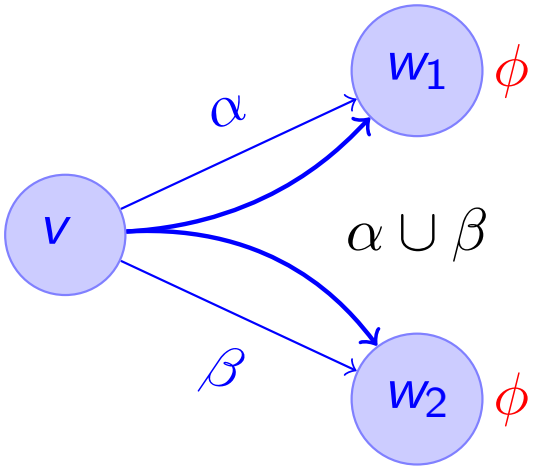




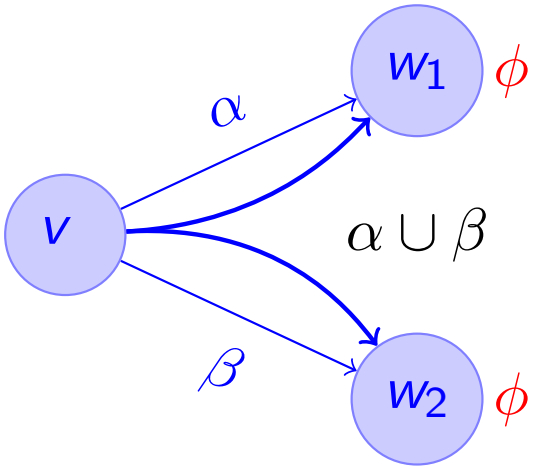
$v^2 \leq 2b\,..$

not compositional

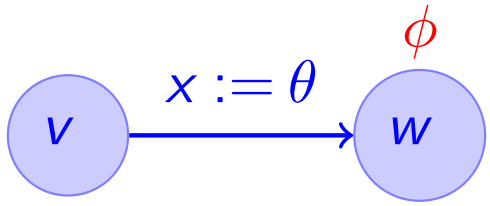
$$\frac{}{[\alpha \cup \beta]\phi}$$



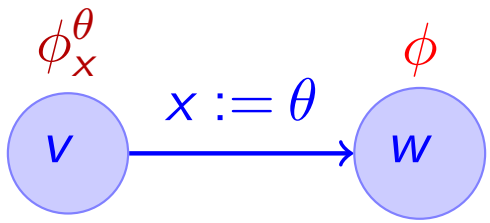
$$\frac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha \cup \beta]\phi}$$



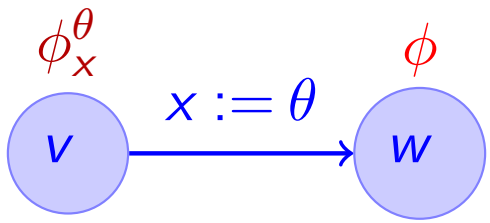
$$\overline{[x := \theta]\phi}$$



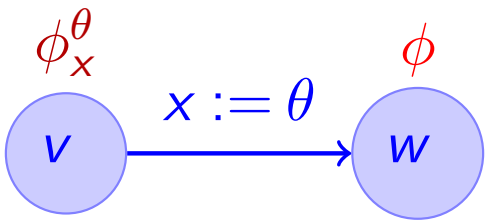
$$\overline{[x := \theta]\phi}$$



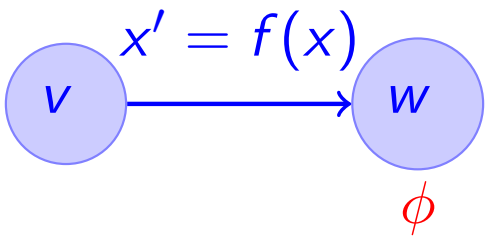
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$



