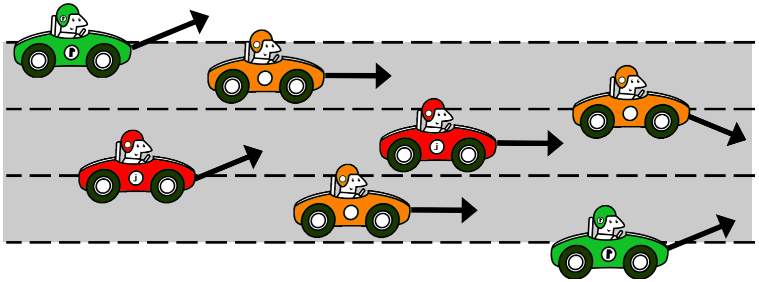
# Differential Refinement Logic

Sarah M. Loos and André Platzer
Computer Science Department
Carnegie Mellon University

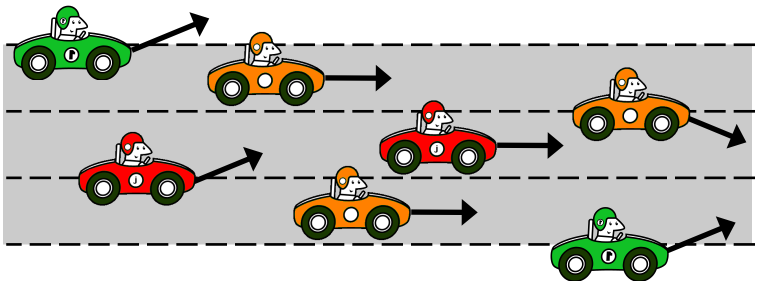
# Verified Cyber-Physical Systems

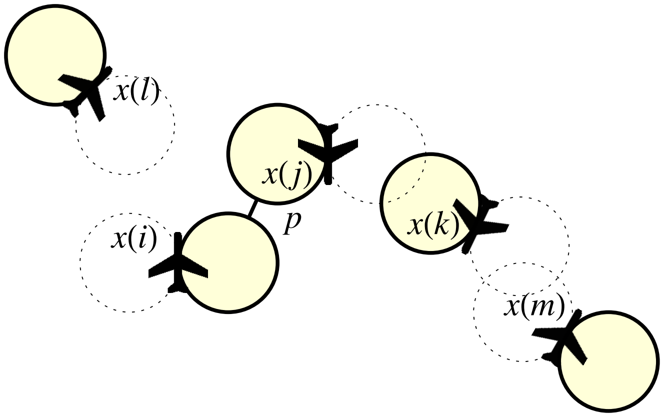




[FM11]

# Verified Cyber-Physical Systems

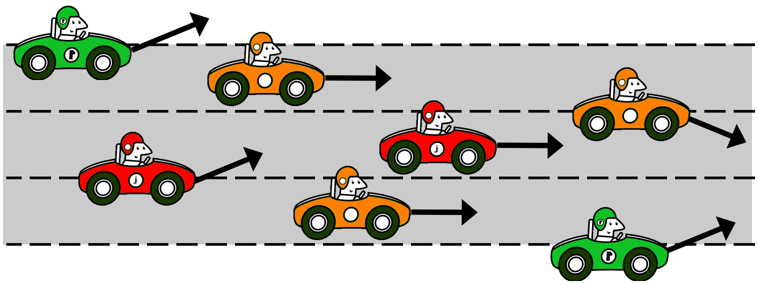
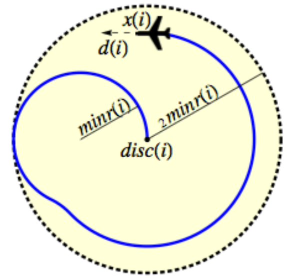


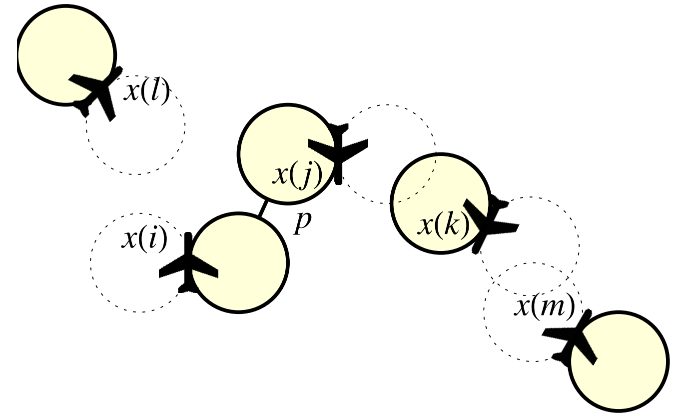


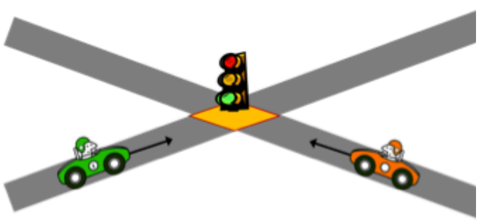
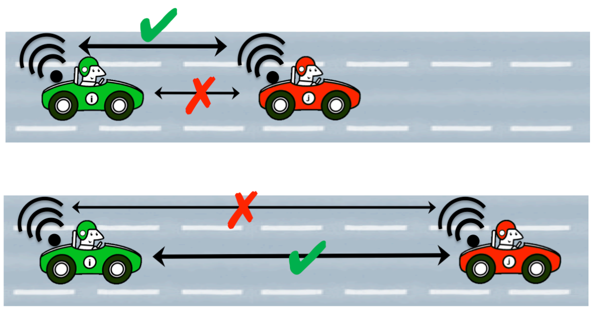
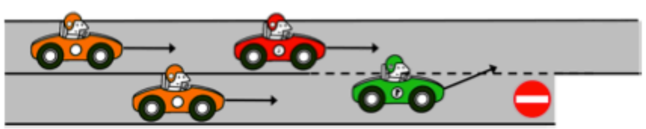
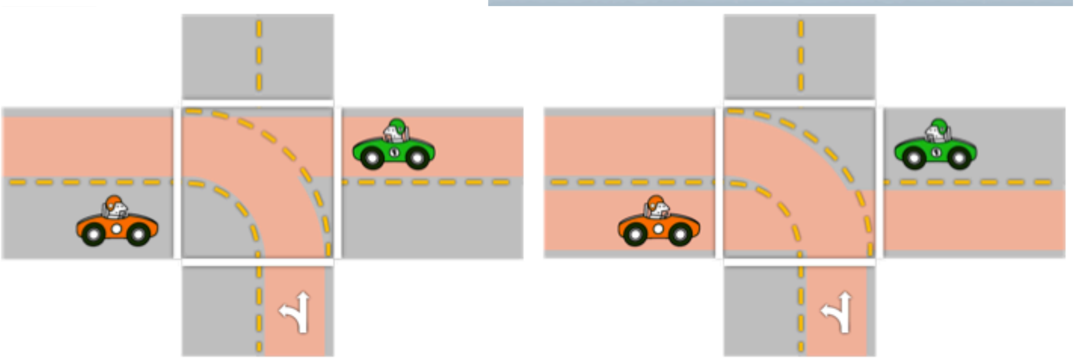
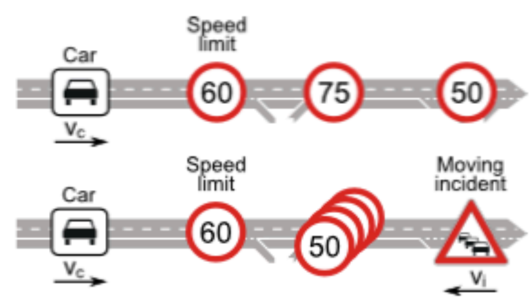



[FM11, HSCC13]

# Verified Cyber-Physical Systems






[FM11, ITSC11, ICCPS12, HSCC13, ITSC13]

# Roadmap

## Differential Refinement Logic (dRL)

$$\boldsymbol{\alpha} \leq \boldsymbol{\beta}$$

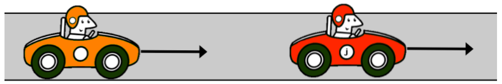
### Proof Calculus

$$\frac{\Gamma \vdash [\beta]\phi, \Delta \qquad \Gamma \vdash \alpha \leq \beta, \Delta}{\Gamma \vdash [\alpha]\phi, \Delta}([\leq])$$

### Time-triggered vs. Event-triggered

$$\mathtt{time}^* \leq \mathtt{event}^*$$

### Verified Car Control



# Roadmap

## Differential Refinement Logic (dRL)

$$\boldsymbol{\alpha \leq \beta}$$

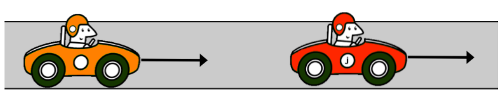
### Proof Calculus

$$\frac{\Gamma \vdash [\beta]\phi, \Delta \qquad \Gamma \vdash \alpha \leq \beta, \Delta}{\Gamma \vdash [\alpha]\phi, \Delta}([\leq])$$

### Time-triggered vs. Event-triggered

$$\texttt{time}^* \leq \texttt{event}^*$$

### Verified Car Control



# Refinement Relation

$$\boldsymbol{\alpha} \leq \boldsymbol{\beta}$$

# Refinement Relation

$$\boldsymbol{\alpha} \leq \boldsymbol{\beta}$$

$$\Big((?\phi; a := \theta \cup a := -B); x'' = a \,\&\, \psi\Big)^*$$

$$\Big((?\phi; a := * \cup a := -B); x'' = a\Big)^*$$

# Refinement Relation

$$\boldsymbol{\alpha \leq \beta}$$

$$\Big(\big(?\phi; \boldsymbol{a := \theta} \cup \boldsymbol{a} := -\boldsymbol{B}\big); \boldsymbol{x'' = a \,\&\, \psi}\Big)^{*}$$

$$\Big(\big(?\phi; \boldsymbol{a := *} \cup \boldsymbol{a} := -\boldsymbol{B}\big); \boldsymbol{x'' = a}\Big)^{*}$$

# Refinement Relation

$$\alpha \leq \beta$$

$$\left((?\phi; a := \theta \cup a := -B); x'' = a \ \& \ \psi\right)^*$$

$$\leq$$

$$\left((?\phi; a := * \cup a := -B); x'' = a\right)^*$$

# Refinement Relation

$$\alpha \leq \beta$$

$$\big((?\phi; a := \theta \cup a := -B); x'' = a \,\&\, \psi\big)^*$$

$$\leq \qquad\qquad\qquad\qquad \leq$$

$$\big((?\phi; a := * \cup a := -B); x'' = a\big)^*$$

# Refinement Relation

$$\boldsymbol{\alpha} \leq \boldsymbol{\beta}$$

$$\big((?\phi; \boldsymbol{a} := \boldsymbol{\theta} \cup \boldsymbol{a} := -\boldsymbol{B}); \boldsymbol{x}'' = \boldsymbol{a} \;\&\; \psi\big)^*$$

$$\leq$$

$$\big((?\phi; \boldsymbol{a} := * \cup \boldsymbol{a} := -\boldsymbol{B}); \boldsymbol{x}'' = \boldsymbol{a}\big)^*$$

# So, what does dRL look like exactly?

Syntax of a dRL formula:

$$\boldsymbol{\phi, \psi ::= \ \theta_1 \leq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x \phi}$$

$\boxed{\mathrm{FOL}_{\mathbb{R}}}$

# So, what does dRL look like exactly?

Syntax of a dRL formula:

$$\boldsymbol{\phi, \psi ::= \ \theta_1 \leq \theta_2 \mid \neg\phi \mid \phi \land \psi \mid \forall x \phi}$$
$$\boldsymbol{\mid [\alpha]\phi \mid \langle\alpha\rangle\phi}$$

dL

# So, what does dRL look like exactly?

Syntax of a dRL formula:

$$\boldsymbol{\phi, \psi ::= \theta_1 \leq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x \phi}$$
$$\boldsymbol{\mid [\alpha]\phi \mid \langle\alpha\rangle\phi}$$
$$\boldsymbol{\mid \alpha \leq \beta}$$

$\boxed{\text{refinement}}$

# So, what does dRL look like exactly?

Syntax of a dRL formula:

$$\begin{aligned}\boldsymbol{\phi, \psi ::=}\ & \boldsymbol{\theta_1 \leq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x \phi} \\ & \boldsymbol{\mid [\alpha]\phi \mid \langle\alpha\rangle\phi} \\ & \boldsymbol{\mid \alpha \leq \beta}\end{aligned}$$

Syntax of a hybrid program:

# So, what does dRL look like exactly?

Syntax of a dRL formula:

$$\begin{aligned}\phi, \psi ::= \ & \theta_1 \leq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x \phi \\ & \mid [\alpha]\phi \mid \langle\alpha\rangle\phi \\ & \mid \alpha \leq \beta\end{aligned}$$

Syntax of a hybrid program:

$$\begin{aligned}\alpha, \beta ::= \ & x := \theta \mid x' = \theta \ \& \ \psi \mid ?\psi \\ & \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^*\end{aligned}$$

d$\mathcal{L}$

# So, what does dRL look like exactly?

Syntax of a dRL formula:

$$\phi, \psi ::= \theta_1 \leq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x \phi$$
$$\mid [\alpha]\phi \mid \langle\alpha\rangle\phi$$
$$\mid \boxed{\alpha \leq \beta}$$

dRL extends d$\mathcal{L}$ by adding refinement directly into the grammar of formulas

Syntax of a hybrid program:

$$\alpha, \beta ::= x := \theta \mid x' = \theta \ \& \ \psi \mid ?\psi$$
$$\mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^*$$

# Semantics of hybrid programs

***Hybrid Programs*** model cyber-physical systems

$$v \xrightarrow{\alpha} w$$

$\rho(\alpha) = \{(v, w) :$ when starting in state $v$ and then following transitions of $\alpha$, state $w$ can be reached. $\}$



[Platzer08]

# Semantics of hybrid programs

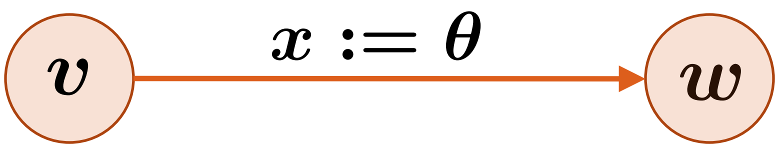
$$v \xrightarrow{x := \theta} w$$

iff $v = w$ except for the value of $x$

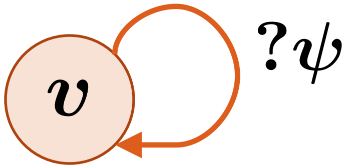


[Platzer08]

# Semantics of hybrid programs




iff $v = w$ except for the value of $x$

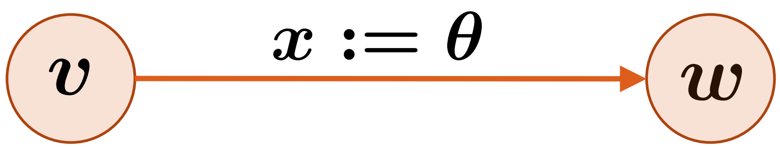



Iff $\psi$ holds in state $v$

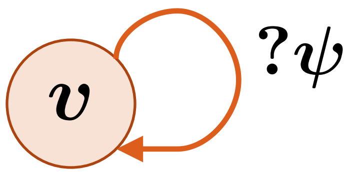


[Platzer08]

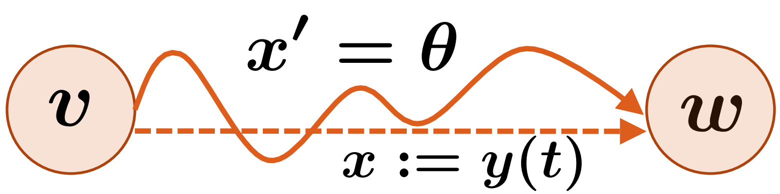
# Semantics of hybrid programs




iff $v = w$ except for the value of $x$




Iff $\psi$ holds in state $v$

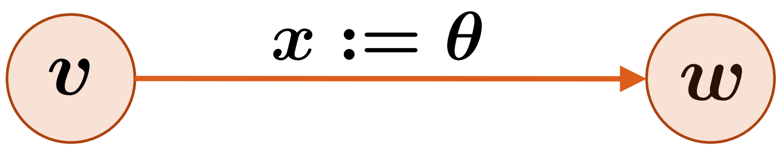



If $y(t)$ solves $x' = \theta$

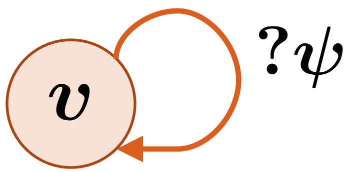


[Platzer08]

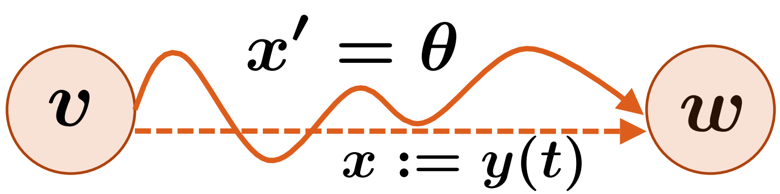
# Semantics of hybrid programs



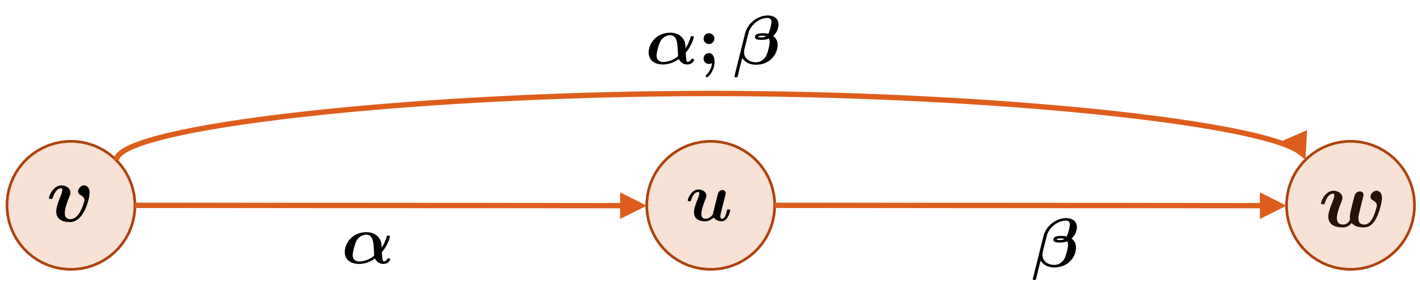

iff $v = w$ except for the value of $x$




Iff $\psi$ holds in state $v$



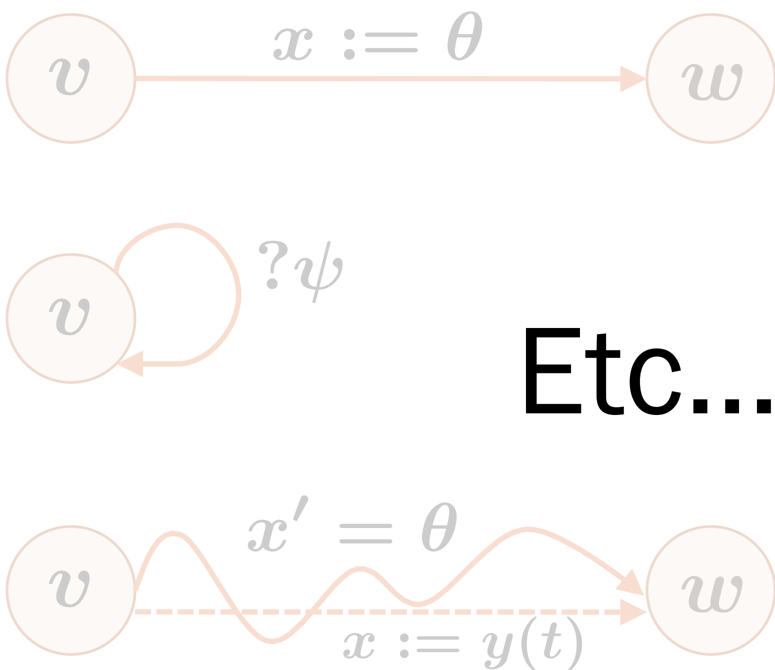

If $y(t)$ solves $x' = \theta$






[Platzer08]

# Semantics of hybrid programs




iff $v = w$ except for the value of $x$

Iff $\psi$ holds in state $v$

Etc...

If $y(t)$ solves $x' = \theta$






[Platzer08]

# Semantics of box modality

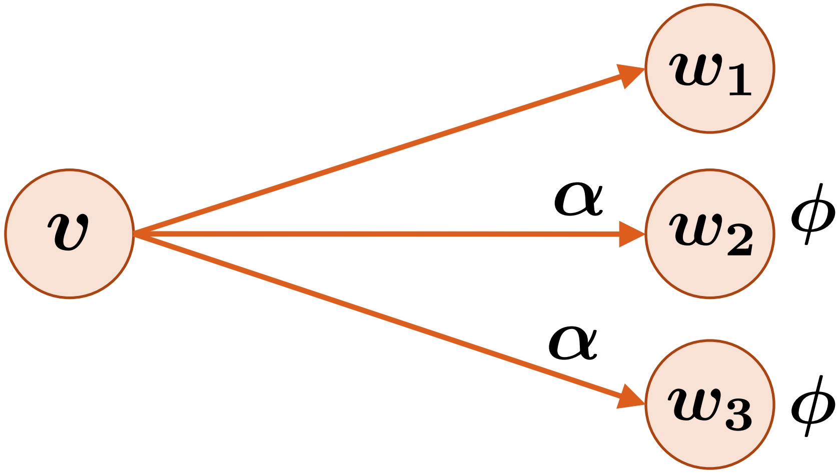
Box Modality:

$$\boldsymbol{v} \models [\boldsymbol{\alpha}]\phi$$

# Semantics of box modality

Box Modality:

$$v \models [\alpha]\phi$$



# Semantics of refinement

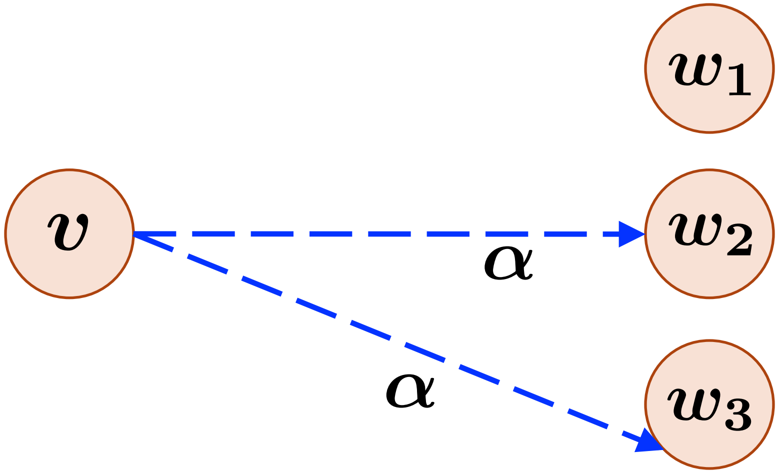
Refinement Relation:

$$\boldsymbol{v} \models \boldsymbol{\alpha} \leq \boldsymbol{\beta}$$

# Semantics of refinement

Refinement Relation:

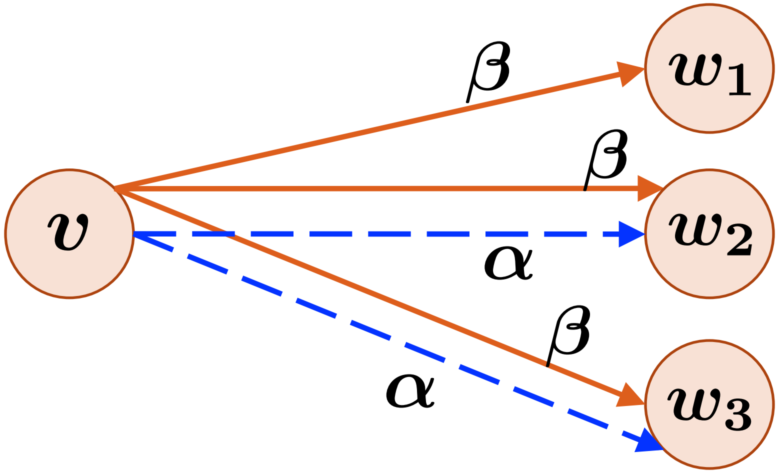
$$v \models \alpha \leq \beta$$



# Semantics of refinement

Refinement Relation:

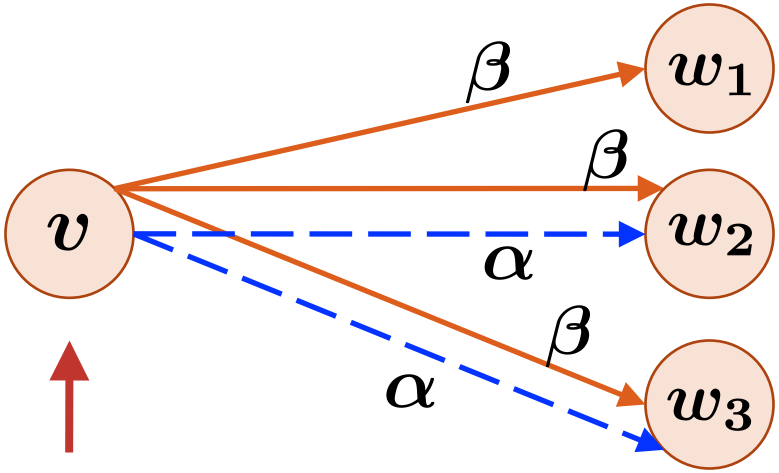
$$v \models \alpha \leq \beta$$



# Semantics of refinement

Refinement Relation:

$$v \models \alpha \leq \beta$$



# Roadmap

## Differential Refinement Logic (dRL)

$$\alpha \leq \beta$$

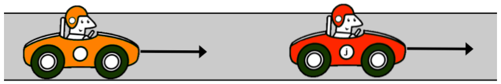
### Proof Calculus

$$\frac{\Gamma \vdash [\beta]\phi, \Delta \qquad \Gamma \vdash \alpha \leq \beta, \Delta}{\Gamma \vdash [\alpha]\phi, \Delta}([\leq])$$

### Time-triggered vs. Event-triggered

$$\mathtt{time}^* \leq \mathtt{event}^*$$

### Verified Car Control



# Roadmap

## Differential Refinement Logic (dRL)

$$\boldsymbol{\alpha} \leq \boldsymbol{\beta}$$

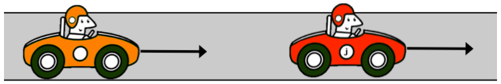
### Proof Calculus

$$\frac{\Gamma \vdash [\beta]\phi, \Delta \qquad \Gamma \vdash \alpha \leq \beta, \Delta}{\Gamma \vdash [\alpha]\phi, \Delta}([\leq])$$

### Time-triggered vs. Event-triggered

$$\mathtt{time}^* \leq \mathtt{event}^*$$

### Verified Car Control



# Combining refinement and box modality

$$\frac{\Gamma \vdash [\beta]\phi, \Delta \qquad \Gamma \vdash \alpha \leq \beta, \Delta}{\Gamma \vdash [\alpha]\phi, \Delta}([\leq])$$

# Combining refinement and box modality

$$\frac{\Gamma \vdash [\beta]\phi, \Delta \qquad \boxed{\Gamma \vdash \alpha \leq \beta, \Delta}}{\Gamma \vdash [\alpha]\phi, \Delta}([\leq])$$

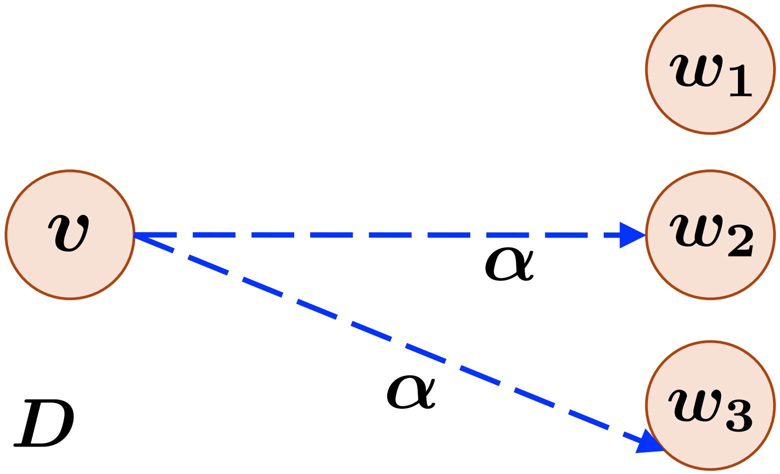
$\boldsymbol{v}$

$$\boldsymbol{v \models G, v \not\models D}$$

for all $\boldsymbol{G \in \Gamma, D \in \Delta}$

# Combining refinement and box modality

$$\frac{\Gamma \vdash [\beta]\phi, \Delta \qquad \boxed{\Gamma \vdash \alpha \leq \beta, \Delta}}{\Gamma \vdash [\alpha]\phi, \Delta}([\leq])$$

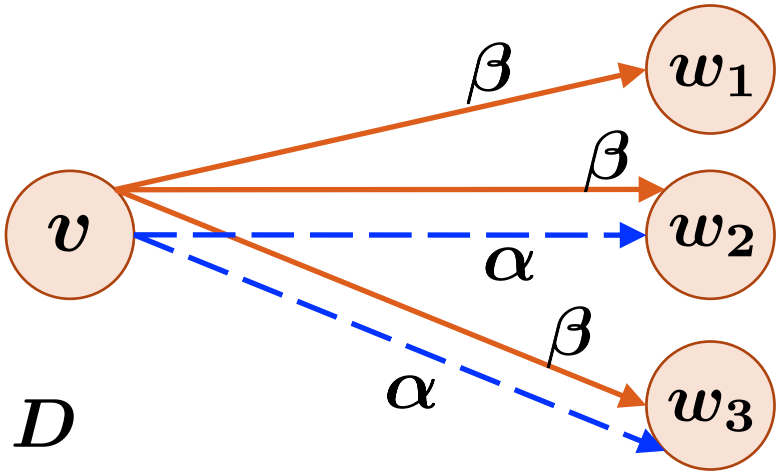



$$v \models G, v \not\models D$$

for all $G \in \Gamma, D \in \Delta$

# Combining refinement and box modality

$$\frac{\Gamma \vdash [\beta]\phi, \Delta \qquad \boxed{\Gamma \vdash \alpha \leq \beta, \Delta}}{\Gamma \vdash [\alpha]\phi, \Delta}([\leq])$$

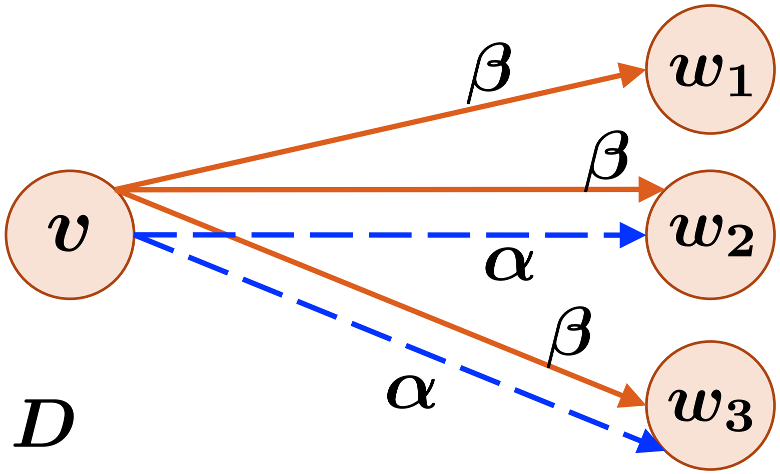



$$v \models G, v \not\models D$$

for all $G \in \Gamma, D \in \Delta$

# Combining refinement and box modality

$$\frac{\boxed{\Gamma \vdash [\beta]\phi, \Delta} \qquad \Gamma \vdash \alpha \leq \beta, \Delta}{\Gamma \vdash [\alpha]\phi, \Delta}\,([\leq])$$

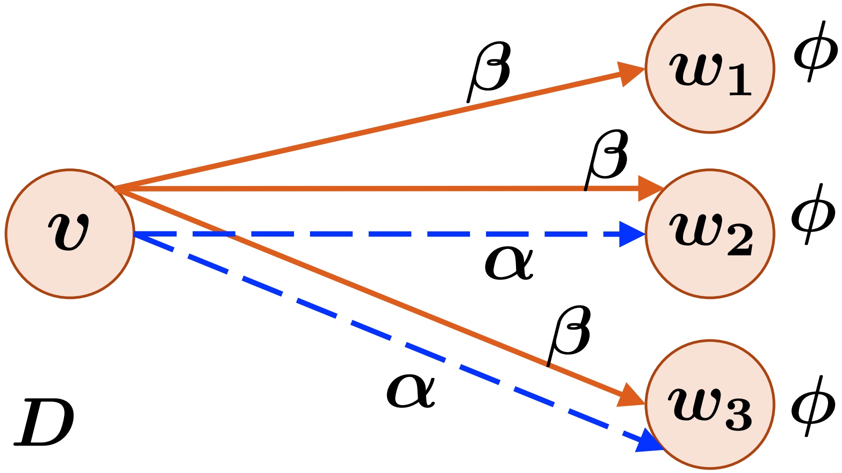



$$v \models G, v \not\models D$$

$$\text{for all } G \in \Gamma, D \in \Delta$$

# Combining refinement and box modality

$$\frac{\boxed{\Gamma \vdash [\beta]\phi, \Delta} \qquad \Gamma \vdash \alpha \leq \beta, \Delta}{\Gamma \vdash [\alpha]\phi, \Delta}([\leq])$$

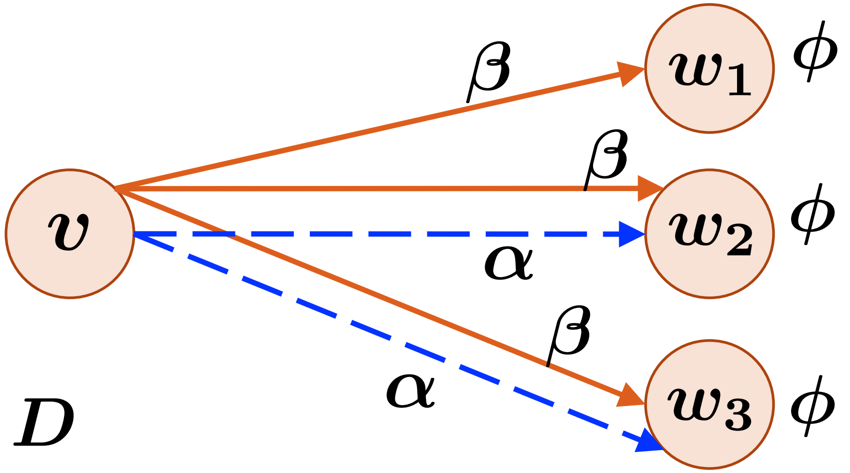



$$v \models G, v \not\models D$$

$$\text{for all } G \in \Gamma, D \in \Delta$$

# Combining refinement and box modality

$$\frac{\Gamma \vdash [\beta]\phi, \Delta \qquad \Gamma \vdash \alpha \leq \beta, \Delta}{\boxed{\Gamma \vdash [\alpha]\phi, \Delta}}([\leq])$$

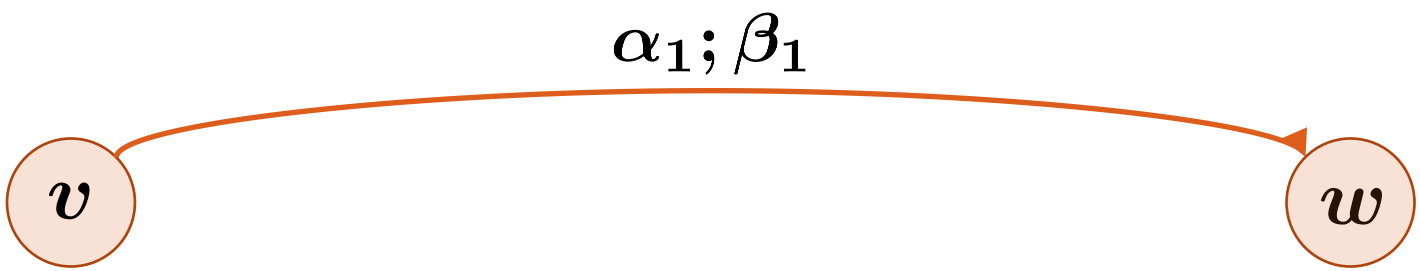



$$v \models G, v \not\models D$$

$$\text{for all } G \in \Gamma, D \in \Delta$$

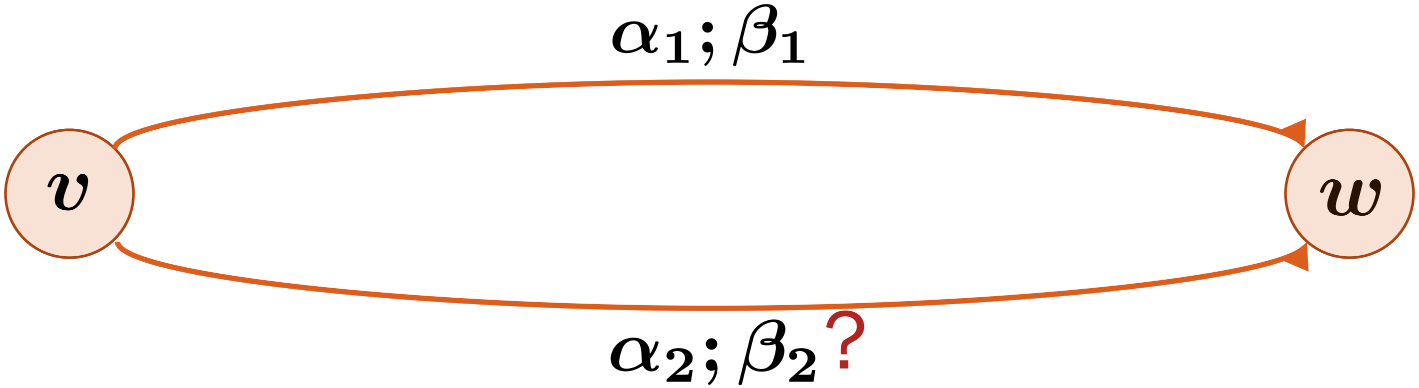
# Sequential Composition

$$\frac{\Gamma \vdash \alpha_1 \leq \alpha_2, \Delta \qquad\qquad \Gamma \vdash (\beta_1 \leq \beta_2), \Delta}{\Gamma \vdash (\alpha_1;\beta_1) \leq (\alpha_2;\beta_2), \Delta}(\,;\,)$$



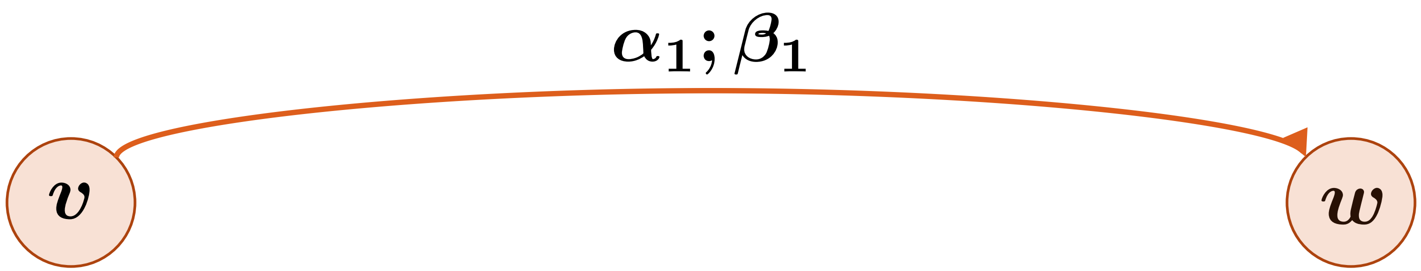
# Sequential Composition

$$\frac{\Gamma \vdash \alpha_1 \leq \alpha_2, \Delta \qquad\qquad \Gamma \vdash (\beta_1 \leq \beta_2), \Delta}{\Gamma \vdash (\alpha_1;\beta_1) \leq (\alpha_2;\beta_2), \Delta}(\,;)$$



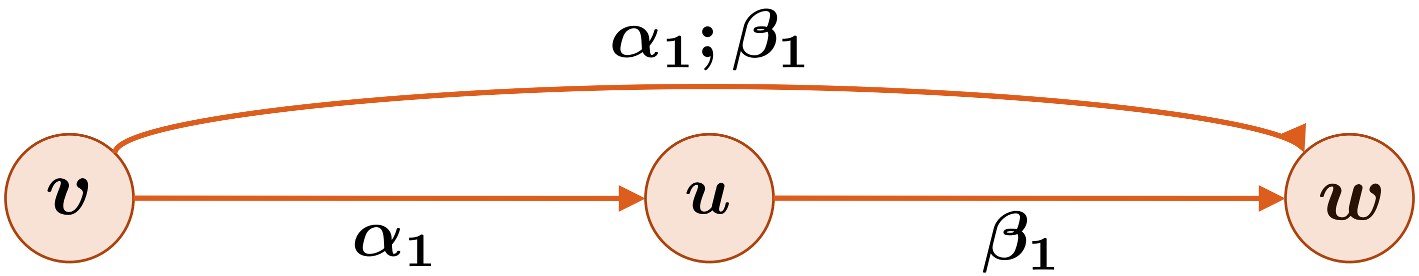
# Sequential Composition

$$\frac{\Gamma \vdash \alpha_1 \leq \alpha_2, \Delta \qquad \Gamma \vdash (\beta_1 \leq \beta_2), \Delta}{\Gamma \vdash (\alpha_1;\beta_1) \leq (\alpha_2;\beta_2), \Delta}(\,;\,)$$



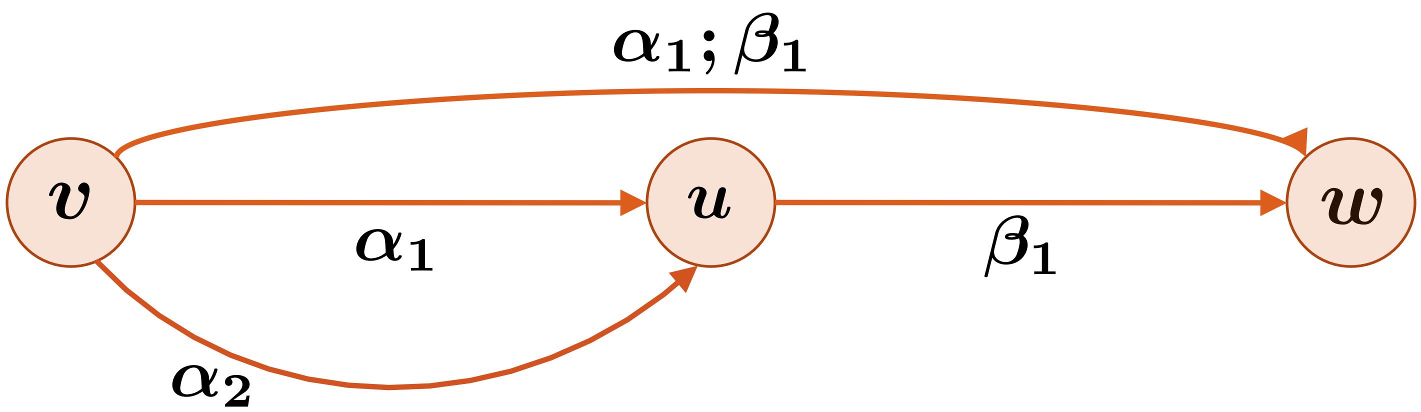
# Sequential Composition

$$\frac{\Gamma \vdash \alpha_1 \leq \alpha_2, \Delta \qquad \Gamma \vdash (\beta_1 \leq \beta_2), \Delta}{\Gamma \vdash (\alpha_1;\beta_1) \leq (\alpha_2;\beta_2), \Delta}(\,;\,)$$



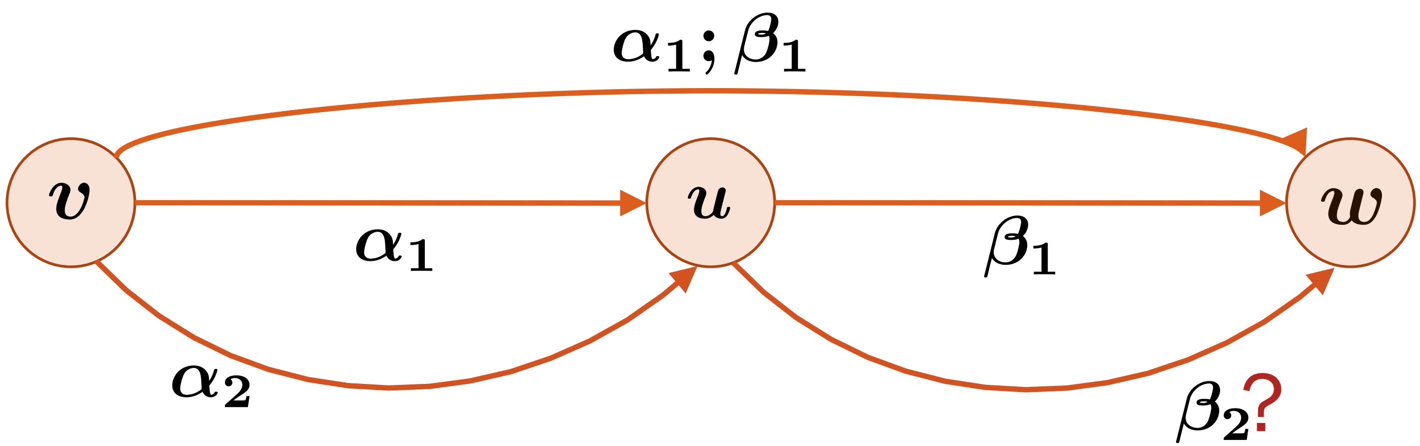
# Sequential Composition

$$\dfrac{\boxed{\Gamma \vdash \alpha_1 \leq \alpha_2, \Delta} \qquad\qquad \Gamma \vdash (\beta_1 \leq \beta_2), \Delta}{\Gamma \vdash (\alpha_1;\beta_1) \leq (\alpha_2;\beta_2), \Delta}\,(\,;\,)$$



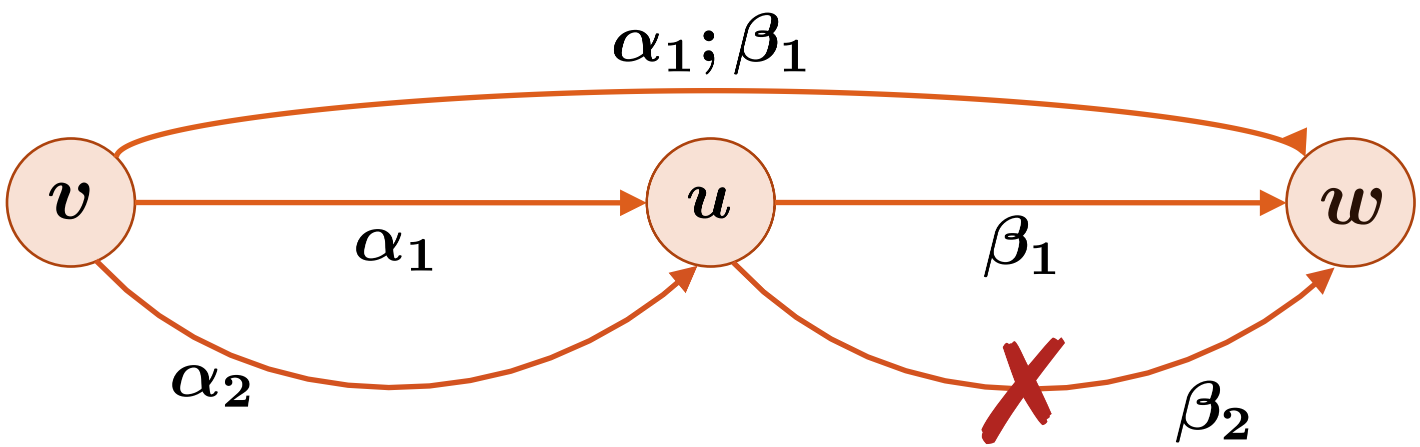
# Sequential Composition

$$\frac{\Gamma \vdash \alpha_1 \leq \alpha_2, \Delta \qquad \boxed{\Gamma \vdash (\beta_1 \leq \beta_2), \Delta}}{\Gamma \vdash (\alpha_1;\beta_1) \leq (\alpha_2;\beta_2), \Delta}(\,;)$$