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

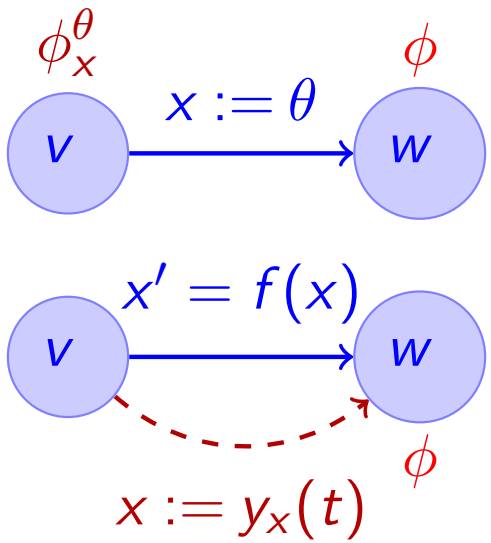


$$\frac{}{\langle x' = f(x)\rangle\phi}$$



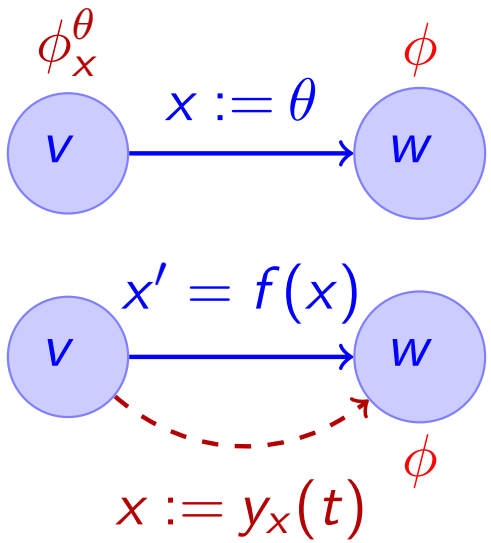
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$

$$\frac{}{\langle x' = f(x)\rangle\phi}$$

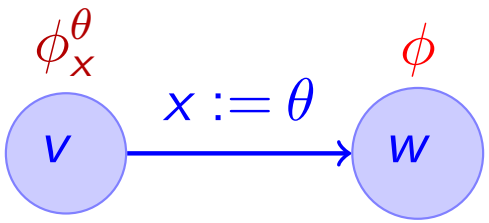


$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$

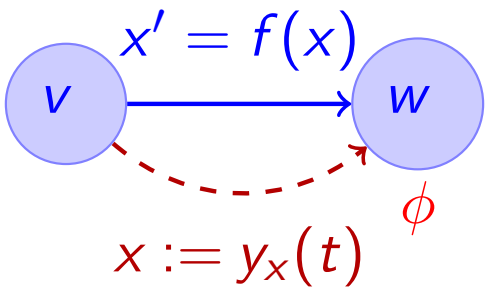
$$\frac{\exists t{\geq}0\, \langle x := y_x(t)\rangle\phi}{\langle x' = f(x)\rangle\phi}$$



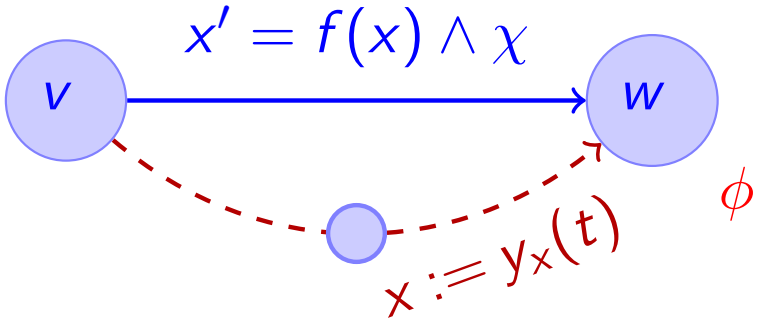
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$



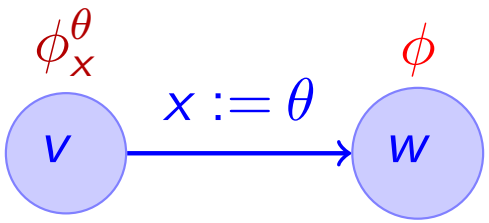
$$\frac{\exists t{\geq}0\, \langle x := y_x(t)\rangle\phi}{\langle x' = f(x)\rangle\phi}$$



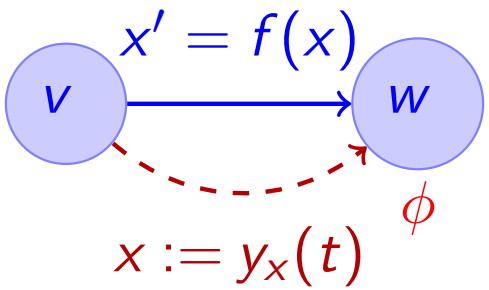
$$\frac{}{\langle x' = f(x) \wedge \chi\rangle\phi}$$



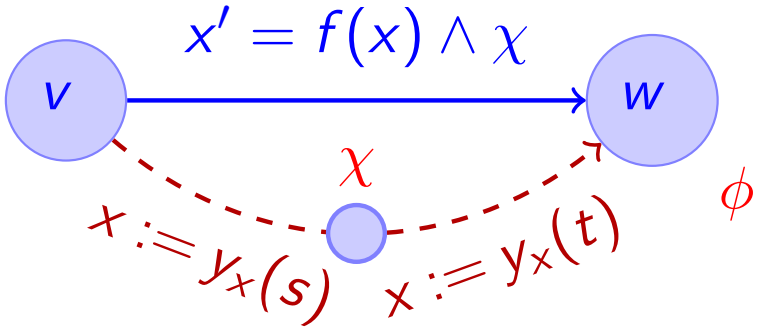
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$



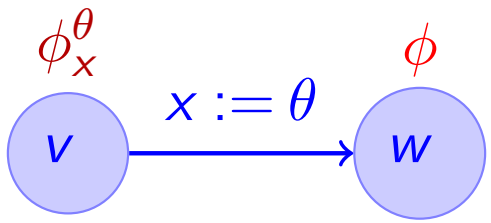
$$\frac{\exists t{\geq}0\, \langle x := y_x(t)\rangle\phi}{\langle x' = f(x)\rangle\phi}$$



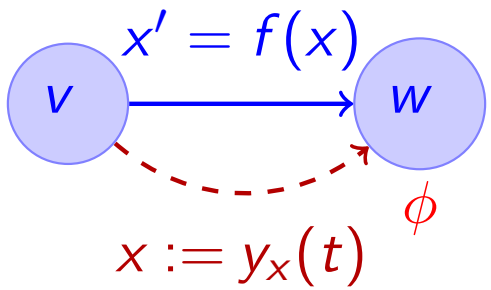
$$\frac{}{\langle x' = f(x) \wedge \chi\rangle\phi}$$



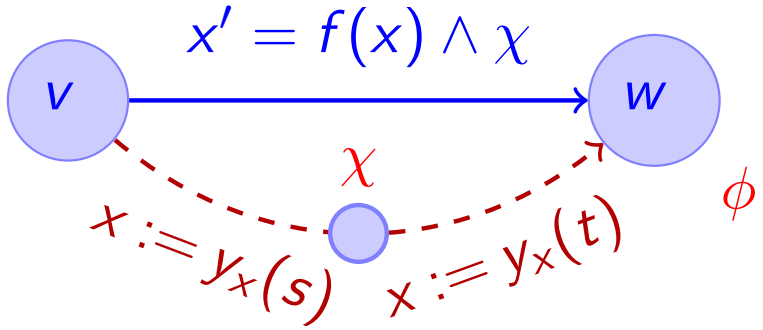
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$



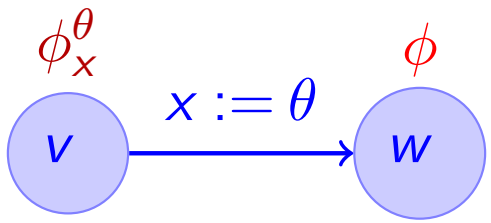
$$\frac{\exists t{\geq}0\, \langle x := y_x(t)\rangle\phi}{\langle x' = f(x)\rangle\phi}$$



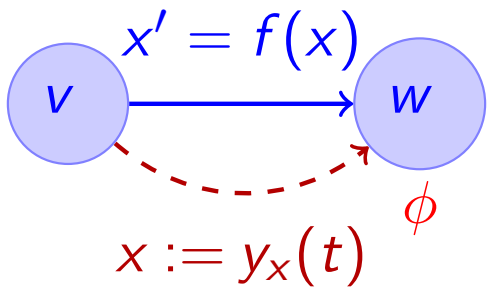
$$\frac{\exists t{\geq}0\, (\bar{\chi} \wedge \langle x := y_x(t)\rangle\phi)}{\langle x' = f(x) \wedge \chi\rangle\phi}$$