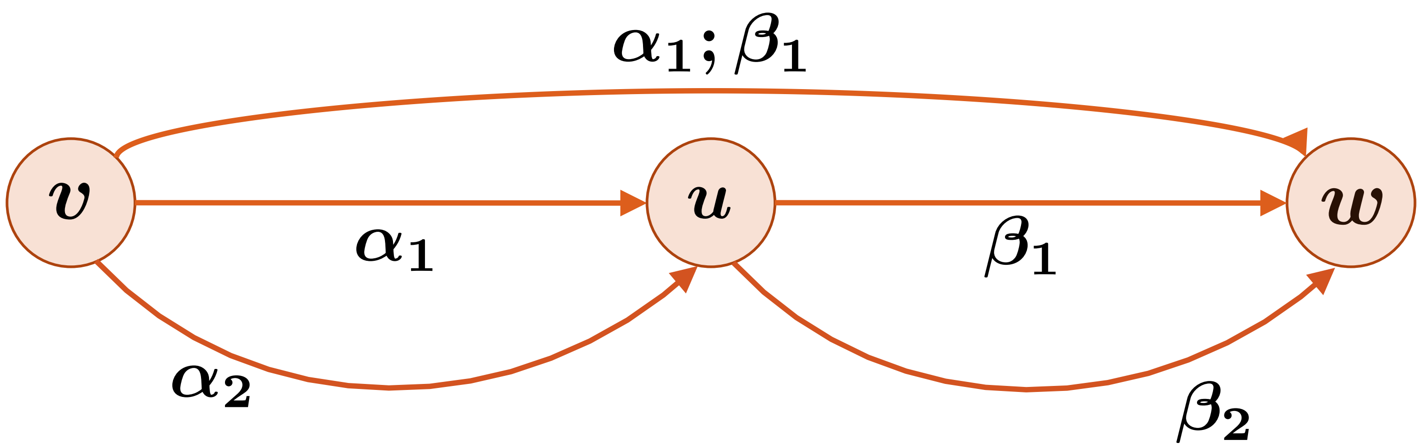
# Sequential Composition

$$\frac{\Gamma \vdash \alpha_1 \leq \alpha_2, \Delta \qquad \boxed{\Gamma \vdash (\beta_1 \leq \beta_2), \Delta}}{\Gamma \vdash (\alpha_1;\beta_1) \leq (\alpha_2;\beta_2), \Delta}(;)$$



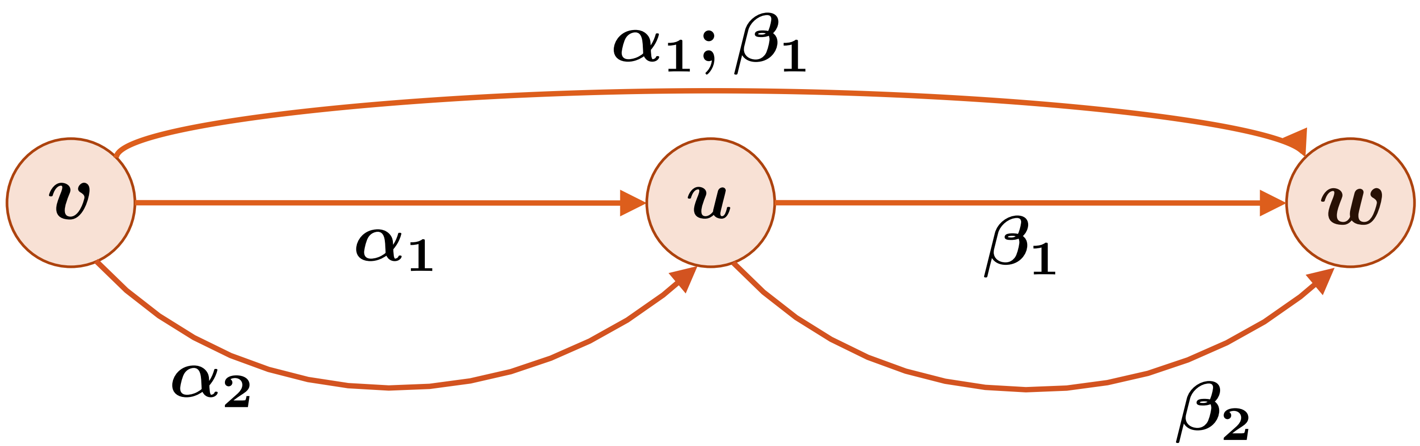
# Sequential Composition

$$\frac{\Gamma \vdash \alpha_1 \leq \alpha_2, \Delta \qquad \boxed{\Gamma \vdash [\alpha_1]\,(\beta_1 \leq \beta_2), \Delta}}{\Gamma \vdash (\alpha_1;\beta_1) \leq (\alpha_2;\beta_2), \Delta}\,(\,;\,)$$



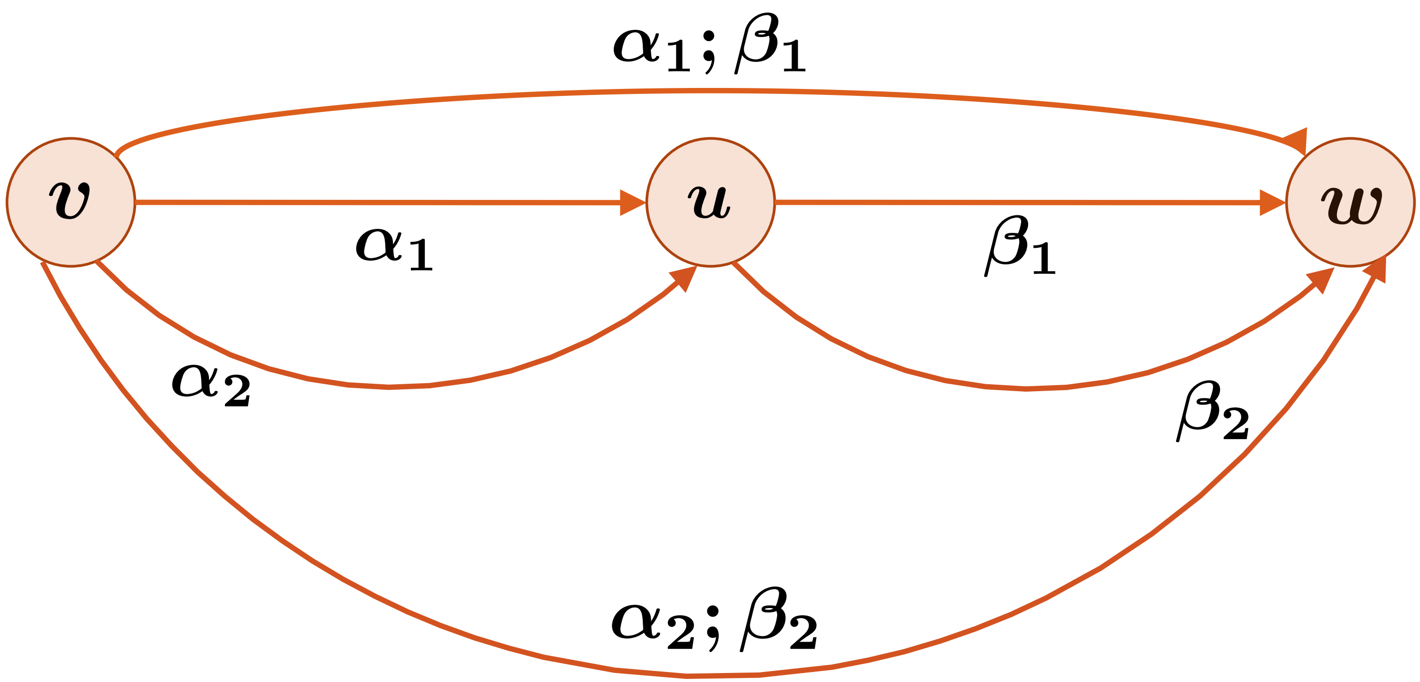
# Sequential Composition

$$\frac{\Gamma \vdash \alpha_1 \leq \alpha_2, \Delta \qquad \Gamma \vdash [\alpha_1]\,(\beta_1 \leq \beta_2), \Delta}{\Gamma \vdash (\alpha_1;\beta_1) \leq (\alpha_2;\beta_2), \Delta}(\,;)$$



# Sequential Composition

$$\frac{\Gamma \vdash \alpha_1 \le \alpha_2, \Delta \qquad \Gamma \vdash [\alpha_1]\,(\beta_1 \le \beta_2), \Delta}{\Gamma \vdash (\alpha_1;\beta_1) \le (\alpha_2;\beta_2), \Delta}(\,;\,)$$



# Differential Equations

$$(\boldsymbol{x'} = \mathbf{1}) \stackrel{?}{\leq} (\boldsymbol{x'} = \mathbf{9})$$

# Differential Equations

$$(\boldsymbol{x}' = \mathbf{1}) \overset{?}{\leq} (\boldsymbol{x}' = \mathbf{9})$$

$$\boldsymbol{x} \in [\boldsymbol{x}_{\mathbf{0}}, \boldsymbol{\infty})$$

# Differential Equations

$$(x' = 1) \overset{?}{\leq} (x' = 9)$$

$$x \in [x_0, \infty) \qquad\qquad x \in [x_0, \infty)$$

# Differential Equations

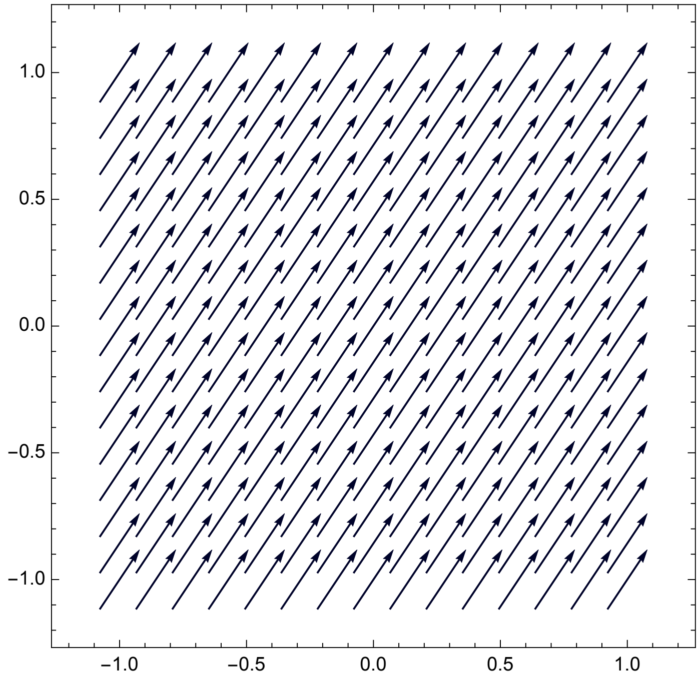
$$(\boldsymbol{x' = 1}) = (\boldsymbol{x' = 9})$$

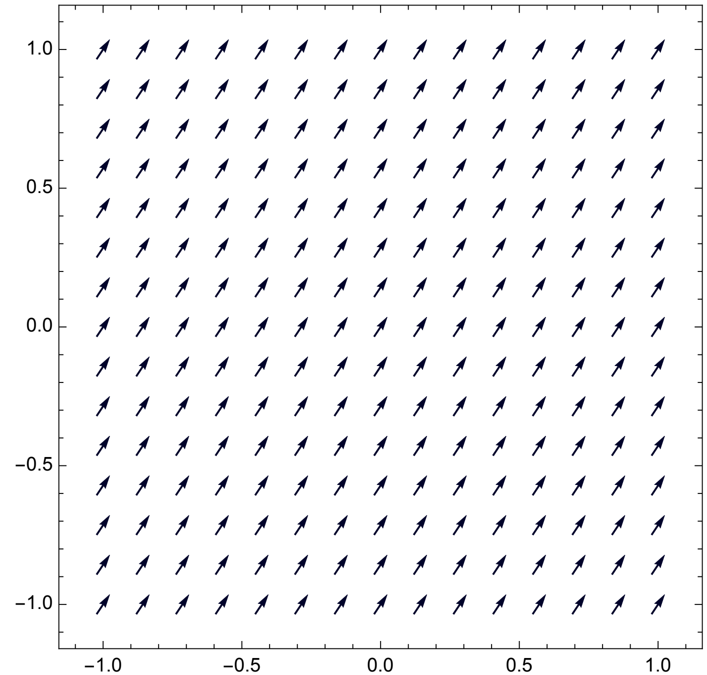
$$\boldsymbol{x \in [x_0, \infty)} \qquad\qquad \boldsymbol{x \in [x_0, \infty)}$$

# Differential Equations

$$\frac{\Gamma \vdash \forall x \left( \frac{\theta_1}{||\theta_1||} = \frac{\theta_2}{||\theta_2||} \wedge (||\theta_1|| = 0 \leftrightarrow ||\theta_2|| = 0) \right), \Delta}{\Gamma \vdash (x' = \theta_1) = (x' = \theta_2), \Delta} \; (mdf)$$

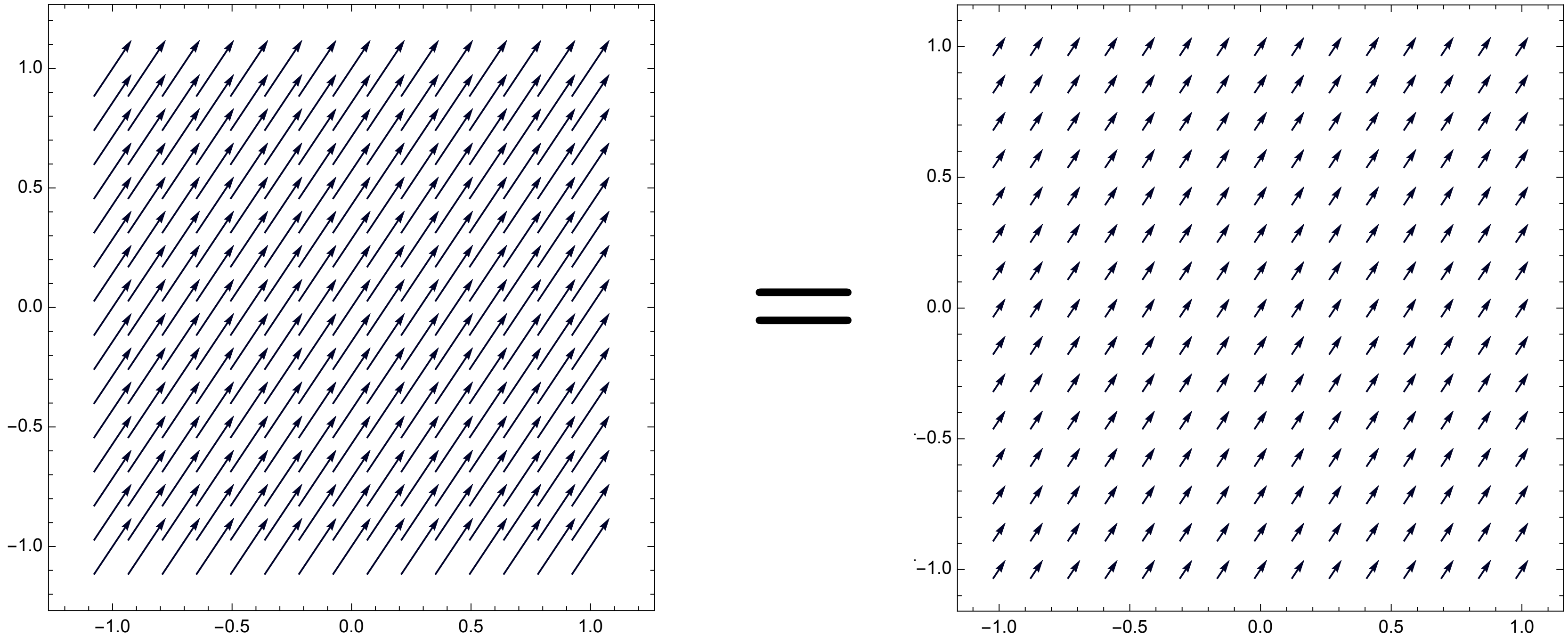
# Differential Equations



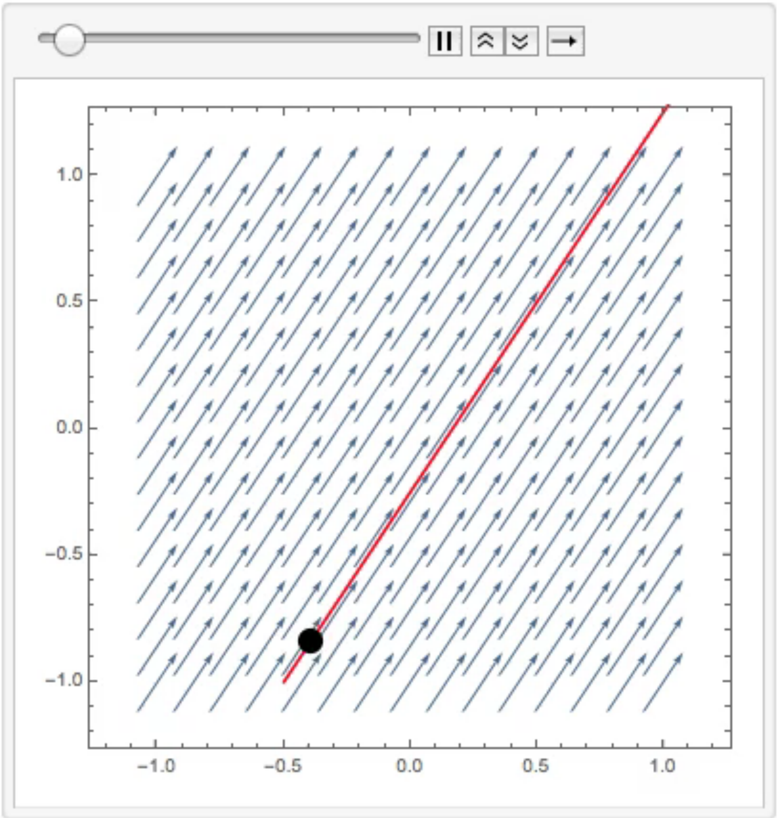

$$\frac{\Gamma \vdash \forall x \left( \dfrac{\theta_1}{\|\theta_1\|} = \dfrac{\theta_2}{\|\theta_2\|} \wedge (\|\theta_1\| = 0 \leftrightarrow \|\theta_2\| = 0) \right), \Delta}{\Gamma \vdash (x' = \theta_1) = (x' = \theta_2), \Delta} \ (mdf)$$

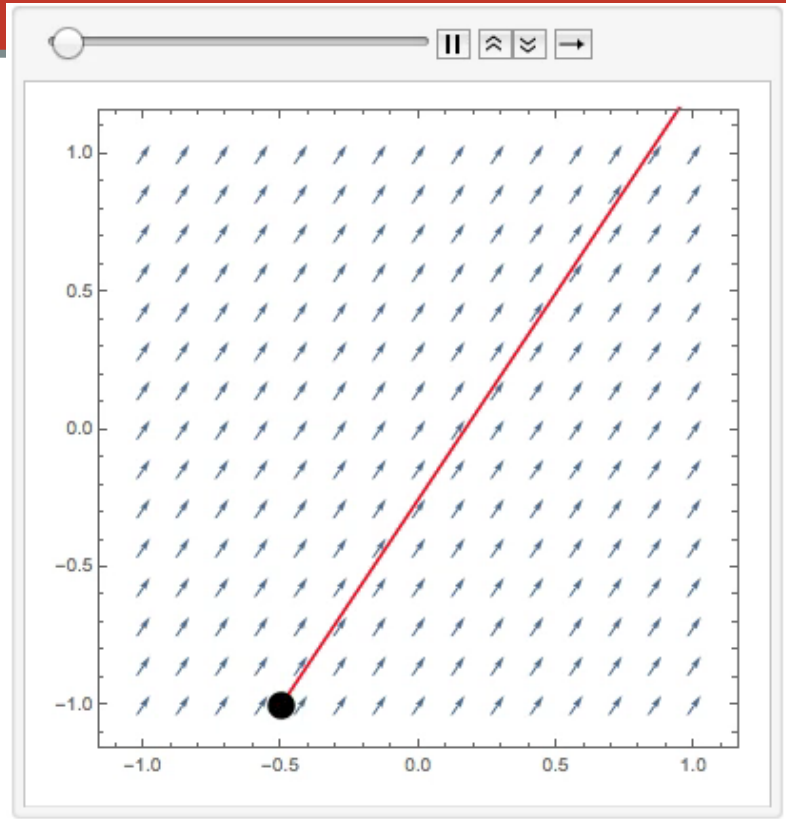
# Differential Equations




$$\frac{\Gamma \vdash \forall x \left( \frac{\theta_1}{\|\theta_1\|} = \frac{\theta_2}{\|\theta_2\|} \wedge (\|\theta_1\| = 0 \leftrightarrow \|\theta_2\| = 0) \right), \Delta}{\Gamma \vdash (x' = \theta_1) = (x' = \theta_2), \Delta} \; (mdf)$$

# Differential Equations




$$\frac{\Gamma \vdash \forall x \left( \frac{\theta_1}{\|\theta_1\|} = \frac{\theta_2}{\|\theta_2\|} \wedge (\|\theta_1\| = 0 \leftrightarrow \|\theta_2\| = 0) \right), \Delta}{\Gamma \vdash (x' = \theta_1) = (x' = \theta_2), \Delta} \ (mdf)$$

# Roadmap

## Differential Refinement Logic (dRL)

$$\alpha \leq \beta$$

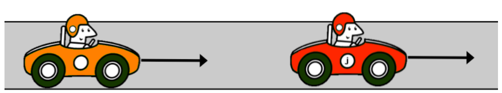
### Proof Calculus

$$\frac{\Gamma \vdash [\beta]\phi, \Delta \qquad \Gamma \vdash \alpha \leq \beta, \Delta}{\Gamma \vdash [\alpha]\phi, \Delta}([\leq])$$

### Time-triggered vs. Event-triggered

$$\mathtt{time}^* \leq \mathtt{event}^*$$

### Verified Car Control



# Roadmap

## Differential Refinement Logic (dRL)

$$\boldsymbol{\alpha} \leq \boldsymbol{\beta}$$

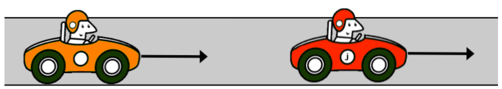
### Proof Calculus

$$\frac{\Gamma \vdash [\beta]\phi, \Delta \qquad \Gamma \vdash \alpha \leq \beta, \Delta}{\Gamma \vdash [\alpha]\phi, \Delta}([\leq])$$

### Time-triggered vs. Event-triggered

$$\texttt{time}^* \leq \texttt{event}^*$$

### Verified Car Control



# Two Modeling Paradigms

## Time-triggered

- Discrete sensing

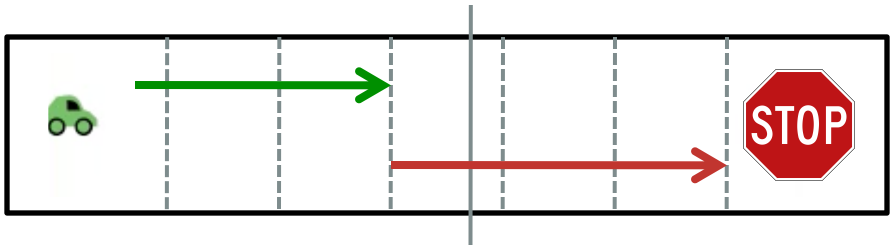
## Event-triggered

- Continuous sensing

# Two Modeling Paradigms

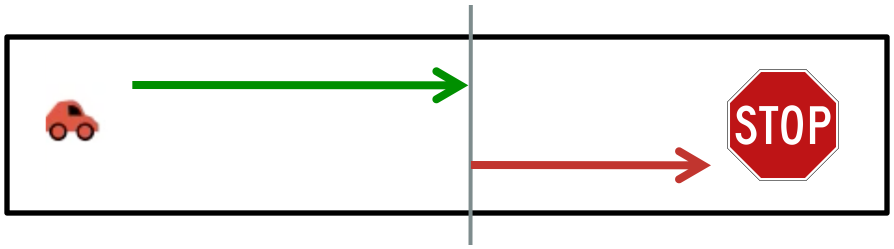
## Time-triggered

- Discrete sensing




## Event-triggered

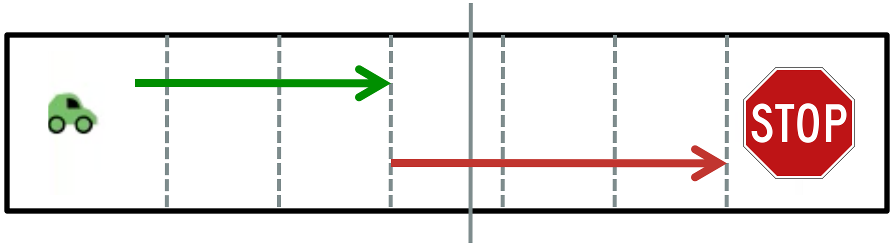
- Continuous sensing



# Two Modeling Paradigms

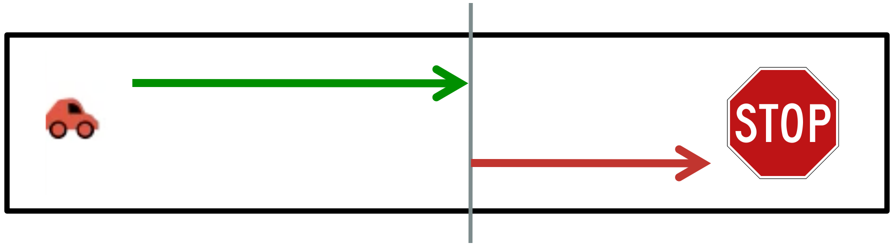
## Time-triggered

- Discrete sensing
- Realistic, easy to implement
- Difficult to design controllers
- Challenging to verify




## Event-triggered

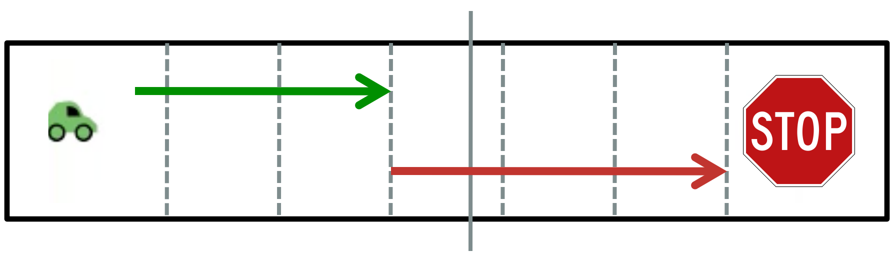
- Continuous sensing
- Unrealistic, hard to implement
- Easier to design controllers
- Easier to verify



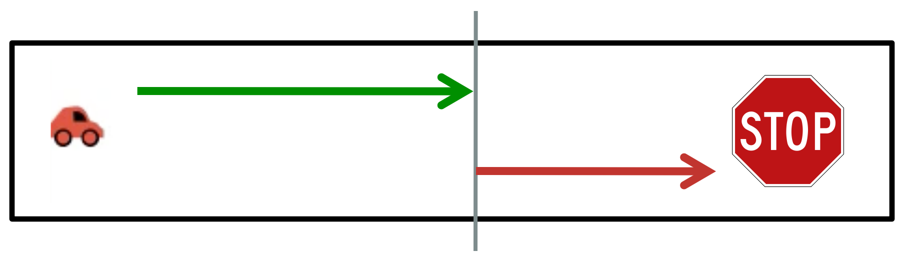
# Two Modeling Paradigms

Time-triggered $\leq$ Event-triggered

- Discrete sensing
- Realistic, easy to implement
- Difficult to design controllers
- Challenging to verify




- Continuous sensing
- Unrealistic, hard to implement
- Easier to design controllers
- Easier to verify



# Roadmap

## Differential Refinement Logic (dRL)

$$\alpha \leq \beta$$

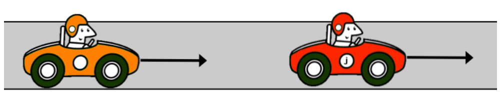
### Proof Calculus

$$\frac{\Gamma \vdash [\beta]\phi, \Delta \qquad \Gamma \vdash \alpha \leq \beta, \Delta}{\Gamma \vdash [\alpha]\phi, \Delta}([\leq])$$

### Time-triggered vs. Event-triggered

$$\texttt{time}^* \leq \texttt{event}^*$$

### Verified Car Control



# Roadmap

## Differential Refinement Logic (dRL)

$$\boldsymbol{\alpha \leq \beta}$$

### Proof Calculus

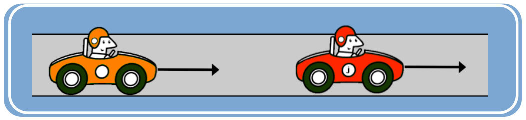
$$\frac{\Gamma \vdash [\beta]\phi, \Delta \qquad \Gamma \vdash \alpha \leq \beta, \Delta}{\Gamma \vdash [\alpha]\phi, \Delta}([\leq])$$

### Time-triggered vs. Event-triggered

$$\texttt{time}^* \leq \texttt{event}^*$$

### Verified Car Control

# Local Lane Control using Refinement

| Proof statistics for local lane controller, with and without refinement | | | |
|---|---|---|---|
|  | Interactive Steps | Computation Time (seconds) | Proof Nodes |
| Time-triggered [FM11] | **656** | **329.8** | **924** |
| Event-triggered | 4 | 73.3 | 140 |
| Controllers satisfy refinement | 0 | 0.6 | 16 |
| “Brake” for epsilon time | 0 | 2.7 | 30 |
| “Accelerate” for epsilon time | 79 | 8.4 | 126 |
| Time-triggered (dRL) | **83** | **85.0** | **312** |

# Contributions

## Differential Refinement Logic

- Maintains a modular and hierarchical proof structure
- Abstracts implementation-specific designs
- Leverages iterative system design
- Prove time-triggered model refines event-triggered
- Encouraging evidence of reduced user interaction and computation time

# Appendix

# Comparing dRL and dL

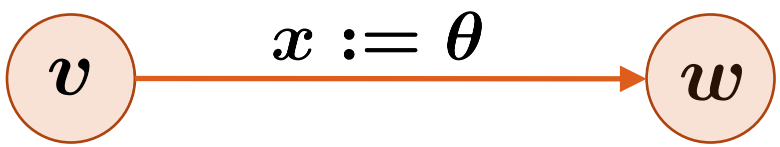
$$\vDash_{\mathsf{dR}\mathcal{L}} \alpha \leq \beta \iff \vDash_{\mathsf{d}\mathcal{L}} \forall \bar{x}\, (\langle \alpha \rangle (x = \bar{x}) \rightarrow \langle \beta \rangle (x = \bar{x}))$$

We have proved that the refinement relation can be embedded in dL. As a result, dL and dRL are equivalent in terms of *expressibility* and *provability*.

However, we can analyze dRL on familiar (challenging) case studies. We can consider:

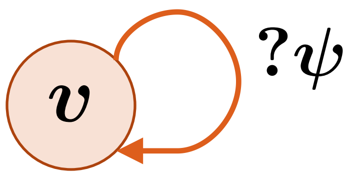
- Number of proof steps
- Computation time
- Qualitative difficulty to complete proof
- Proof structure

# Semantics of hybrid programs



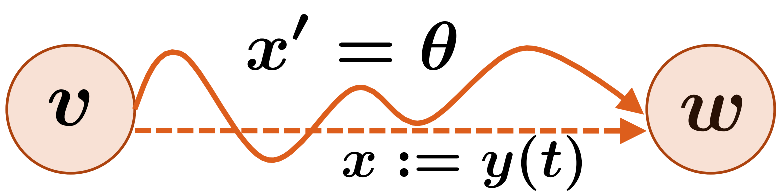

iff $v = w$ except for the value of $x$

$$\rho(x := \theta) = \{(v, w) : w = v \text{ except } [[x]]_w = [[\theta]]_v\}$$




Iff $\psi$ holds in state $v$

$$\rho(?\psi) = \{(v, v) : v \models \psi\}$$



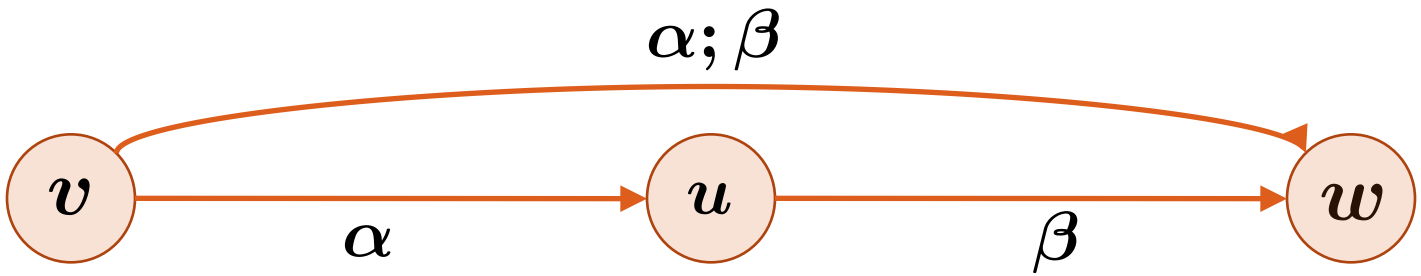

If $y(t)$ solves $x' = \theta$

$$\rho(x' = \theta) = \{(\varphi(0), \varphi(t)) : \varphi(s) \models x' = \theta \text{ for all } 0 \leq s \leq t\}$$



[Platzer08]

# Semantics of hybrid programs




$$\rho(\alpha;\beta) = \{(v,w) : (v,u) \in \rho(\alpha), (u,w) \in \rho(\beta)\}$$



[Platzer08]

# Combining refinement and diamond modality

$$\frac{\Gamma \vdash \boxed{[\beta]\phi}, \Delta \qquad \Gamma \vdash \alpha \leq \beta, \Delta}{\Gamma \vdash \boxed{[\alpha]\phi}, \Delta}([\leq])$$

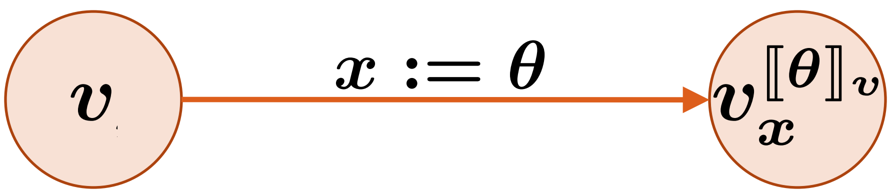
$$\frac{\Gamma \vdash \boxed{\langle\alpha\rangle\phi}, \Delta \qquad \Gamma \vdash \alpha \leq \beta, \Delta}{\Gamma \vdash \boxed{\langle\beta\rangle\phi}, \Delta}(\langle\leq\rangle)$$

# Nondeterministic Assignment

$$\frac{}{\Gamma \vdash (x := \theta) \leq (x := *), \Delta}(:= *)$$

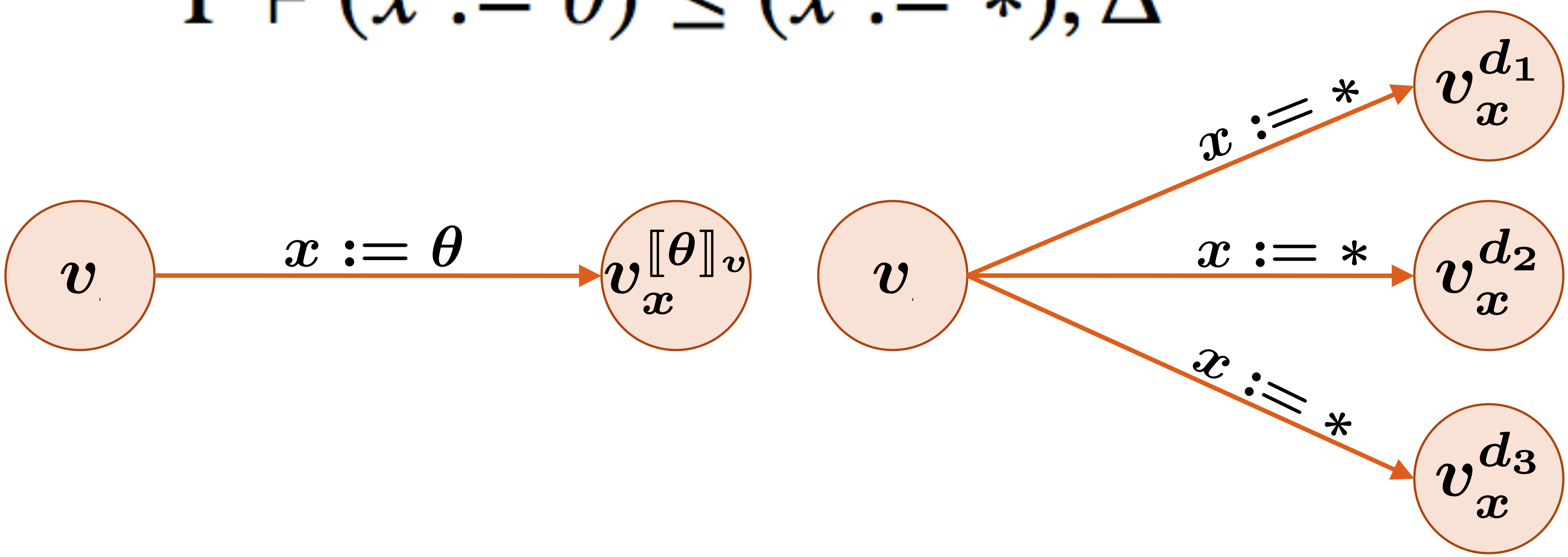
# Nondeterministic Assignment

$$\frac{}{\Gamma \vdash (x := \theta) \leq (x := *), \Delta}\,(:= *)$$



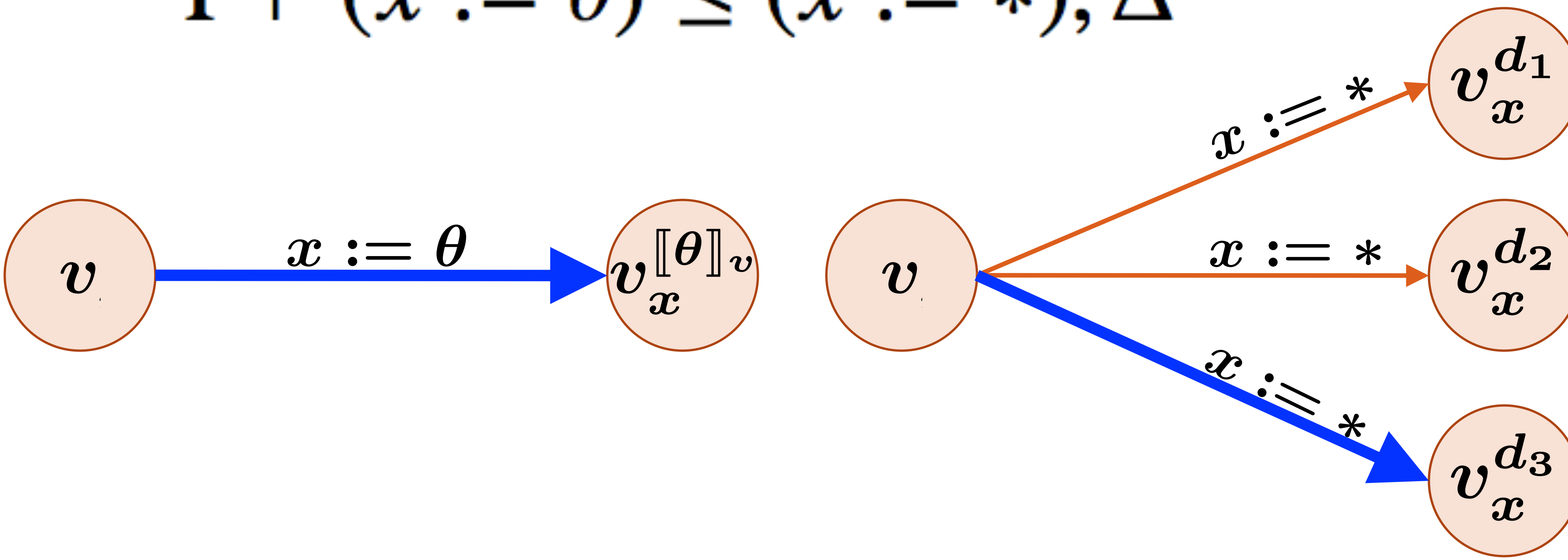
# Nondeterministic Assignment

$$\frac{}{\Gamma \vdash (x := \theta) \leq (x := *), \Delta}(:= *)$$



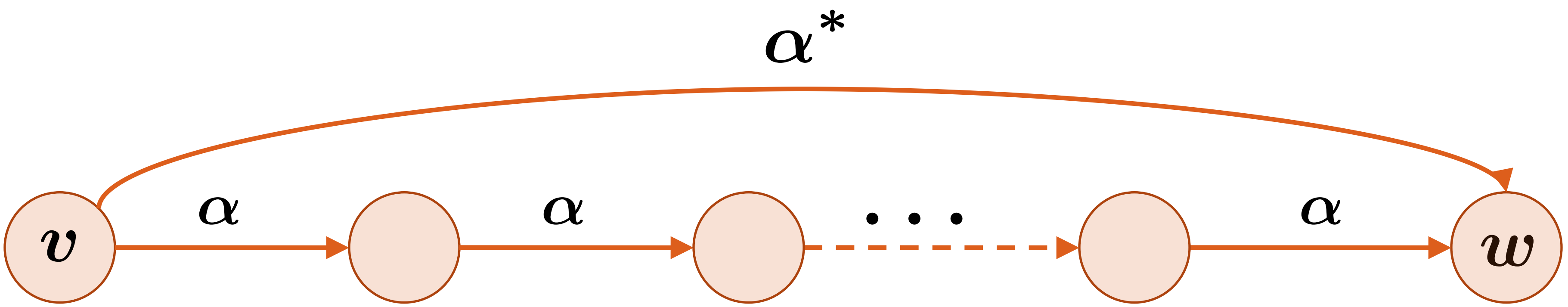
# Nondeterministic Assignment

$$\frac{}{\Gamma \vdash (x := \theta) \leq (x := *), \Delta}(:= *)$$



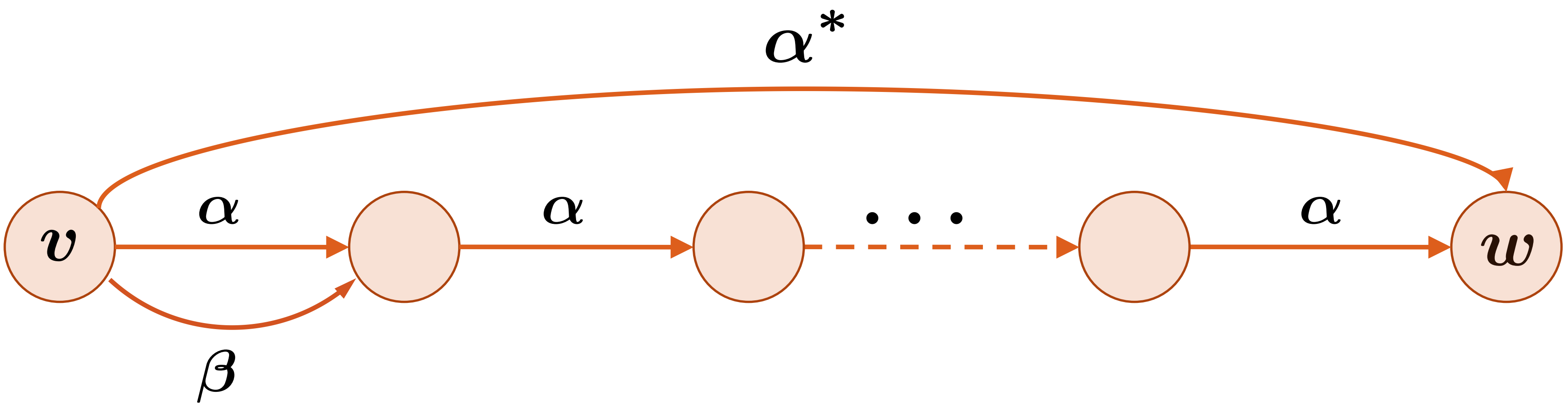
# Nondeterministic Repetition

$$\frac{\Gamma \vdash (\alpha \leq \beta), \Delta}{\Gamma \vdash \alpha^* \leq \beta^*, \Delta}(unloop)$$



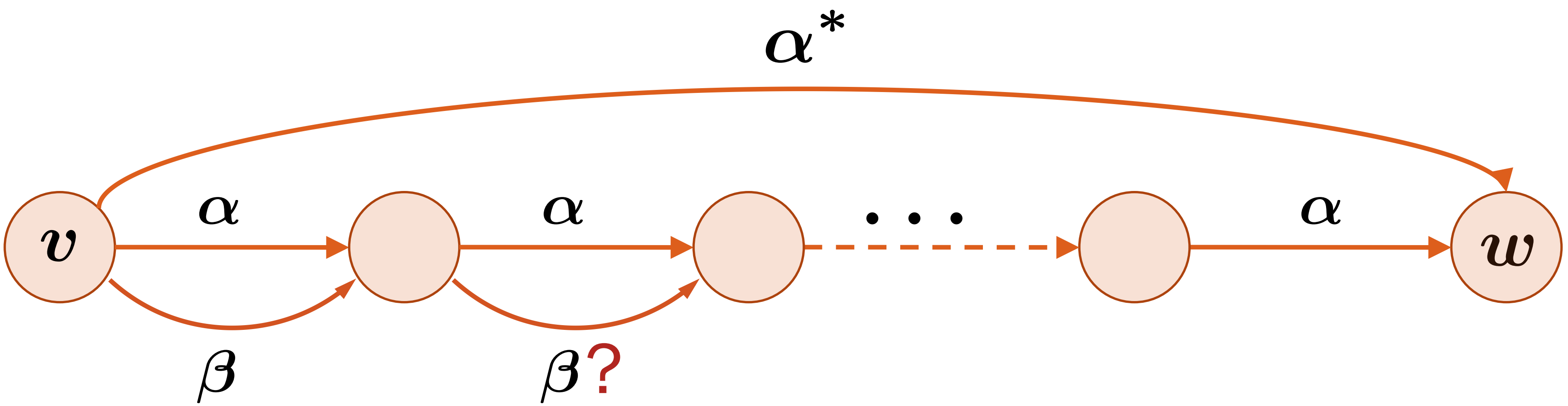
# Nondeterministic Repetition

$$\frac{\boxed{\Gamma \vdash (\alpha \leq \beta), \Delta}}{\Gamma \vdash \alpha^* \leq \beta^*, \Delta}(unloop)$$