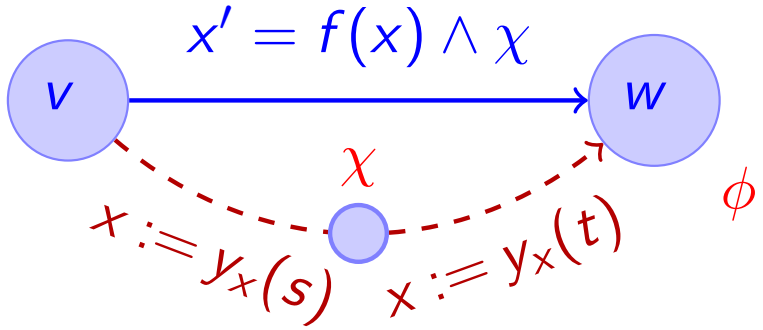
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$



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



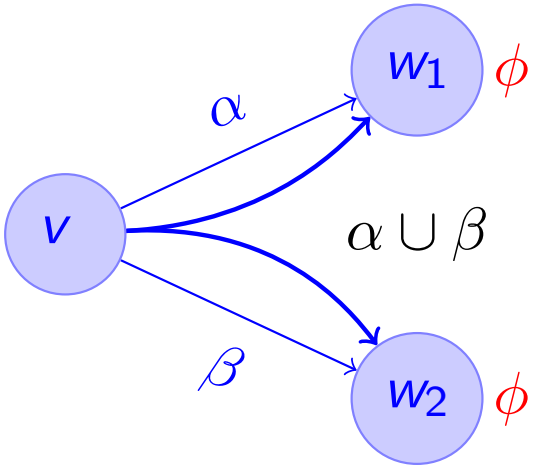
$$\frac{\exists t{\geq}0\, (\bar{\chi} \wedge \langle x := y_x(t)\rangle\phi)}{\langle x' = f(x) \wedge \chi\rangle\phi}$$



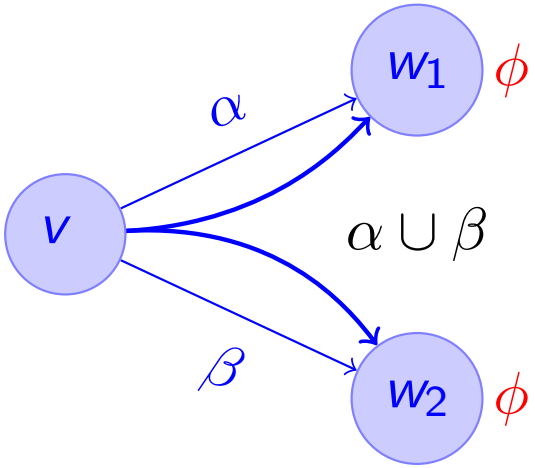
$$\bar{\chi} \;\equiv\; \forall 0{\leq}s{\leq}t\, \langle x := y_x(s)\rangle\chi$$

compositional semantics $\Rightarrow$ compositional rules!

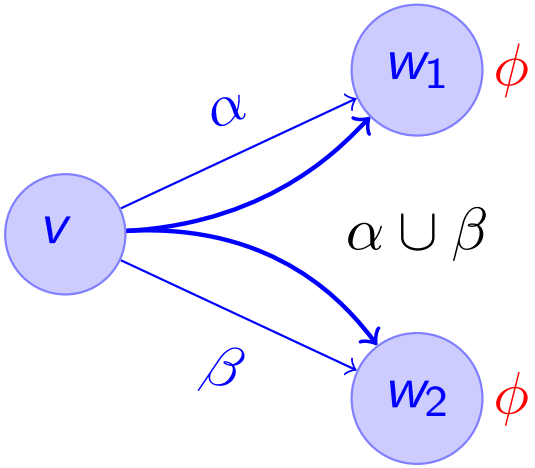
$$\frac{}{[\alpha \cup \beta]\phi}$$



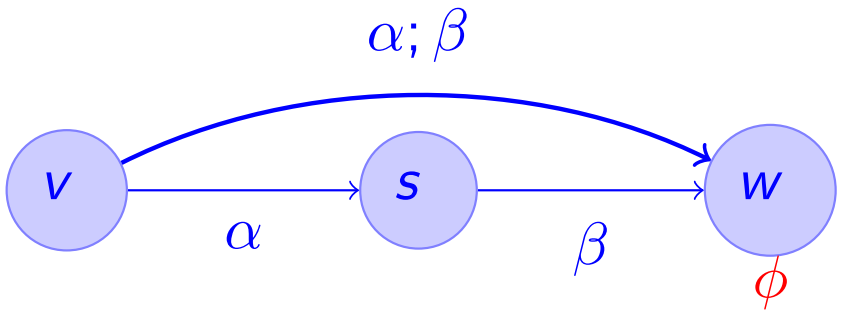
$$\frac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha \cup \beta]\phi}$$