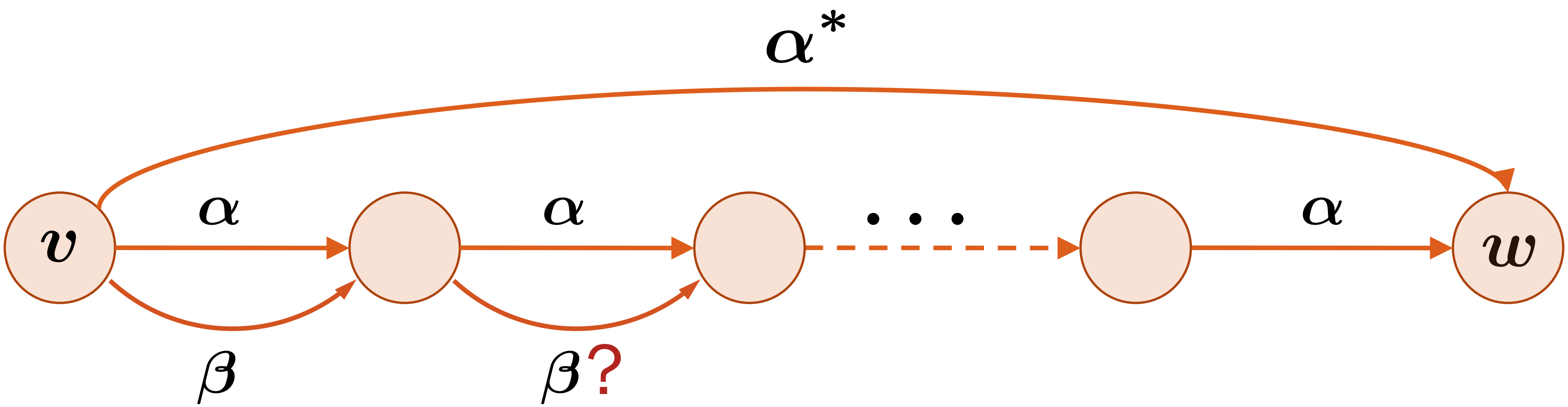
# Nondeterministic Repetition

$$\frac{\boxed{\Gamma \vdash (\alpha \leq \beta), \Delta}}{\Gamma \vdash \alpha^* \leq \beta^*, \Delta}\,(unloop)$$



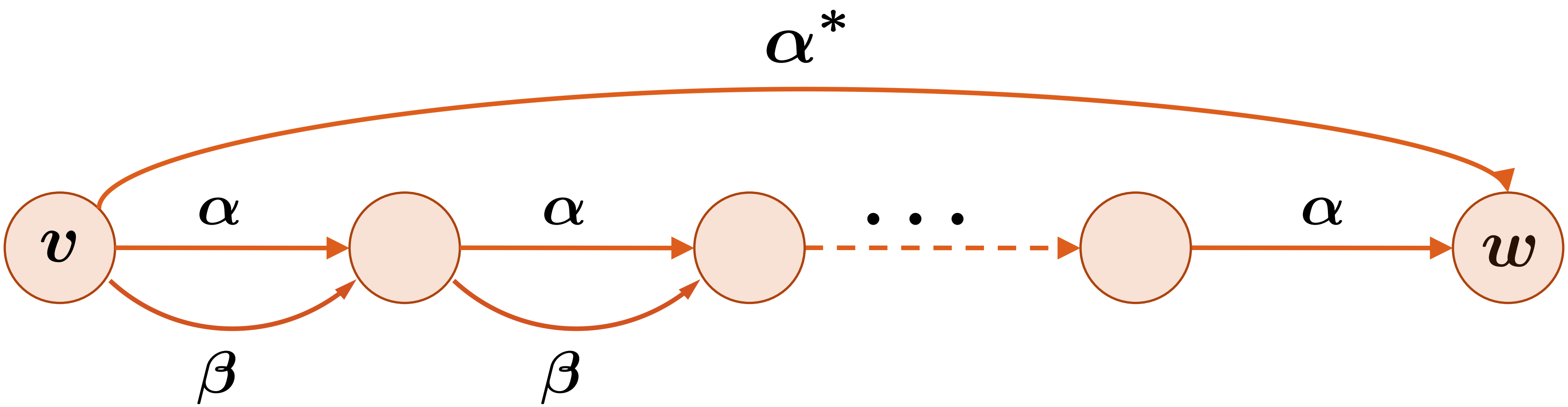
# Nondeterministic Repetition

$$\frac{\boxed{\Gamma \vdash [\alpha\ ](\alpha \leq \beta), \Delta}}{\Gamma \vdash \alpha^* \leq \beta^*, \Delta}(unloop)$$



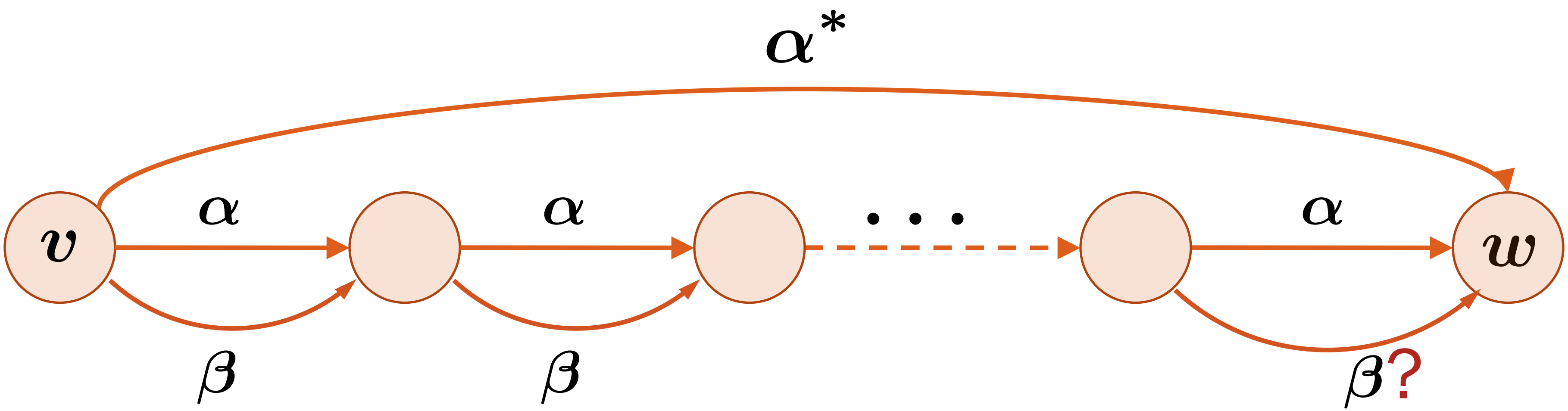
# Nondeterministic Repetition

$$\frac{\boxed{\Gamma \vdash [\alpha](\alpha \leq \beta), \Delta}}{\Gamma \vdash \alpha^{*} \leq \beta^{*}, \Delta}(unloop)$$



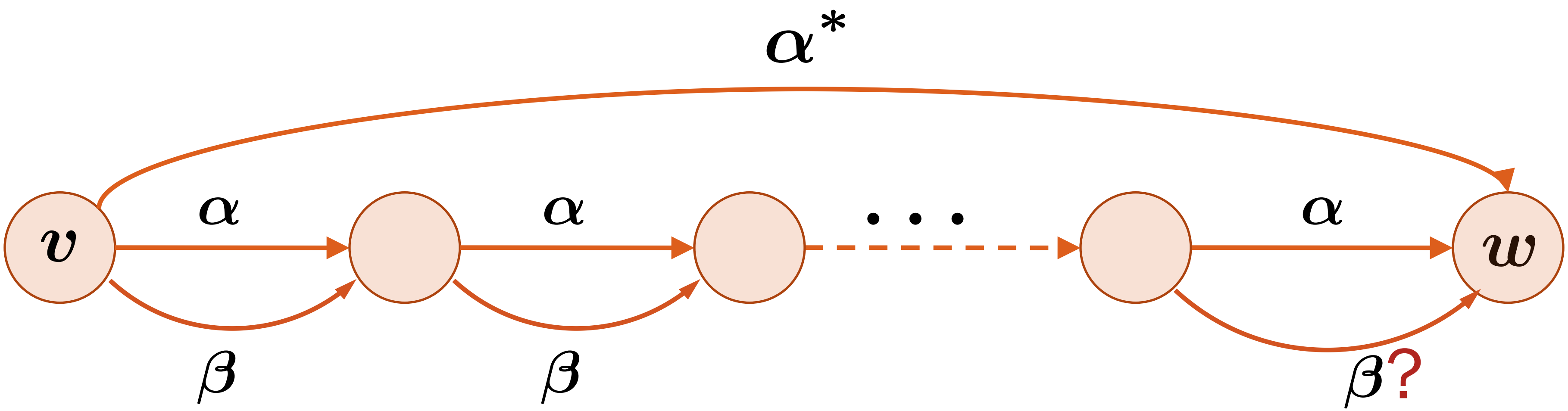
# Nondeterministic Repetition

$$\frac{\boxed{\Gamma \vdash [\alpha\ ](\alpha \leq \beta), \Delta}}{\Gamma \vdash \alpha^{*} \leq \beta^{*}, \Delta}\,(unloop)$$



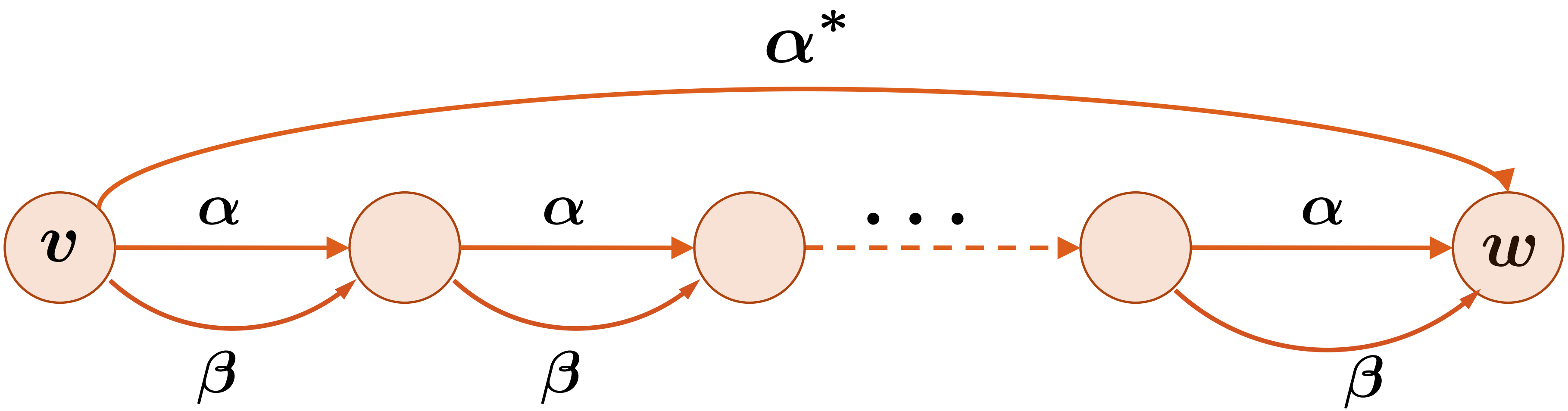
# Nondeterministic Repetition

$$\frac{\boxed{\Gamma \vdash [\alpha^*](\alpha \leq \beta), \Delta}}{\Gamma \vdash \alpha^* \leq \beta^*, \Delta}(unloop)$$



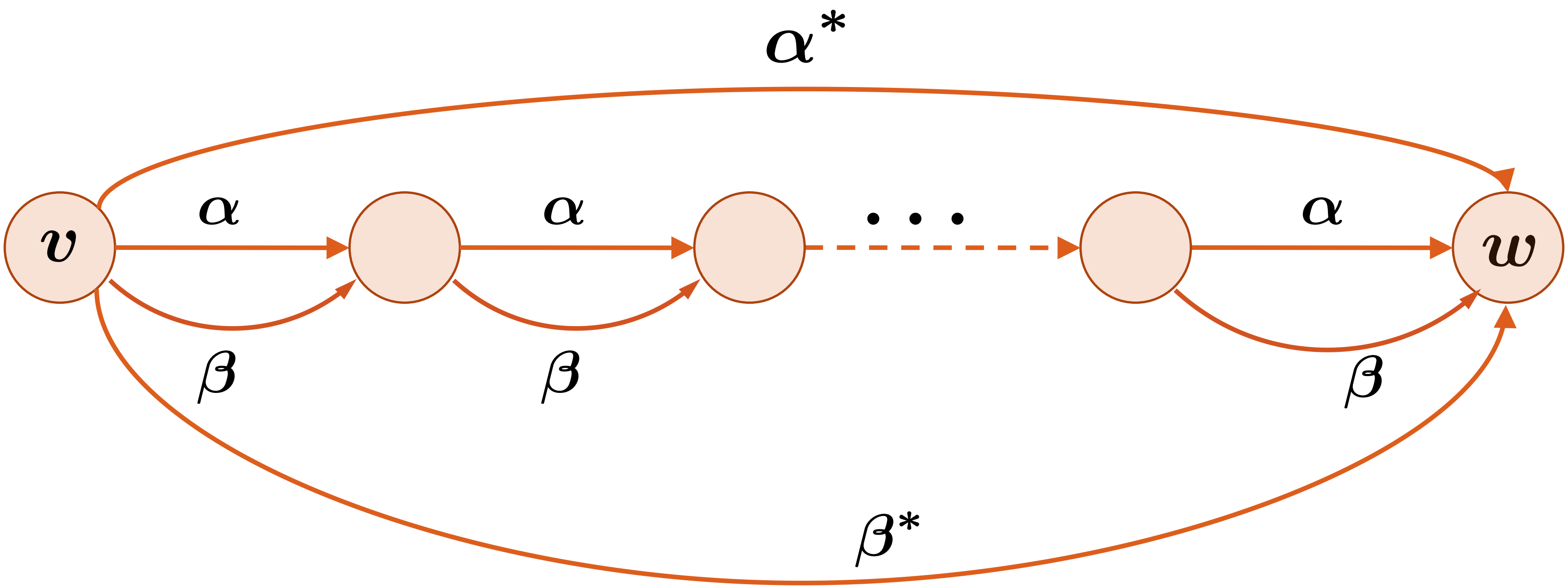
# Nondeterministic Repetition

$$\frac{\boxed{\Gamma \vdash [\alpha^*](\alpha \leq \beta), \Delta}}{\Gamma \vdash \alpha^* \leq \beta^*, \Delta}(unloop)$$



# Nondeterministic Repetition

$$\frac{\boxed{\Gamma \vdash [\alpha^*](\alpha \leq \beta), \Delta}}{\Gamma \vdash \alpha^* \leq \beta^*, \Delta}(unloop)$$



# Nondeterministic Repetition (KAT style)

$$\frac{\Gamma \vdash (\alpha;\gamma) \leq \gamma, \Delta \qquad \Gamma \vdash \beta \leq \gamma, \Delta}{\Gamma \vdash \alpha^*;\beta \leq \gamma, \Delta}(loop_l)$$

# Nondeterministic Repetition (KAT style)

$$\frac{\Gamma \vdash (\alpha;\gamma) \leq \gamma, \Delta \qquad \Gamma \vdash \beta \leq \gamma, \Delta}{\Gamma \vdash \alpha^*;\beta \leq \gamma, \Delta}(loop_l)$$

$$v \xrightarrow{\alpha} w_1 \xrightarrow{\cdots} w_2 \xrightarrow{\alpha} w_3 \xrightarrow{\beta} w_4$$

# Nondeterministic Repetition (KAT style)

$$\frac{\boxed{\Gamma \vdash (\alpha;\gamma) \leq \gamma, \Delta} \qquad \Gamma \vdash \beta \leq \gamma, \Delta}{\Gamma \vdash \alpha^*;\beta \leq \gamma, \Delta}\,(loop_l)$$

$$v \xrightarrow{\alpha} w_1 \xrightarrow{\cdots} w_2 \xrightarrow{\alpha} w_3 \xrightarrow{\beta} w_4$$

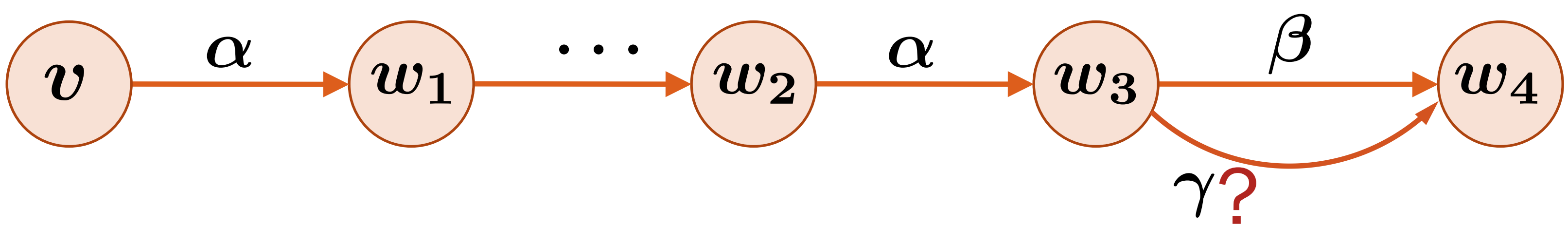
# Nondeterministic Repetition (KAT style)

$$\frac{\Gamma \vdash (\alpha;\gamma) \leq \gamma, \Delta \qquad \boxed{\Gamma \vdash \beta \leq \gamma, \Delta}}{\Gamma \vdash \alpha^*;\beta \leq \gamma, \Delta}\,(loop_l)$$

$$v \xrightarrow{\alpha} w_1 \xrightarrow{\cdots} w_2 \xrightarrow{\alpha} w_3 \xrightarrow{\beta} w_4$$

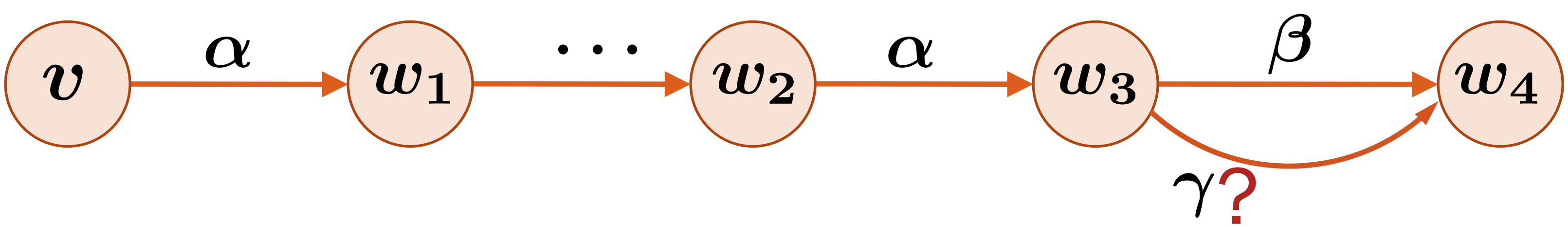
# Nondeterministic Repetition (KAT style)

$$\frac{\Gamma \vdash (\alpha;\gamma) \le \gamma, \Delta \qquad \boxed{\Gamma \vdash \beta \le \gamma, \Delta}}{\Gamma \vdash \alpha^*;\beta \le \gamma, \Delta}(loop_l)$$



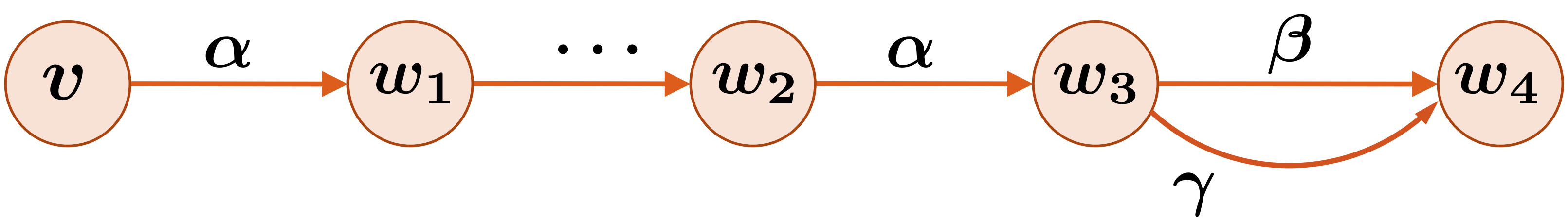
# Nondeterministic Repetition (KAT style)

$$\frac{\Gamma \vdash (\alpha;\gamma) \leq \gamma, \Delta \qquad \boxed{\Gamma \vdash [\alpha^*]\beta \leq \gamma, \Delta}}{\Gamma \vdash \alpha^*;\beta \leq \gamma, \Delta}(loop_l)$$



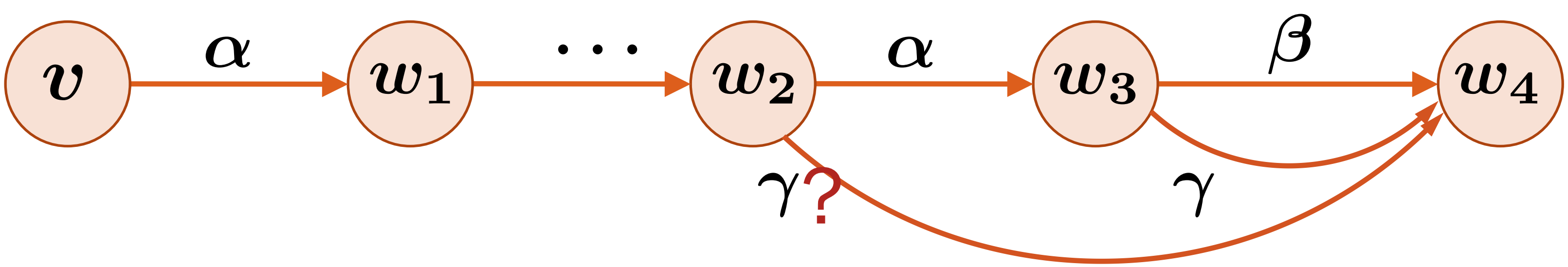
# Nondeterministic Repetition (KAT style)

$$\frac{\Gamma \vdash (\alpha;\gamma) \leq \gamma, \Delta \qquad \Gamma \vdash [\alpha^*]\beta \leq \gamma, \Delta}{\Gamma \vdash \alpha^*;\beta \leq \gamma, \Delta}(loop_l)$$



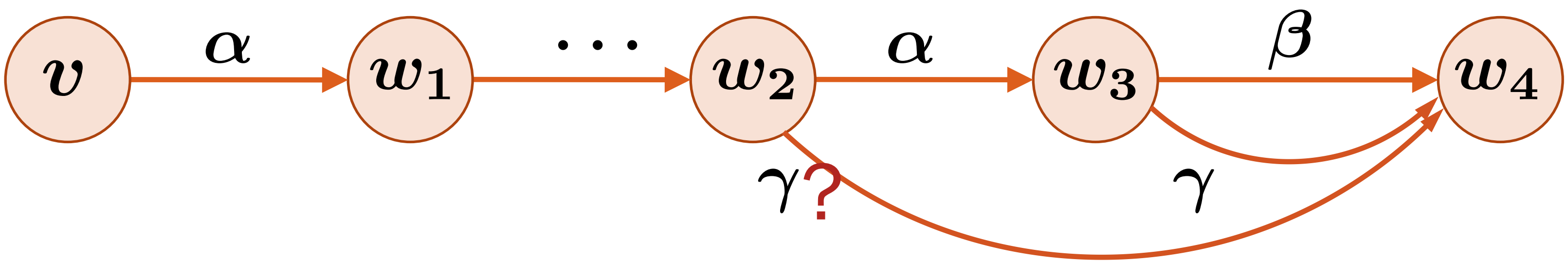
# Nondeterministic Repetition (KAT style)

$$\frac{\Gamma \vdash (\alpha;\gamma) \leq \gamma, \Delta \qquad \Gamma \vdash [\alpha^*]\beta \leq \gamma, \Delta}{\Gamma \vdash \alpha^*;\beta \leq \gamma, \Delta} (loop_l)$$