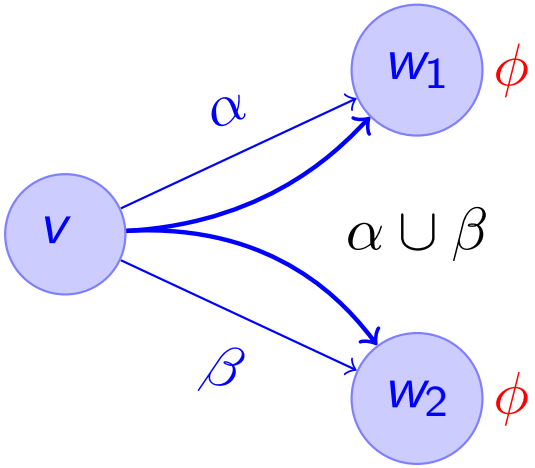
$$\frac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha \cup \beta]\phi}$$



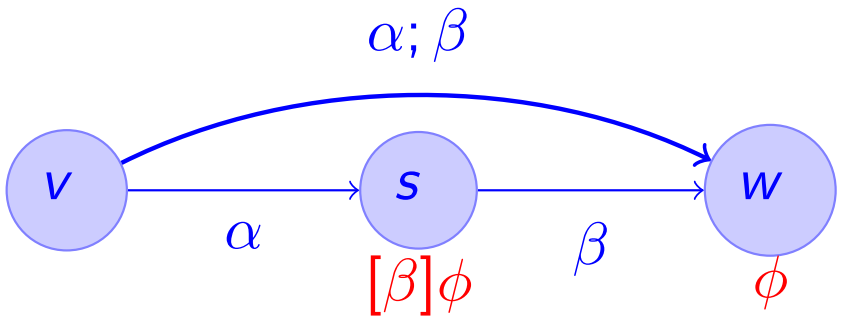
$$\overline{[\alpha;\beta]\phi}$$



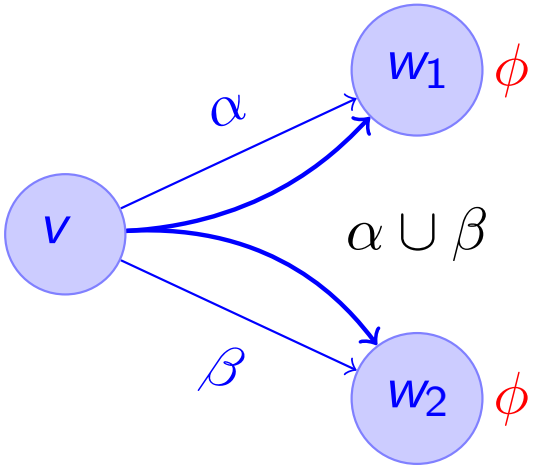
$$\frac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha \cup \beta]\phi}$$



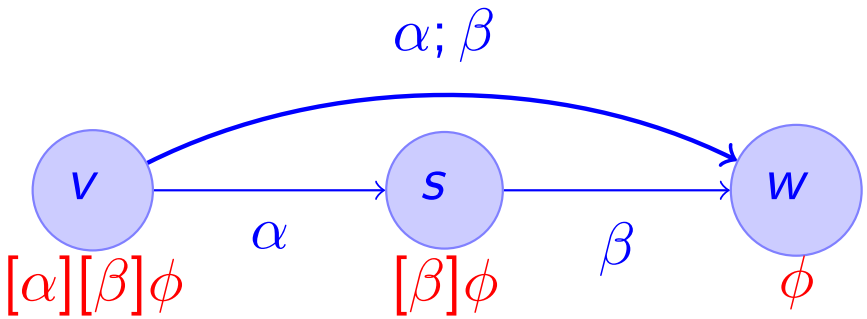
$$\overline{[\alpha;\beta]\phi}$$



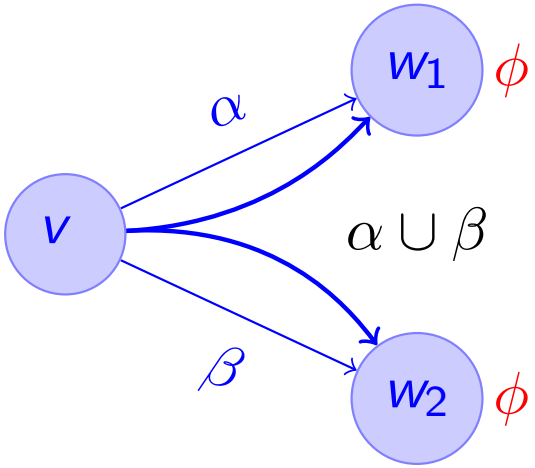
$$\frac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha \cup \beta]\phi}$$



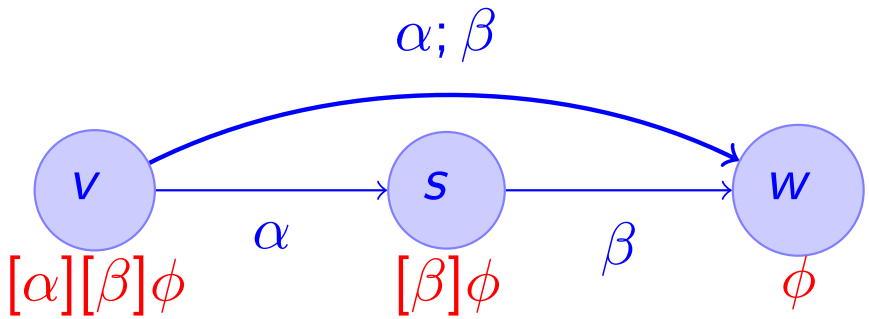
$$\overline{[\alpha;\beta]\phi}$$



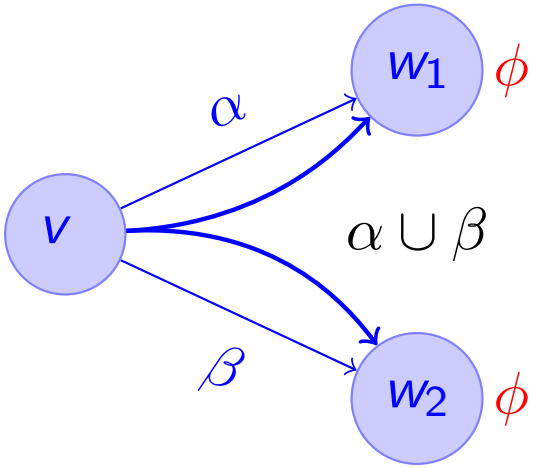
$$\frac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha \cup \beta]\phi}$$



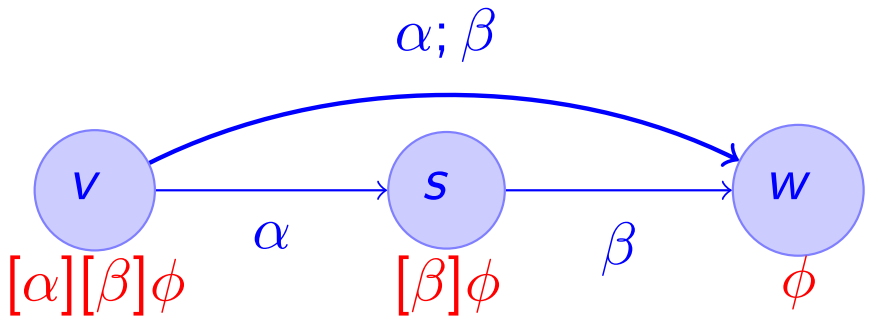
$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$



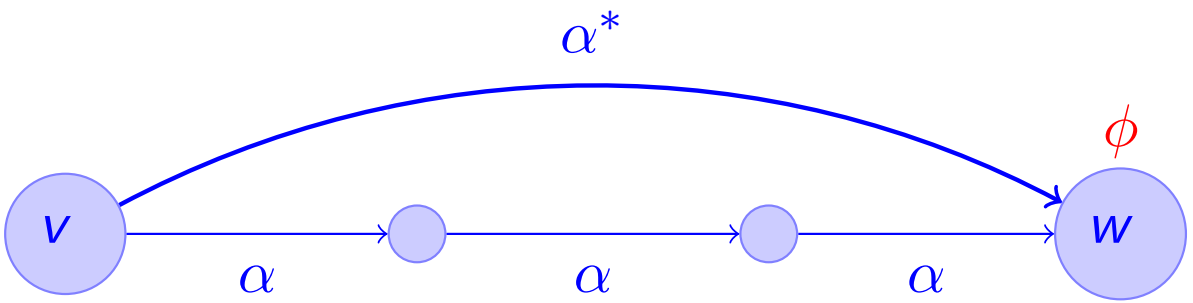
$$\frac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha \cup \beta]\phi}$$