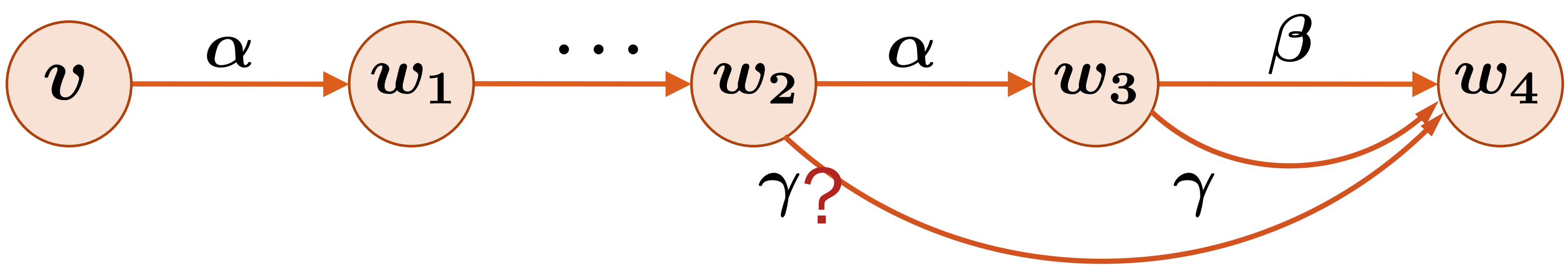
# Nondeterministic Repetition (KAT style)

$$\frac{\boxed{\Gamma \vdash (\alpha;\gamma) \leq \gamma, \Delta} \qquad \Gamma \vdash [\alpha^*]\beta \leq \gamma, \Delta}{\Gamma \vdash \alpha^*;\beta \leq \gamma, \Delta}(loop_l)$$



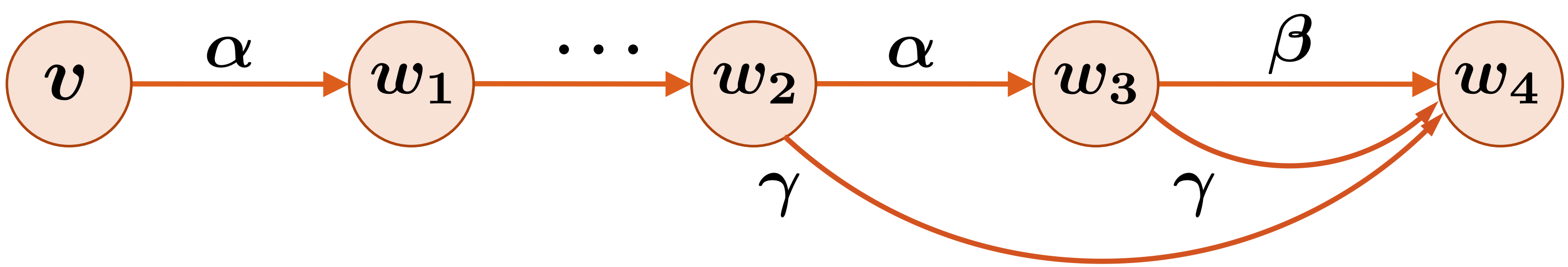
# Nondeterministic Repetition (KAT style)

$$\frac{\boxed{\Gamma \vdash [\alpha^*](\alpha;\gamma) \leq \gamma, \Delta} \qquad \Gamma \vdash [\alpha^*]\beta \leq \gamma, \Delta}{\Gamma \vdash \alpha^*;\beta \leq \gamma, \Delta}(loop_l)$$



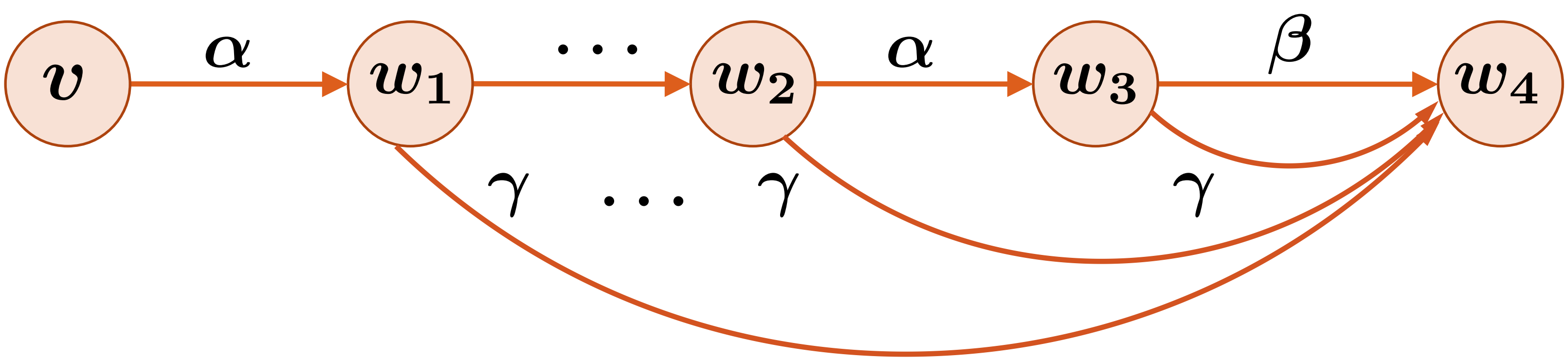
# Nondeterministic Repetition (KAT style)

$$\frac{\boxed{\Gamma \vdash [\alpha^*](\alpha;\gamma) \leq \gamma, \Delta} \qquad \Gamma \vdash [\alpha^*]\beta \leq \gamma, \Delta}{\Gamma \vdash \alpha^*;\beta \leq \gamma, \Delta}\,(loop_l)$$



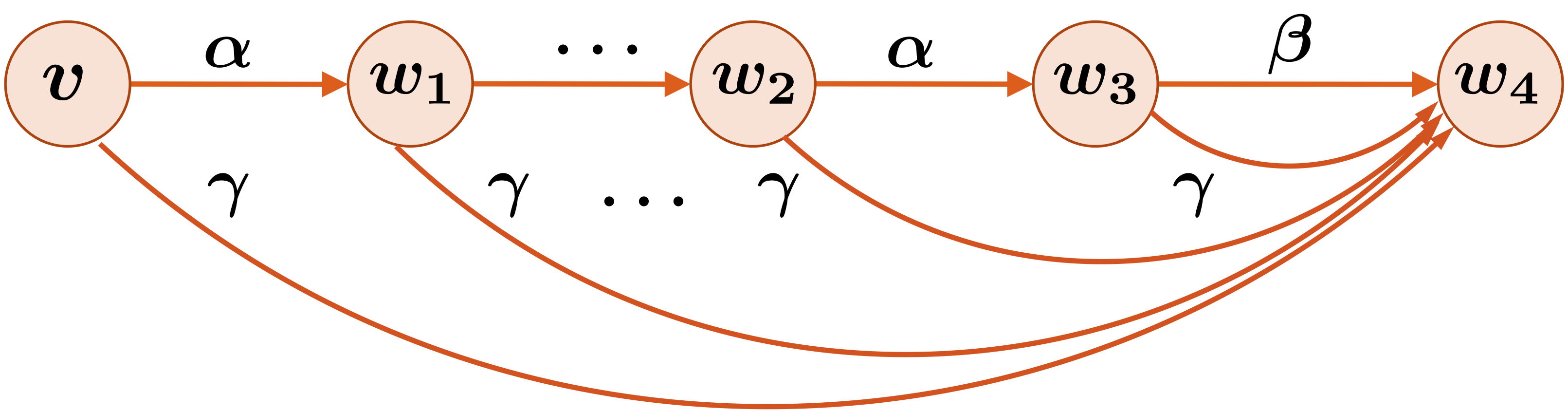
# Nondeterministic Repetition (KAT style)

$$\frac{\boxed{\Gamma \vdash [\alpha^*](\alpha;\gamma) \leq \gamma, \Delta} \qquad \Gamma \vdash [\alpha^*]\beta \leq \gamma, \Delta}{\Gamma \vdash \alpha^*;\beta \leq \gamma, \Delta} (loop_l)$$



# Nondeterministic Repetition (KAT style)

$$\frac{\boxed{\Gamma \vdash [\alpha^*](\alpha;\gamma) \leq \gamma, \Delta} \qquad \Gamma \vdash [\alpha^*]\beta \leq \gamma, \Delta}{\Gamma \vdash \alpha^*;\beta \leq \gamma, \Delta}(loop_l)$$



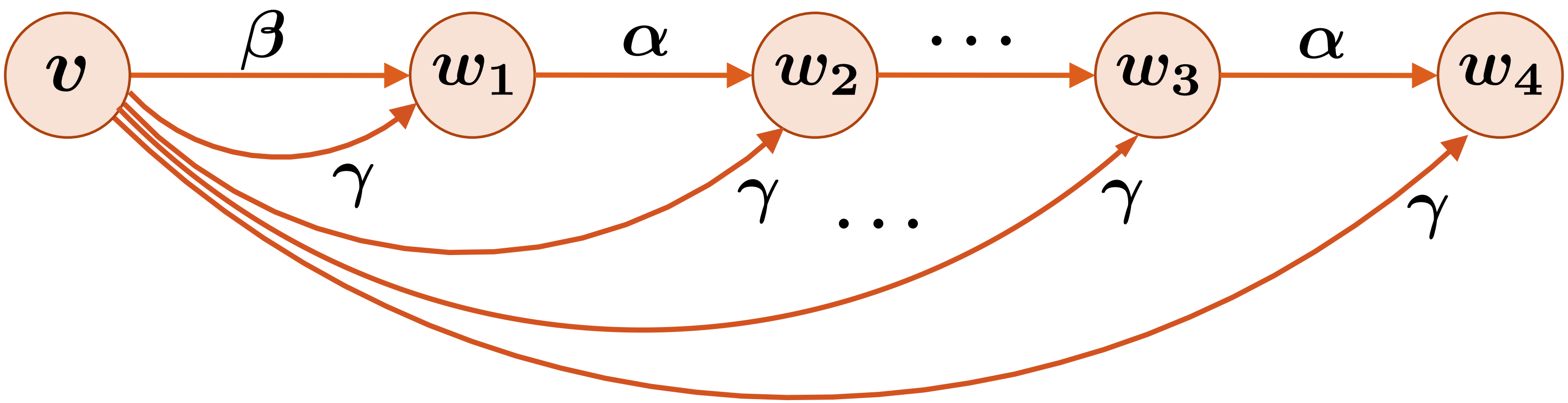
# Nondeterministic Repetition (KAT style)

$$\frac{\Gamma \vdash \beta \leq \gamma, \Delta \qquad \Gamma \vdash (\gamma; \alpha) \leq \gamma, \Delta}{\Gamma \vdash \beta; \alpha^* \leq \gamma, \Delta}(loop_r)$$

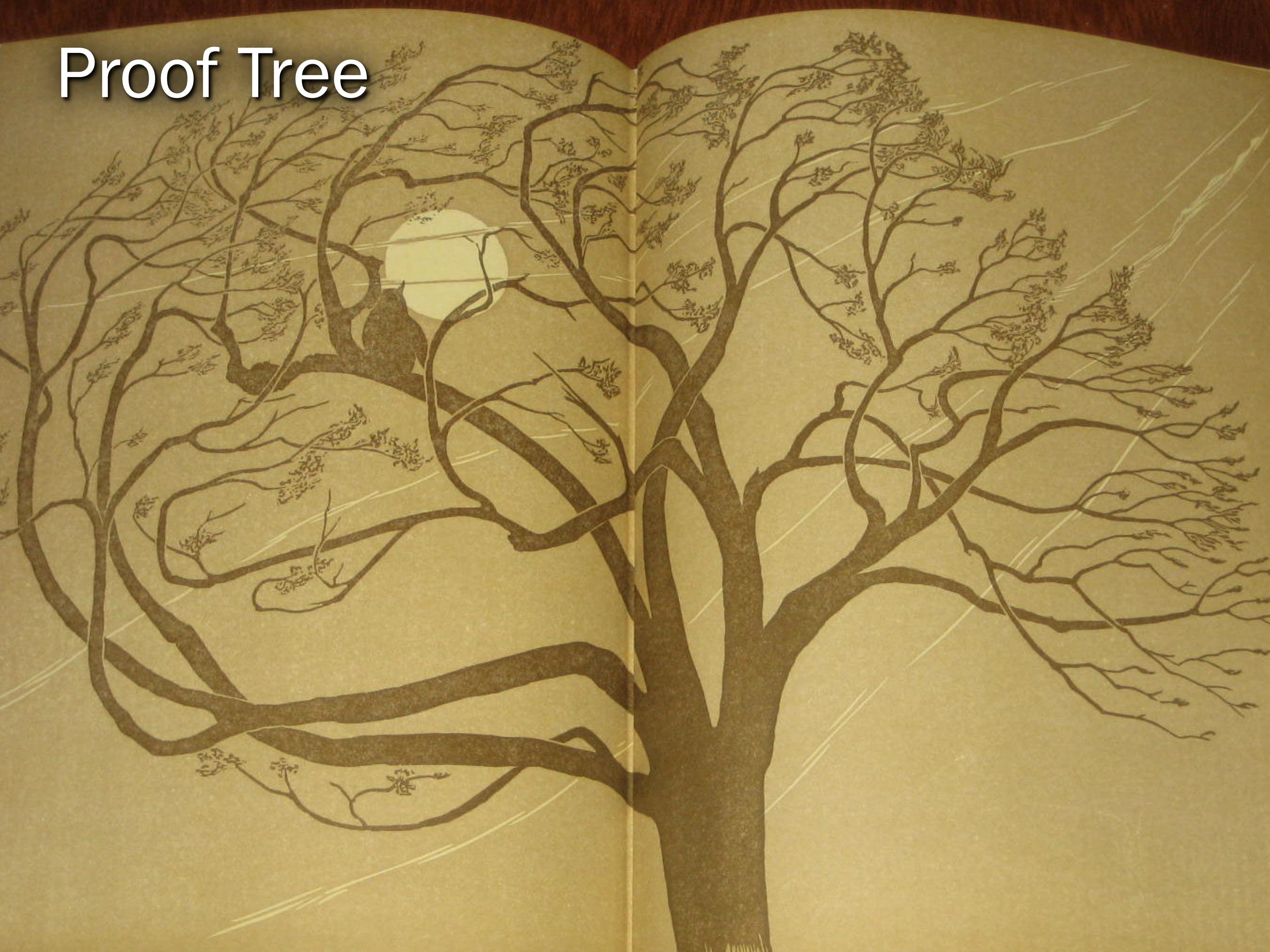
$$\boldsymbol{v} \xrightarrow{\boldsymbol{\beta}} \boldsymbol{w_1} \xrightarrow{\boldsymbol{\alpha}} \boldsymbol{w_2} \xrightarrow{\cdots} \boldsymbol{w_3} \xrightarrow{\boldsymbol{\alpha}} \boldsymbol{w_4}$$

# Nondeterministic Repetition (KAT style)

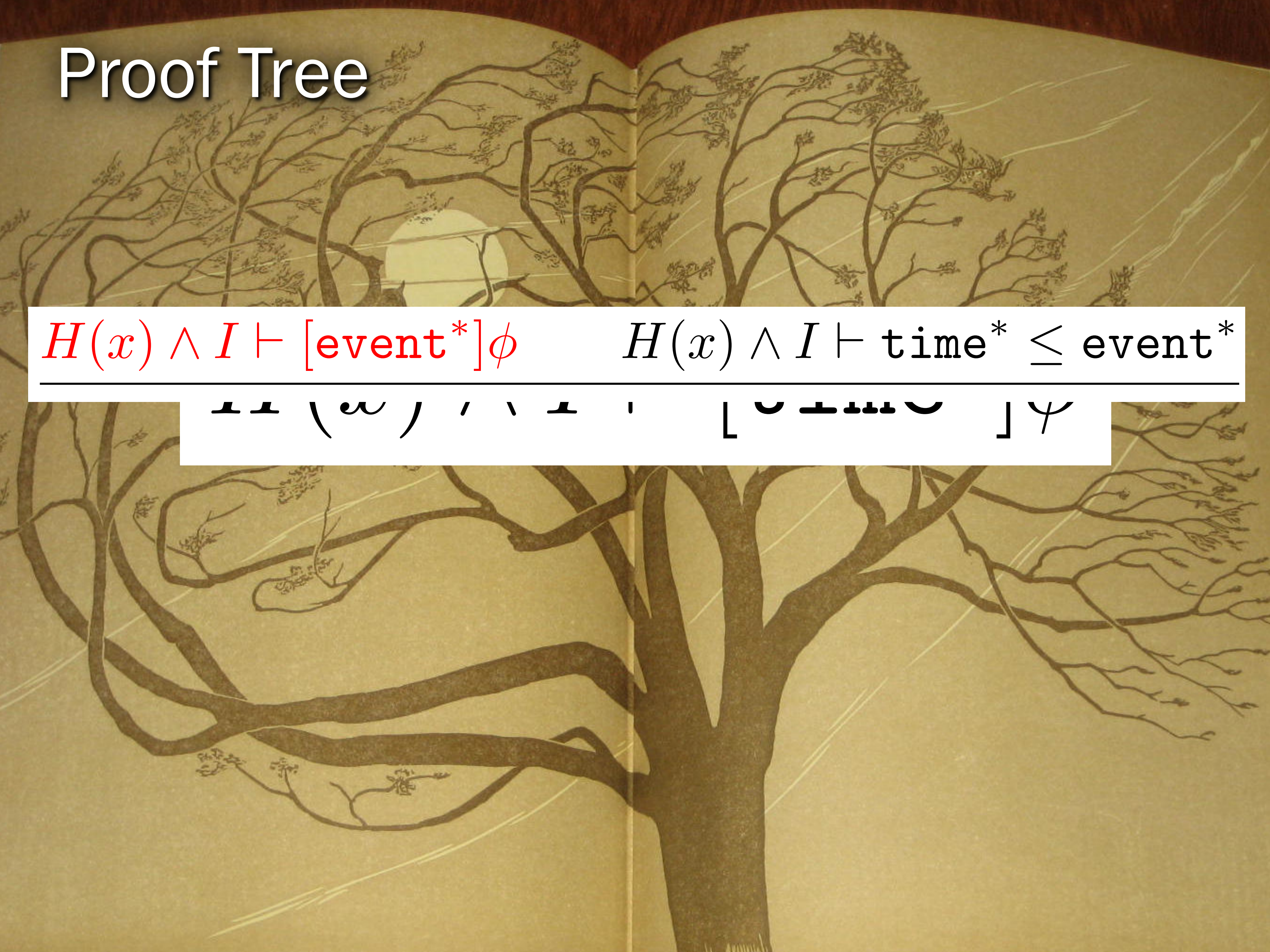
$$\frac{\Gamma \vdash \beta \leq \gamma, \Delta \qquad \Gamma \vdash (\gamma; \alpha) \leq \gamma, \Delta}{\Gamma \vdash \beta; \alpha^* \leq \gamma, \Delta}(loop_r)$$



# Proof Tree

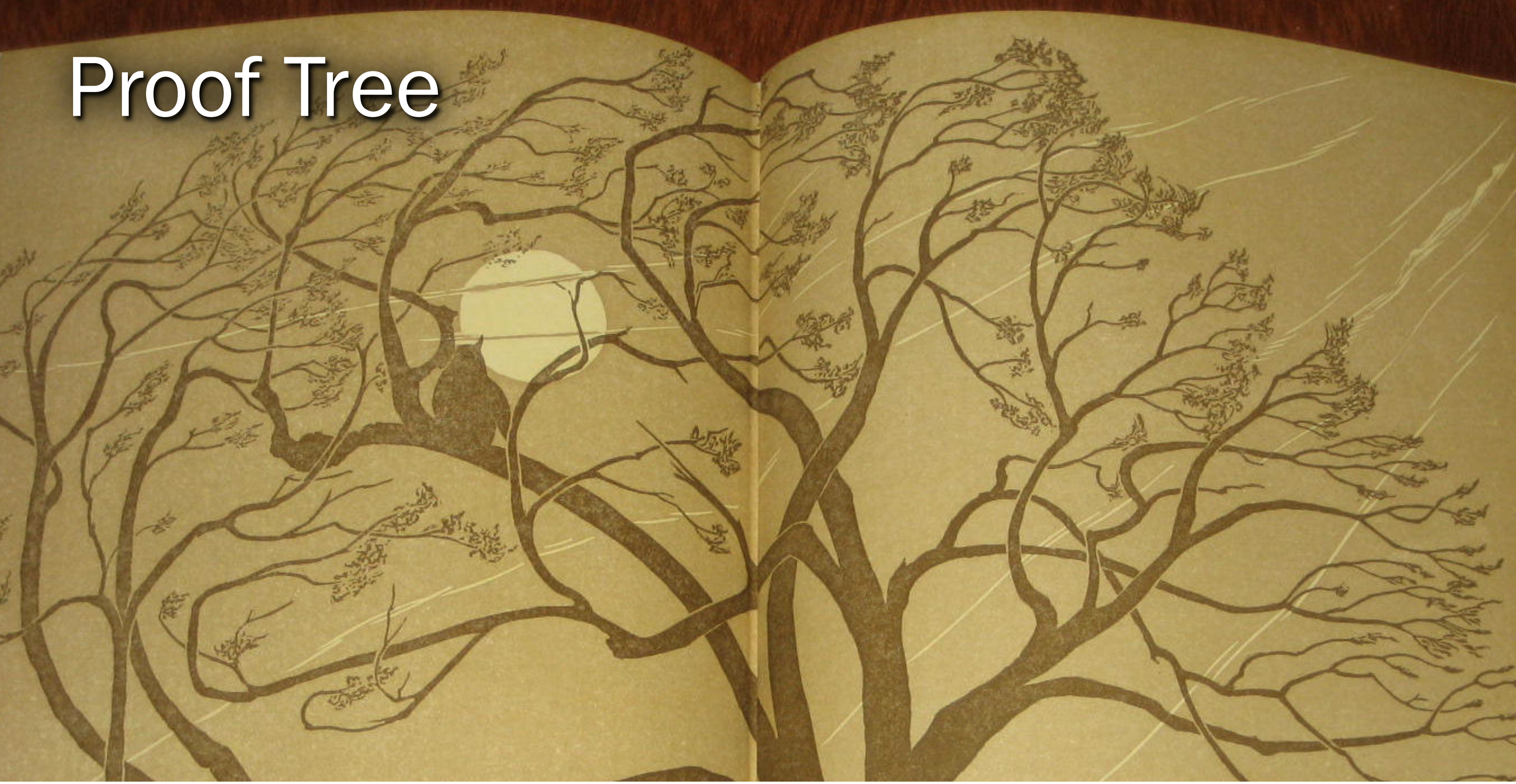


# Proof Tree



$$\frac{\color{red}{H(x) \wedge I \vdash [\mathtt{event}^*]\phi} \qquad H(x) \wedge I \vdash \mathtt{time}^* \leq \mathtt{event}^*}{H(x) \wedge I \vdash [\mathtt{time}^*]\phi}$$

# Proof Tree



$$\frac{H(x) \land I \vdash [a := c](dyn_t \le dyn_{Ev}) \qquad H(x) \land I \vdash [a := *; ?\mathrm{Safe}_\varepsilon(x,a)](dyn_t \le dyn_{Ev})}{H(x) \land I \vdash [a := c \;\cup\; (a := *; ?\mathrm{Safe}_\varepsilon(x,a))](dyn_t \le dyn_{Ev})}\;[\cup]$$

$$\frac{H(x) \land I \vdash [a := c \;\cup\; (a := *; ?\mathrm{Safe}_\varepsilon(x,a))](dyn_t \le dyn_{Ev})}{H(x) \land I \vdash [ctrl_t](dyn_t \le dyn_{Ev})}\;\mathit{subst}$$

$$\frac{H(x) \land I \vdash ctrl_t \le ctrl_{Ev} \qquad H(x) \land I \vdash [ctrl_t](dyn_t \le dyn_{Ev})}{H(x) \land I \vdash ctrl_t; dyn_t \le ctrl_{Ev}; dyn_{Ev}}\;;_A$$