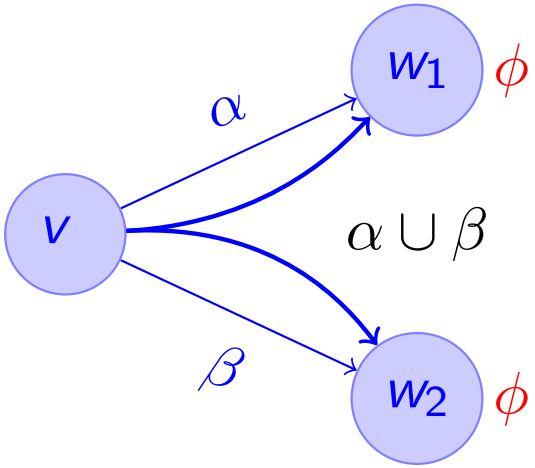
$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$



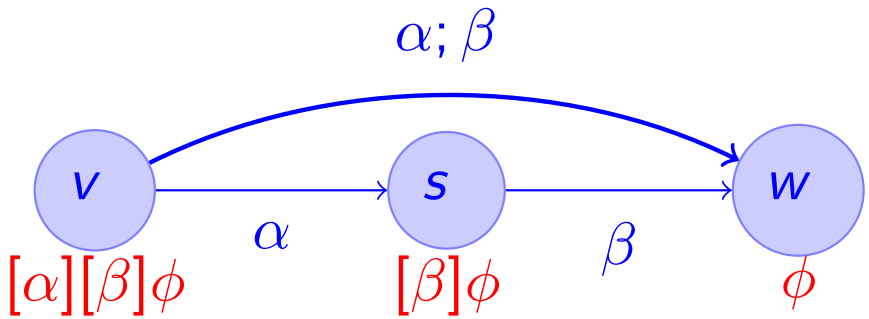
$$\frac{}{\vdash [\alpha^*]\phi}$$



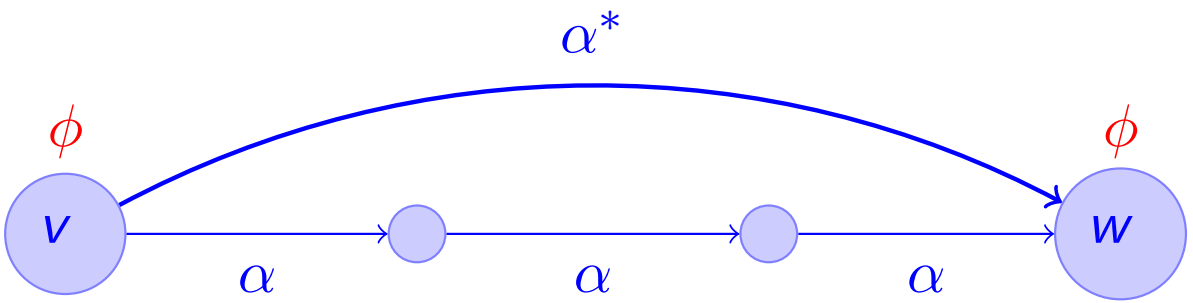
$$\frac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha \cup \beta]\phi}$$



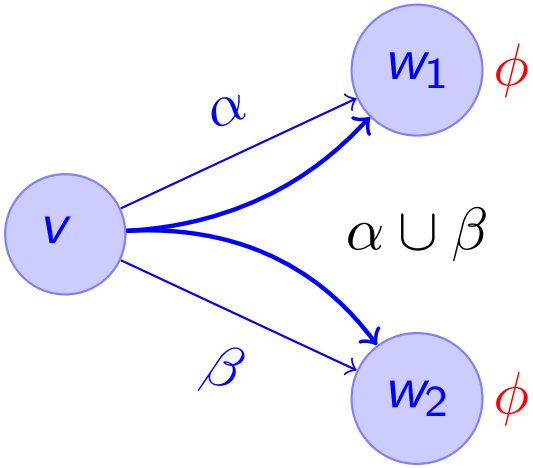
$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$