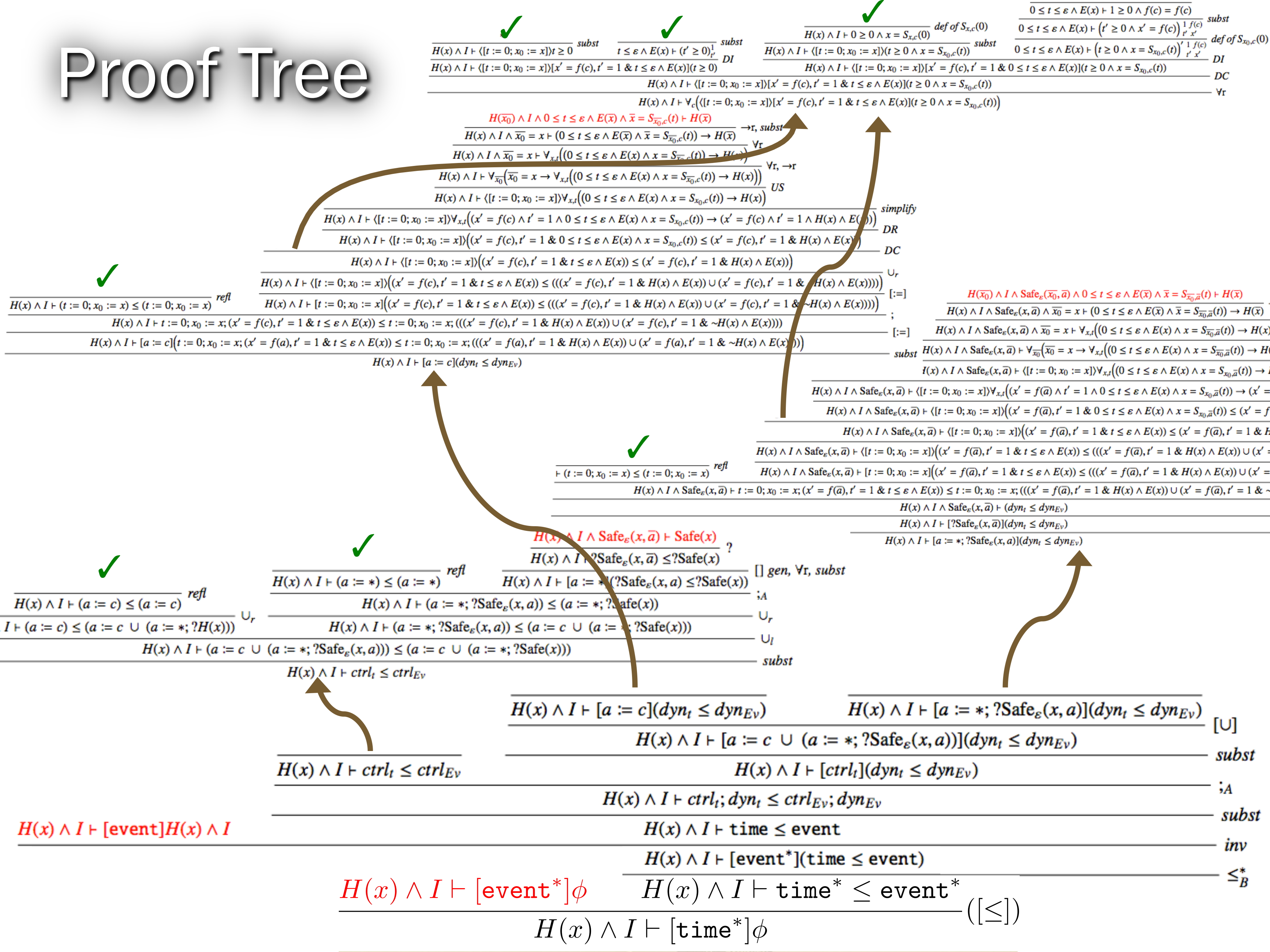
$$\frac{H(x) \land I \vdash ctrl_t; dyn_t \le ctrl_{Ev}; dyn_{Ev}}{H(x) \land I \vdash \mathtt{time} \le \mathtt{event}}\;\mathit{subst}$$

$$\frac{\color{red}{H(x) \land I \vdash [\mathtt{event}]H(x) \land I} \qquad H(x) \land I \vdash \mathtt{time} \le \mathtt{event}}{H(x) \land I \vdash [\mathtt{event}^*](\mathtt{time} \le \mathtt{event})}\;\mathit{inv}$$

$$\frac{H(x) \land I \vdash [\mathtt{event}^*](\mathtt{time} \le \mathtt{event})}{H(x) \land I \vdash \mathtt{time}^* \le \mathtt{event}^*}\;\le_B^*$$

$$\frac{\color{red}{H(x) \land I \vdash [\mathtt{event}^*]\phi} \qquad H(x) \land I \vdash \mathtt{time}^* \le \mathtt{event}^*}{H(x) \land I \vdash [\mathtt{time}^*]\phi}\;([\le])$$

# Proof Tree



H(x) ∧ I ⊢ [a := c](dyn_t ≤ dyn_Ev)
H(x) ∧ I ⊢ [a := ∗; ?Safe_ε(x, a)](dyn_t ≤ dyn_Ev)
[∪]
H(x) ∧ I ⊢ [a := c ∪ (a := ∗; ?Safe_ε(x, a))](dyn_t ≤ dyn_Ev)
subst
H(x) ∧ I ⊢ ctrl_t ≤ ctrl_Ev
H(x) ∧ I ⊢ [ctrl_t](dyn_t ≤ dyn_Ev)
;A
H(x) ∧ I ⊢ ctrl_t; dyn_t ≤ ctrl_Ev; dyn_Ev
subst
H(x) ∧ I ⊢ [event]H(x) ∧ I
H(x) ∧ I ⊢ time ≤ event
inv
H(x) ∧ I ⊢ [event*](time ≤ event)
≤*_B
H(x) ∧ I ⊢ [event*]ϕ
H(x) ∧ I ⊢ time* ≤ event*
([≤])
H(x) ∧ I ⊢ [time*]ϕ

# Proof Tree

# Open goals

$$\dfrac{\dfrac{\checkmark}{H(x)\wedge I \vdash \langle [t:=0;x_0:=x]\rangle t\geq 0}\,\text{subst} \quad \dfrac{\dfrac{\checkmark}{t\leq\varepsilon\wedge E(x)\vdash (t'\geq 0)'^{1}_{t'}}\,\text{subst}}{}\,\text{DI}}{H(x)\wedge I\vdash \langle[t:=0;x_0:=x]\rangle[x'=f(c),t'=1\,\&\,t\leq\varepsilon\wedge E(x)](t\geq 0)}$$

$$\dfrac{\dfrac{\dfrac{\checkmark}{H(x)\wedge I\vdash 0\geq 0\wedge x=S_{x,c}(0)}\,\text{def of }S_{x,c}(0)}{H(x)\wedge I\vdash\langle[t:=0;x_0:=x]\rangle(t\geq 0\wedge x=S_{x_0,c}(t))}\,\text{subst} \quad \dfrac{\dfrac{\dfrac{0\leq t\leq\varepsilon\wedge E(x)\vdash 1\geq 0\wedge f(c)=f(c)}{0\leq t\leq\varepsilon\wedge E(x)\vdash (t'\geq 0\wedge x'=f(c))^{1\,f(c)}_{t'\,x'}}\,\text{subst}}{0\leq t\leq\varepsilon\wedge E(x)\vdash (t\geq 0\wedge x=S_{x_0,c}(t))'^{1\,f(c)}_{t'\,x'}}\,\text{def of }S_{x_0,c}(0)}{}\,\text{DI}}{H(x)\wedge I\vdash\langle[t:=0;x_0:=x]\rangle[x'=f(c),t'=1\,\&\,0\leq t\leq\varepsilon\wedge E(x)](t\geq 0\wedge x=S_{x_0,c}(t))}$$

$$\dfrac{\dfrac{\ldots}{H(x)\wedge I\vdash\langle[t:=0;x_0:=x]\rangle[x'=f(c),t'=1\,\&\,t\leq\varepsilon\wedge E(x)](t\geq 0\wedge x=S_{x_0,c}(t))}\,\text{DC}}{H(x)\wedge I\vdash\forall_c(\langle[t:=0;x_0:=x]\rangle[x'=f(c),t'=1\,\&\,t\leq\varepsilon\wedge E(x)](t\geq 0\wedge x=S_{x_0,c}(t)))}\,\forall\text{r}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{H(\overline{x_0})\wedge I\wedge 0\leq t\leq\varepsilon\wedge E(\overline{x})\wedge\overline{x}=S_{\overline{x_0},c}(t)\vdash H(\overline{x})}{H(x)\wedge I\wedge\overline{x_0}=x\vdash(0\leq t\leq\varepsilon\wedge E(\overline{x})\wedge\overline{x}=S_{\overline{x_0},c}(t))\to H(\overline{x})}\,\to\text{r, subst}}{H(x)\wedge I\wedge\overline{x_0}=x\vdash\forall_{x,t}((0\leq t\leq\varepsilon\wedge E(x)\wedge x=S_{\overline{x_0},c}(t))\to H(x))}\,\forall\text{r}}{H(x)\wedge I\vdash\forall_{\overline{x_0}}(\overline{x_0}=x\to\forall_{x,t}((0\leq t\leq\varepsilon\wedge E(x)\wedge x=S_{\overline{x_0},c}(t))\to H(x)))}\,\forall\text{r},\to\text{r}}{H(x)\wedge I\vdash\langle[t:=0;x_0:=x]\rangle\forall_{x,t}((0\leq t\leq\varepsilon\wedge E(x)\wedge x=S_{x_0,c}(t))\to H(x))}\,\text{US}}{H(x)\wedge I\vdash\langle[t:=0;x_0:=x]\rangle\forall_{x,t}((x'=f(c)\wedge t'=1\wedge 0\leq t\leq\varepsilon\wedge E(x)\wedge x=S_{x_0,c}(t))\to(x'=f(c)\wedge t'=1\wedge H(x)\wedge E(x)))}\,\text{simplify}}{H(x)\wedge I\vdash\langle[t:=0;x_0:=x]\rangle((x'=f(c),t'=1\,\&\,0\leq t\leq\varepsilon\wedge E(x)\wedge x=S_{x_0,c}(t))\leq(x'=f(c),t'=1\,\&\,H(x)\wedge E(x)))}\,\text{DR}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\ldots}{H(x)\wedge I\vdash\langle[t:=0;x_0:=x]\rangle((x'=f(c),t'=1\,\&\,t\leq\varepsilon\wedge E(x))\leq(x'=f(c),t'=1\,\&\,H(x)\wedge E(x)))}\,\text{DC}}{H(x)\wedge I\vdash\langle[t:=0;x_0:=x]\rangle((x'=f(c),t'=1\,\&\,t\leq\varepsilon\wedge E(x))\leq(((x'=f(c),t'=1\,\&\,H(x)\wedge E(x))\cup(x'=f(c),t'=1\,\&\,\sim H(x)\wedge E(x))))}\,\cup_r}{\dfrac{\checkmark}{H(x)\wedge I\vdash(t:=0;x_0:=x)\leq(t:=0;x_0:=x)}\,\text{refl} \quad H(x)\wedge I\vdash[t:=0;x_0:=x]((x'=f(c),t'=1\,\&\,t\leq\varepsilon\wedge E(x))\leq(((x'=f(c),t'=1\,\&\,H(x)\wedge E(x))\cup(x'=f(c),t'=1\,\&\,\sim H(x)\wedge E(x))))}\,[:=]}{H(x)\wedge I\vdash t:=0;x_0:=x;(x'=f(c),t'=1\,\&\,t\leq\varepsilon\wedge E(x))\leq t:=0;x_0:=x;(((x'=f(c),t'=1\,\&\,H(x)\wedge E(x))\cup(x'=f(c),t'=1\,\&\,\sim H(x)\wedge E(x))))}\,;}{H(x)\wedge I\vdash[a:=c](t:=0;x_0:=x;(x'=f(a),t'=1\,\&\,t\leq\varepsilon\wedge E(x))\leq t:=0;x_0:=x;(((x'=f(a),t'=1\,\&\,H(x)\wedge E(x))\cup(x'=f(a),t'=1\,\&\,\sim H(x)\wedge E(x))))}\,[:=]}{H(x)\wedge I\vdash[a:=c](dyn_t\leq dyn_{Ev})}\,\text{subst}$$

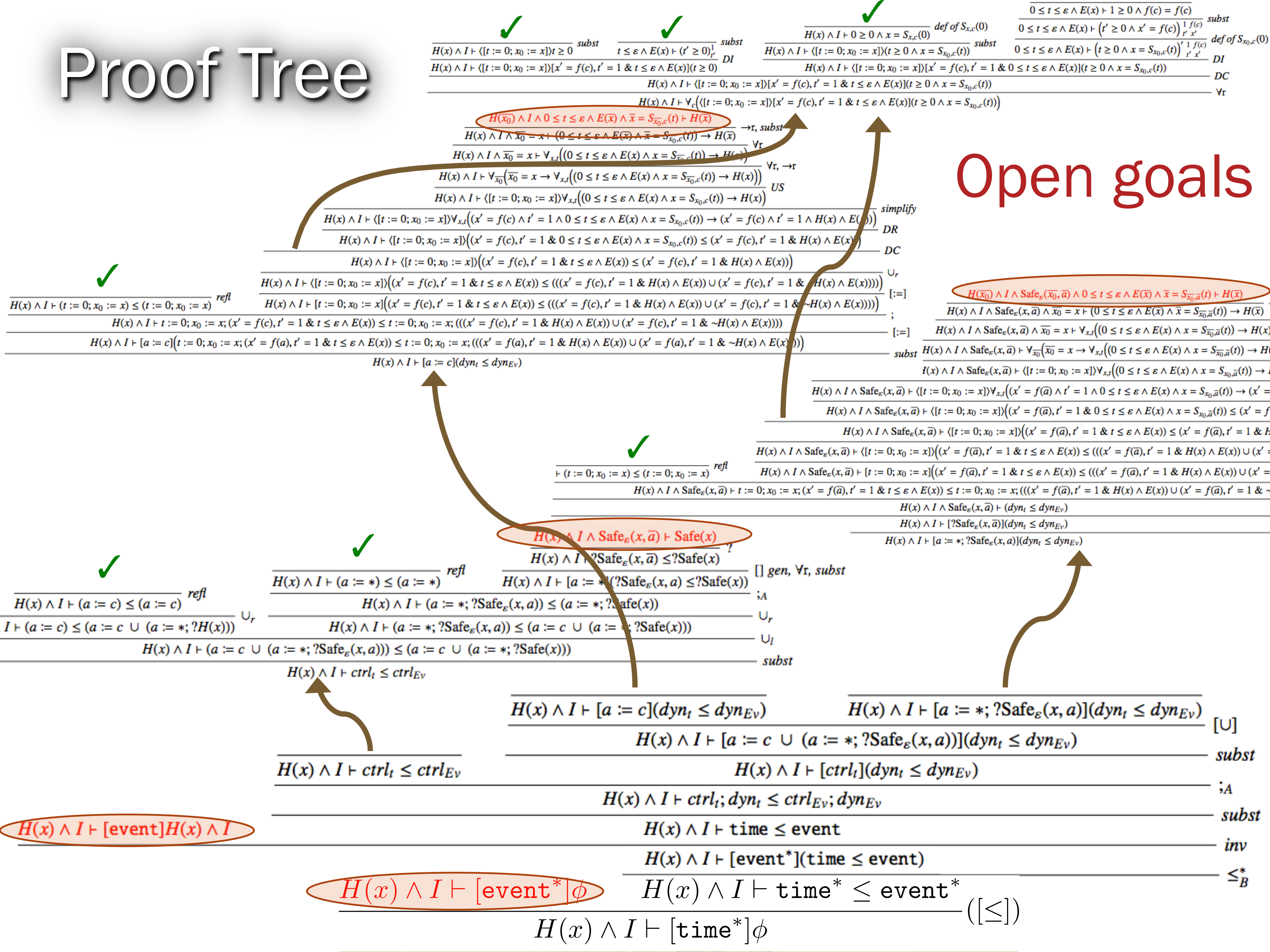
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{H(\overline{x_0})\wedge I\wedge \text{Safe}_\varepsilon(\overline{x_0},\overline{a})\wedge 0\leq t\leq\varepsilon\wedge E(\overline{x})\wedge\overline{x}=S_{\overline{x_0},\overline{a}}(t)\vdash H(\overline{x})}{H(x)\wedge I\wedge\text{Safe}_\varepsilon(x,\overline{a})\wedge\overline{x_0}=x\vdash(0\leq t\leq\varepsilon\wedge E(\overline{x})\wedge\overline{x}=S_{\overline{x_0},\overline{a}}(t))\to H(\overline{x})}}{H(x)\wedge I\wedge\text{Safe}_\varepsilon(x,\overline{a})\wedge\overline{x_0}=x\vdash\forall_{x,t}((0\leq t\leq\varepsilon\wedge E(x)\wedge x=S_{\overline{x_0},\overline{a}}(t))\to H(x))}}{H(x)\wedge I\wedge\text{Safe}_\varepsilon(x,\overline{a})\vdash\forall_{\overline{x_0}}(\overline{x_0}=x\to\forall_{x,t}((0\leq t\leq\varepsilon\wedge E(x)\wedge x=S_{\overline{x_0},\overline{a}}(t))\to H(x)))}}{H(x)\wedge I\wedge\text{Safe}_\varepsilon(x,\overline{a})\vdash\langle[t:=0;x_0:=x]\rangle\forall_{x,t}((0\leq t\leq\varepsilon\wedge E(x)\wedge x=S_{x_0,\overline{a}}(t))\to\ldots}}{H(x)\wedge I\wedge\text{Safe}_\varepsilon(x,\overline{a})\vdash\langle[t:=0;x_0:=x]\rangle\forall_{x,t}((x'=f(\overline{a})\wedge t'=1\wedge 0\leq t\leq\varepsilon\wedge E(x)\wedge x=S_{x_0,\overline{a}}(t))\to(x'=\ldots}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\ldots}{H(x)\wedge I\wedge\text{Safe}_\varepsilon(x,\overline{a})\vdash\langle[t:=0;x_0:=x]\rangle((x'=f(\overline{a}),t'=1\,\&\,0\leq t\leq\varepsilon\wedge E(x)\wedge x=S_{x_0,\overline{a}}(t))\leq(x'=f\ldots}}{H(x)\wedge I\wedge\text{Safe}_\varepsilon(x,\overline{a})\vdash\langle[t:=0;x_0:=x]\rangle((x'=f(\overline{a}),t'=1\,\&\,t\leq\varepsilon\wedge E(x))\leq(x'=f(\overline{a}),t'=1\,\&\,H\ldots}}{H(x)\wedge I\wedge\text{Safe}_\varepsilon(x,\overline{a})\vdash\langle[t:=0;x_0:=x]\rangle((x'=f(\overline{a}),t'=1\,\&\,t\leq\varepsilon\wedge E(x))\leq(((x'=f(\overline{a}),t'=1\,\&\,H(x)\wedge E(x))\cup(x'\ldots}}{\dfrac{\checkmark}{\vdash(t:=0;x_0:=x)\leq(t:=0;x_0:=x)}\,\text{refl}\quad H(x)\wedge I\wedge\text{Safe}_\varepsilon(x,\overline{a})\vdash[t:=0;x_0:=x]((x'=f(\overline{a}),t'=1\,\&\,t\leq\varepsilon\wedge E(x))\leq(((x'=f(\overline{a}),t'=1\,\&\,H(x)\wedge E(x))\cup(x'\ldots}}{H(x)\wedge I\wedge\text{Safe}_\varepsilon(x,\overline{a})\vdash t:=0;x_0:=x;(x'=f(\overline{a}),t'=1\,\&\,t\leq\varepsilon\wedge E(x))\leq t:=0;x_0:=x;(((x'=f(\overline{a}),t'=1\,\&\,H(x)\wedge E(x))\cup(x'=f(\overline{a}),t'=1\,\&\,\sim\ldots}}{H(x)\wedge I\wedge\text{Safe}_\varepsilon(x,\overline{a})\vdash(dyn_t\leq dyn_{Ev})}}{H(x)\wedge I\vdash[?\text{Safe}_\varepsilon(x,\overline{a})](dyn_t\leq dyn_{Ev})}}{H(x)\wedge I\vdash[a:=*;?\text{Safe}_\varepsilon(x,a)](dyn_t\leq dyn_{Ev})}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\checkmark}{H(x)\wedge I\vdash(a:=c)\leq(a:=c)}\,\text{refl}}{I\vdash(a:=c)\leq(a:=c\,\cup\,(a:=*;?H(x)))}\,\cup_r \quad \dfrac{\dfrac{\dfrac{\checkmark}{H(x)\wedge I\vdash(a:=*)\leq(a:=*)}\,\text{refl}\quad\dfrac{\dfrac{H(x)\wedge I\wedge\text{Safe}_\varepsilon(x,\overline{a})\vdash\text{Safe}(x)}{H(x)\wedge I\vdash ?\text{Safe}_\varepsilon(x,\overline{a})\leq ?\text{Safe}(x)}\,?}{H(x)\wedge I\vdash[a:=*](?\text{Safe}_\varepsilon(x,a)\leq ?\text{Safe}(x))}\,[]\text{ gen},\forall\text{r, subst}}{H(x)\wedge I\vdash(a:=*;?\text{Safe}_\varepsilon(x,a))\leq(a:=*;?\text{Safe}(x))}\,;A}{H(x)\wedge I\vdash(a:=*;?\text{Safe}_\varepsilon(x,a))\leq(a:=c\,\cup\,(a:=*;?\text{Safe}(x)))}\,\cup_r}{H(x)\wedge I\vdash(a:=c\,\cup\,(a:=*;?\text{Safe}_\varepsilon(x,a)))\leq(a:=c\,\cup\,(a:=*;?\text{Safe}(x)))}\,\cup_l}{H(x)\wedge I\vdash ctrl_t\leq ctrl_{Ev}}\,\text{subst}$$

$$\dfrac{H(x)\wedge I\vdash[\texttt{event}^*]\phi \qquad \dfrac{\dfrac{H(x)\wedge I\vdash[\texttt{event}]H(x)\wedge I \qquad \dfrac{\dfrac{\dfrac{H(x)\wedge I\vdash ctrl_t\leq ctrl_{Ev}\qquad\dfrac{\dfrac{H(x)\wedge I\vdash[a:=c](dyn_t\leq dyn_{Ev})\qquad H(x)\wedge I\vdash[a:=*;?\text{Safe}_\varepsilon(x,a)](dyn_t\leq dyn_{Ev})}{H(x)\wedge I\vdash[a:=c\,\cup\,(a:=*;?\text{Safe}_\varepsilon(x,a))](dyn_t\leq dyn_{Ev})}\,[\cup]}{H(x)\wedge I\vdash[ctrl_t](dyn_t\leq dyn_{Ev})}\,\text{subst}}{H(x)\wedge I\vdash ctrl_t;dyn_t\leq ctrl_{Ev};dyn_{Ev}}\,;A}{H(x)\wedge I\vdash\texttt{time}\leq\texttt{event}}\,\text{subst}}{H(x)\wedge I\vdash[\texttt{event}^*](\texttt{time}\leq\texttt{event})}\,\text{inv}}{H(x)\wedge I\vdash\texttt{time}^*\leq\texttt{event}^*}\,\leq^*_B}{H(x)\wedge I\vdash[\texttt{time}^*]\phi}\,([\leq])$$

# Proof Tree



Open goals
H(x) ∧ I ⊢ [a := c](dyn_t ≤ dyn_Ev)
H(x) ∧ I ⊢ [a := ∗; ?Safe_ε(x, a)](dyn_t ≤ dyn_Ev)
[∪]
H(x) ∧ I ⊢ [a := c ∪ (a := ∗; ?Safe_ε(x, a))](dyn_t ≤ dyn_Ev)
subst
H(x) ∧ I ⊢ ctrl_t ≤ ctrl_Ev
H(x) ∧ I ⊢ [ctrl_t](dyn_t ≤ dyn_Ev)
;A
H(x) ∧ I ⊢ ctrl_t; dyn_t ≤ ctrl_Ev; dyn_Ev
subst
H(x) ∧ I ⊢ [event]H(x) ∧ I
H(x) ∧ I ⊢ time ≤ event
inv
H(x) ∧ I ⊢ [event*](time ≤ event)
≤*_B
H(x) ∧ I ⊢ [event*]φ
H(x) ∧ I ⊢ time* ≤ event*
([≤])
H(x) ∧ I ⊢ [time*]φ
H(x) ∧ I ⊢ ctrl_t ≤ ctrl_Ev
H(x) ∧ I ⊢ (a := c) ≤ (a := c)
refl
H(x) ∧ I ⊢ (a := ∗) ≤ (a := ∗)
refl
H(x) ∧ I ∧ Safe_ε(x, a) ⊢ Safe(x)
H(x) ∧ I ⊢ [a := c](dyn_t ≤ dyn_Ev)
H(x) ∧ I ⊢ [a := ∗; ?Safe_ε(x, a)](dyn_t ≤ dyn_Ev)