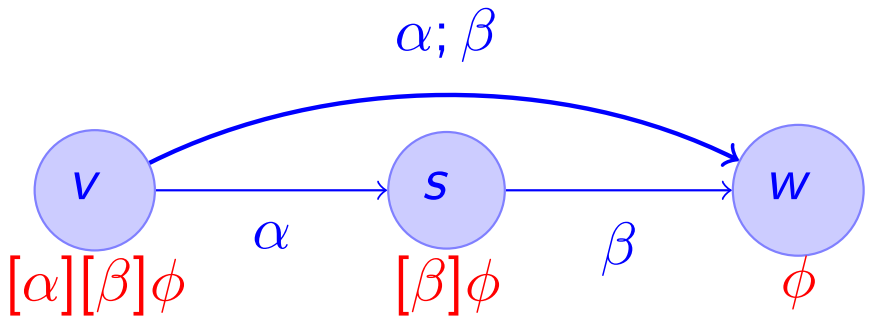
$$\frac{\vdash \phi}{\vdash [\alpha^*]\phi}$$



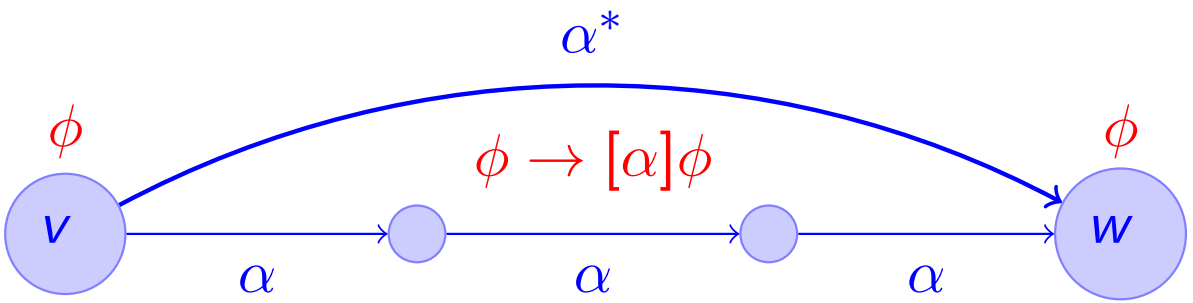
$$\frac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha \cup \beta]\phi}$$



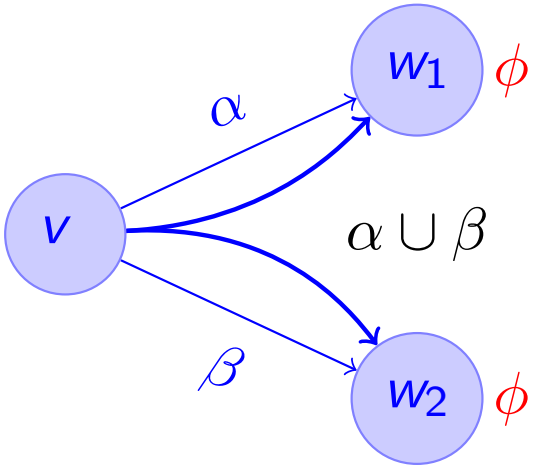
$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$



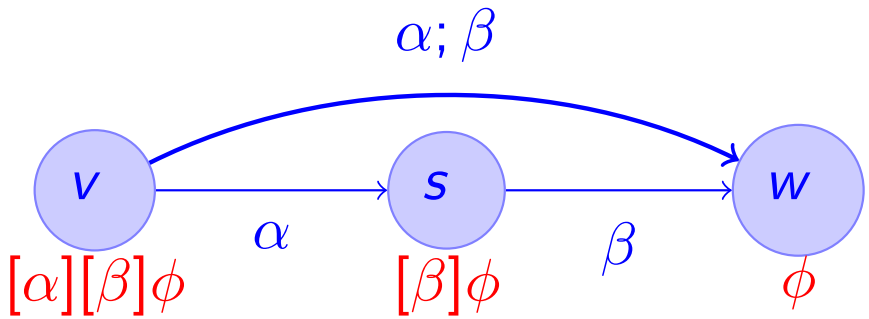
$$\frac{\vdash \phi}{\vdash [\alpha^*]\phi}$$



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



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



$$\frac{\vdash \phi \quad \vdash \forall^{\alpha}(\phi \to [\alpha]\phi)}{\vdash [\alpha^*]\phi}$$