# Proof Tree

"Braking" is safe for $\varepsilon$ time

$H(S_c(0)) \land 0 \le t \le \varepsilon \vdash H(S_c(t))$

"Accelerating" is safe for $\varepsilon$ time

$\texttt{Safe}_\varepsilon(S_a(0)) \land 0 \le t \le \varepsilon \vdash H(S_a(t))$

Controllers satisfy refinement

$\vdash \ \texttt{Safe}_\varepsilon \to \texttt{Safe}$

Event-triggered is safe

d$\mathcal{L}$

$H(x) \land I \vdash [\texttt{event}]H(x) \land I$

---

Time-triggered is safe

$H(x) \land I \vdash [\texttt{time}^*]\phi$

# Proof Tree

$\mathrm{FOL}_{\mathbb{R}}$

"Braking" is safe for $\varepsilon$ time

$H(S_c(0)) \land 0 \leq t \leq \varepsilon \vdash H(S_c(t))$

$\mathrm{FOL}_{\mathbb{R}}$

"Accelerating" is safe for $\varepsilon$ time

$\mathtt{Safe}_\varepsilon(S_a(0)) \land 0 \leq t \leq \varepsilon \vdash H(S_a(t))$

Controllers satisfy refinement

$\vdash \ \mathtt{Safe}_\varepsilon \to \mathtt{Safe}$

$\mathrm{FOL}_{\mathbb{R}}$

Event-triggered is safe

$H(x) \land I \vdash [\mathtt{event}]H(x) \land I$

$\mathrm{d}\mathcal{L}$

---

Time-triggered is safe

$H(x) \land I \vdash [\mathtt{time}^*]\phi$

# dRL Proof Rules: Partial Order

Reflexive:

$$\frac{}{\Gamma \vdash \alpha \leq \alpha, \Delta}(\leq_{refl})$$

Transitive:

$$\frac{\Gamma \vdash \alpha \leq \beta, \Delta \qquad \Gamma \vdash \beta \leq \gamma, \Delta}{\Gamma \vdash \alpha \leq \gamma, \Delta}(\leq_{trans})$$

Antisymmetric:

$$\frac{\Gamma \vdash \alpha \leq \beta, \Delta \qquad \Gamma \vdash \beta \leq \alpha, \Delta}{\Gamma \vdash \alpha = \beta, \Delta}(\leq_{antisym})^1$$

# dRL Proof Rules: KAT

$$\frac{}{\Gamma \vdash \alpha \cup (\beta \cup \gamma) = (\alpha \cup \beta) \cup \gamma, \Delta}(\cup_{assoc}) \qquad \frac{}{\Gamma \vdash \alpha \cup \beta = \beta \cup \alpha, \Delta}(\cup_{comm})$$

$$\frac{}{\Gamma \vdash \alpha \cup ?\bot = \alpha, \Delta}(\cup_{id}) \qquad \frac{}{\Gamma \vdash (\alpha \cup \alpha) = \alpha, \Delta}(\cup_{idemp})$$

$$\frac{}{\Gamma \vdash \alpha; (\beta; \gamma) = (\alpha; \beta); \gamma, \Delta}(;_{assoc}) \qquad \frac{}{\Gamma \vdash (?\top; \alpha) = \alpha, \Delta}(;_{id-l}) \qquad \frac{}{\Gamma \vdash (\alpha; ?\top) = \alpha, \Delta}(;_{id-r})$$

$$\frac{}{\Gamma \vdash \alpha; (\beta \cup \gamma) = ((\alpha; \beta) \cup (\alpha; \gamma)), \Delta}(dist\text{-}l) \qquad \frac{}{\Gamma \vdash (\alpha \cup \beta); \gamma = ((\alpha; \gamma) \cup (\beta; \gamma)), \Delta}(dist - r)$$

$$\frac{}{\Gamma \vdash (\alpha; ?\bot) = ?\bot, \Delta}(;_{annih-r}) \qquad \frac{}{\Gamma \vdash (?\bot; \alpha) = ?\bot, \Delta}(;_{annih-l})$$

$$\frac{}{\Gamma \vdash (?\top \cup (\alpha; \alpha^*)) = \alpha^*, \Delta}(unroll_l) \qquad \frac{}{\Gamma \vdash (?\top \cup (\alpha^*; \alpha)) = \alpha^*, \Delta}(unroll_r)$$

$$\frac{\Gamma \vdash [\alpha^*](\alpha; \gamma) \le \gamma, \Delta \qquad \Gamma \vdash [\alpha^*]\beta \le \gamma, \Delta}{\Gamma \vdash \alpha^*; \beta \le \gamma, \Delta}(loop_l) \qquad \frac{\Gamma \vdash \beta \le \gamma, \Delta \qquad \Gamma \vdash (\gamma; \alpha) \le \gamma, \Delta}{\Gamma \vdash \beta; \alpha^* \le \gamma, \Delta}(loop_r)$$

# dRL Proof Rules: Differential Equations

$$\frac{\Gamma \vdash [x' = \theta \,\&\, H_1]H_2, \Delta}{\Gamma \vdash (x' = \theta \,\&\, H_1) = (x' = \theta \,\&\, H_1 \wedge H_2), \Delta}(DC)$$

$$\frac{\Gamma \vdash \forall x\, (H_1 \rightarrow H_2), \Delta}{\Gamma \vdash (x' = \theta \,\&\, H_1) \leq (x' = \theta \,\&\, H_2), \Delta}(DR)$$

$$\frac{\Gamma \vdash \forall x \Big(\theta_1 ||\theta_2|| = \theta_2 ||\theta_1|| \wedge (||\theta_1||^2 = 0 \leftrightarrow ||\theta_2||^2 = 0)\Big), \Delta}{\Gamma \vdash (x' = \theta_1) = (x' = \theta_2), \Delta} \,(\textit{match direction field})^2$$

$$\frac{\Gamma \vdash \forall x \left(\frac{\theta_1}{||\theta_1||} = \frac{\theta_2}{||\theta_2||} \wedge (||\theta_1|| = 0 \leftrightarrow ||\theta_2|| = 0)\right), \Delta}{\Gamma \vdash (x' = \theta_1) = (x' = \theta_2), \Delta} \,(\textit{mdf})^2$$

# dRL Proof Rules: Structural

$$\frac{\Gamma \vdash \alpha \leq \gamma \wedge \beta \leq \gamma, \Delta}{\Gamma \vdash \alpha \cup \beta \leq \gamma, \Delta}(\cup_l)$$

$$\frac{\Gamma \vdash \alpha \leq \beta \vee \alpha \leq \gamma, \Delta}{\Gamma \vdash \alpha \leq \beta \cup \gamma, \Delta}(\cup_r)$$

$$\frac{\Gamma \vdash [\alpha^*](\alpha \leq \beta), \Delta}{\Gamma \vdash \alpha^* \leq \beta^*, \Delta}(unloop)$$

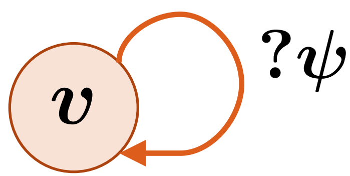
$$\frac{\Gamma \vdash \alpha_1 \leq \alpha_2, \Delta \qquad \Gamma \vdash [\alpha_1]\,(\beta_1 \leq \beta_2), \Delta}{\Gamma \vdash (\alpha_1;\beta_1) \leq (\alpha_2;\beta_2), \Delta}(\,;\,)$$

$$\frac{}{\Gamma \vdash (x := \theta) \leq (x := *), \Delta}(:= *)$$

$$\frac{\Gamma \vdash \phi \rightarrow \psi, \Delta}{\Gamma \vdash ?\phi \leq ?\psi, \Delta}(?)$$

# Test

$$\frac{\Gamma \vdash \phi \rightarrow \psi, \Delta}{\Gamma \vdash ?\phi \leq ?\psi, \Delta}(?)$$

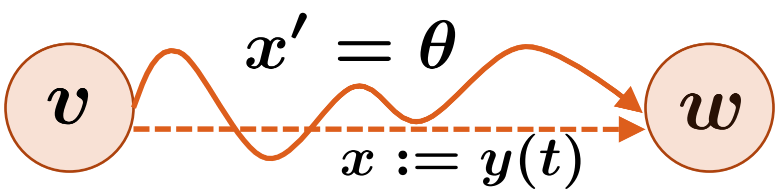



Iff $\psi$ holds in state $v$

$$\rho(?\psi) = \{(v, v) : v \models \psi\}$$

# Differential Refinement

$$\frac{\Gamma \vdash \forall x\,(H_1 \rightarrow H_2), \Delta}{\Gamma \vdash (x' = \theta \,\&\, H_1) \leq (x' = \theta \,\&\, H_2), \Delta}\,(DR)$$

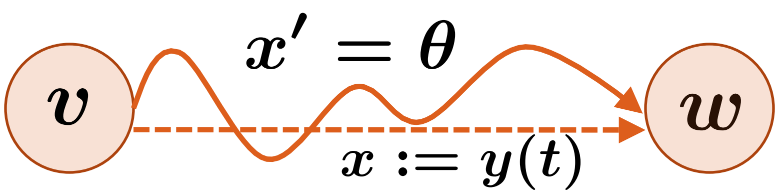



If $y(t)$ solves $x' = \theta$

$$\rho(x' = \theta) = \{(\varphi(0), \varphi(t)) : \varphi(s) \models x' = \theta \text{ for all } 0 \leq s \leq t\}$$

# dRL Proof Rules: Differential Equations

$$\frac{\Gamma \vdash [x' = \theta \,\&\, H_1]H_2, \Delta}{\Gamma \vdash (x' = \theta \,\&\, H_1) = (x' = \theta \,\&\, H_1 \wedge H_2), \Delta}(DC)$$



# Kleene Algebra with Tests (KAT)

- Kleene algebra with tests is a system for manipulating programs that are equivalent.
- KAT doesn't have continuous dynamics, but we can see that it is still relevant to hybrid programs



[Kozen97]

# Verifying a specific local lane controller

$$
\begin{aligned}
\texttt{llc} &\equiv (ctrl; dyn)^* \\
ctrl &\equiv \ell_{ctrl} \,||\, f_{ctrl}; \\
\ell_{ctrl} &\equiv (a_\ell := *;\ \ ?(-B \le a_\ell \le A)) \\
f_{ctrl} &\equiv \texttt{brake} \cup \texttt{safe}_* \cup \texttt{stopped} \\
\texttt{brake} &\equiv (a_f := *;\ \ ?(-B \le a_f \le -b)) \\
\texttt{safe}_* &\equiv (?\mathbf{Safe}_\varepsilon;\ \ a_f := *;\ \ ?(-B \le a_f \le A)) \\
\texttt{stopped} &\equiv (?(v_f = 0);\ a_f := 0) \\
\mathbf{Safe}_\varepsilon &\equiv x_f + \frac{v_f^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v_f\right) < x_\ell + \frac{v_\ell^2}{2B} \\
dyn &\equiv (t := 0;\ x_f' = v_f,\ v_f' = a_f,\ x_\ell' = v_\ell,\ v_\ell' = a_\ell, t' = 1 \\
&\qquad \&\ v_f \ge 0 \ \wedge\ v_\ell \ge 0 \ \wedge\ t \le \varepsilon)
\end{aligned}
$$

# Verifying a specific local lane controller

$$
\begin{aligned}
\mathtt{llc}_\theta &\equiv (ctrl_\theta; dyn)^* \\
ctrl_\theta &\equiv \ell_{ctrl} \parallel f_{ctrl_\theta}; \\
\ell_{ctrl} &\equiv (a_\ell := *;\ \ ?(-B \le a_\ell \le A)) \\
f_{ctrl_\theta} &\equiv \mathtt{brake} \cup \mathtt{safe}_\theta \cup \mathtt{stopped} \\
\mathtt{brake} &\equiv (a_f := *;\ \ ?(-B \le a_f \le -b)) \\
\mathtt{safe}_\theta &\equiv a_f := \theta(x_f, x_\ell, v_f, v_\ell) \\
\mathtt{stopped} &\equiv (?(v_f = 0);\ a_f := 0) \\
&\cancel{\mathbf{Safe}_\varepsilon \equiv x_f + \frac{v_f^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v_f\right) < x_\ell + \frac{v_\ell^2}{2B}} \\
dyn &\equiv (t := 0;\ x_f' = v_f,\ v_f' = a_f,\ x_\ell' = v_\ell,\ v_\ell' = a_\ell, t' = 1 \\
&\quad \&\, v_f \ge 0\ \wedge\ v_\ell \ge 0\ \wedge\ t \le \varepsilon)
\end{aligned}
$$

# Additional dRL applications

- Designing proof search heuristics that exploit refinement to automatically create more hierarchical proof structures.
- Shifting the proof responsibility completely to determining refinement.
- Code synthesis – verifying that refinement relation is satisfied with each transformation step.

# Event-triggered vs. Time-triggered

## Event-triggered

- Continuous sensing
- Unrealistic, hard to implement
- Easier to design controllers
- Easier to verify

## Time-triggered

- Discrete sensing
- Realistic, easy to implement
- Difficult to design controllers
- Challenging to verify

$$\Big(\underbrace{\texttt{ctrl}}_{\text{discrete controller}};\underbrace{\texttt{dyn}}_{\text{continuous dynamics}}\Big)^*$$

# Event-triggered vs. Time-triggered

## Event-triggered

- Continuous sensing
- Unrealistic, hard to implement
- Easier to design controllers
- Easier to verify

## Time-triggered

- Discrete sensing
- Realistic, easy to implement
- Difficult to design controllers
- Challenging to verify

$$(\underbrace{\texttt{ctrl}}_{\text{discrete controller}};\ \underbrace{x' = \theta}_{\text{continuous dynamics}})^*$$

# Event-triggered vs. Time-triggered

| Event-triggered | Time-triggered |
|---|---|
| • Continuous sensing | • Discrete sensing |
| • Unrealistic, hard to implement | • Realistic, easy to implement |
| • Easier to design controllers | • Difficult to design controllers |
| • Easier to verify | • Challenging to verify |

$$(\underbrace{\texttt{ctrl}}_{\text{discrete controller}};\ \underbrace{x' = \theta \,\&\, H}_{\text{continuous dynamics}})^*$$

# Event-triggered vs. Time-triggered

| Event-triggered | Time-triggered |
|---|---|
| • Continuous sensing | • Discrete sensing |
| • Unrealistic, hard to implement | • Realistic, easy to implement |
| • Easier to design controllers | • Difficult to design controllers |
| • Easier to verify | • Challenging to verify |

$$(\texttt{ctrl};\ x' = \theta \,\&\, H)^*$$

discrete
controller

?

# Event-triggered vs. Time-triggered

| Event-triggered | Time-triggered |
|---|---|
| • Continuous sensing | • Discrete sensing |
| • Unrealistic, hard to implement | • Realistic, easy to implement |
| • Easier to design controllers | • Difficult to design controllers |
| • Easier to verify | • Challenging to verify |

$$(\mathtt{ctrl_t}; x' = \theta \,\&\, t \le \varepsilon)^*$$

discrete
controller

?

# Event-triggered vs. Time-triggered

## Event-triggered

- Continuous sensing
- Unrealistic, hard to implement
- Easier to design controllers
- Easier to verify

## Time-triggered

- Discrete sensing
- Realistic, easy to implement
- Difficult to design controllers
- Challenging to verify

$$(\mathtt{ctrl}_{\mathtt{t}};\, x' = \theta \;\&\; t \leq \varepsilon)^*$$

# Event-triggered vs. Time-triggered

## Event-triggered

- Continuous sensing
- Unrealistic, hard to implement
- Easier to design controllers
- Easier to verify

$$(\texttt{ctrl}_{\texttt{e}};\ x' = \theta\ \&\ x + \frac{v^2}{2B} \leq S)^*$$

## Time-triggered

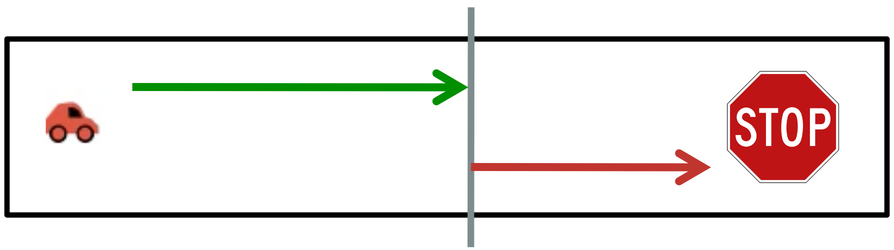
- Discrete sensing
- Realistic, easy to implement
- Difficult to design controllers
- Challenging to verify

$$(\texttt{ctrl}_{\texttt{t}}; x' = \theta\ \&\ t \leq \varepsilon)^*$$

# Event-triggered vs. Time-triggered

## Event-triggered

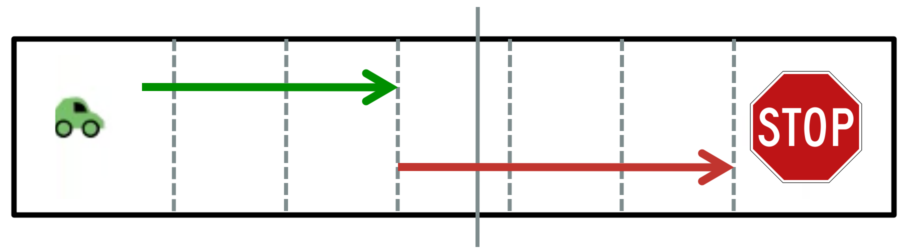
- Continuous sensing




$$(\mathtt{ctrl_e};\ x' = \theta \,\&\, x + \frac{v^2}{2B} \leq S)^*$$

## Time-triggered

- Discrete sensing

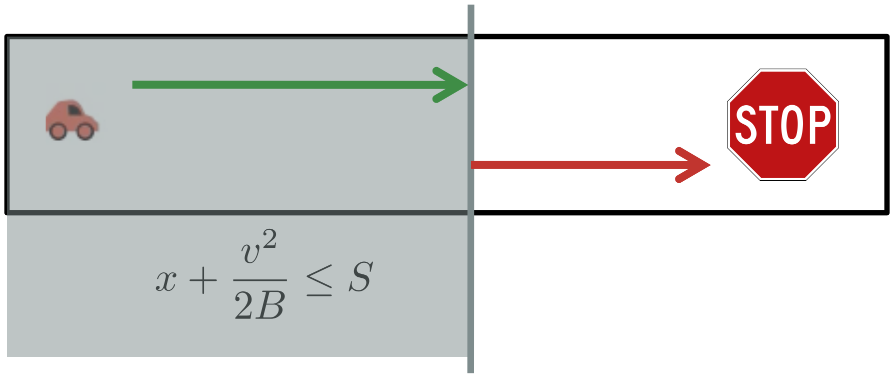



$$(\mathtt{ctrl_t}; x' = \theta \,\&\, t \leq \varepsilon)^*$$

# Event-triggered vs. Time-triggered

## Event-triggered

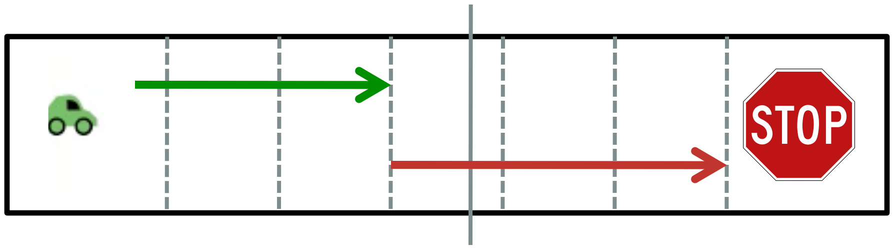
- Continuous sensing




$$(\mathtt{ctrl_e};\ x' = \theta \,\&\, x + \frac{v^2}{2B} \leq S)^*$$

## Time-triggered

- Discrete sensing

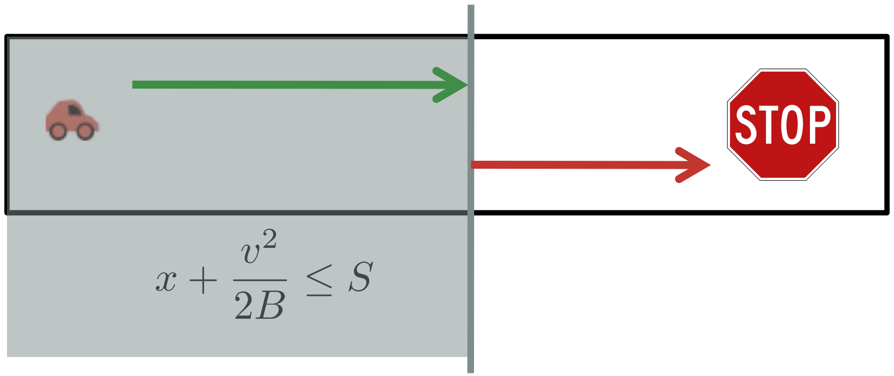



$$(\mathtt{ctrl_t}; x' = \theta \,\&\, t \leq \varepsilon)^*$$

# Event-triggered vs. Time-triggered

## Event-triggered

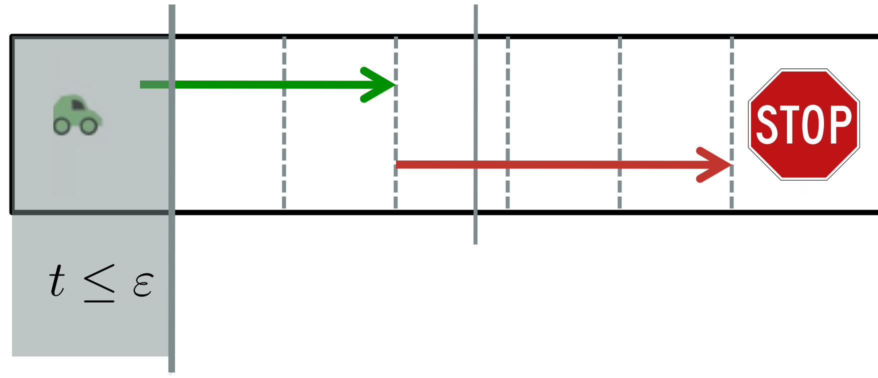
- Continuous sensing




$$(\mathtt{ctrl_e};\ x' = \theta \,\&\, x + \frac{v^2}{2B} \le S)^*$$

## Time-triggered

- Discrete sensing

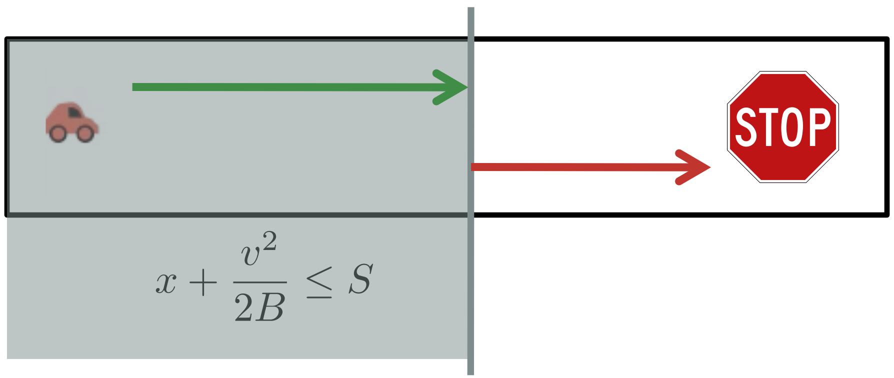



$$(\mathtt{ctrl_t}; x' = \theta \,\&\, t \le \varepsilon)^*$$

# Event-triggered vs. Time-triggered

## Event-triggered

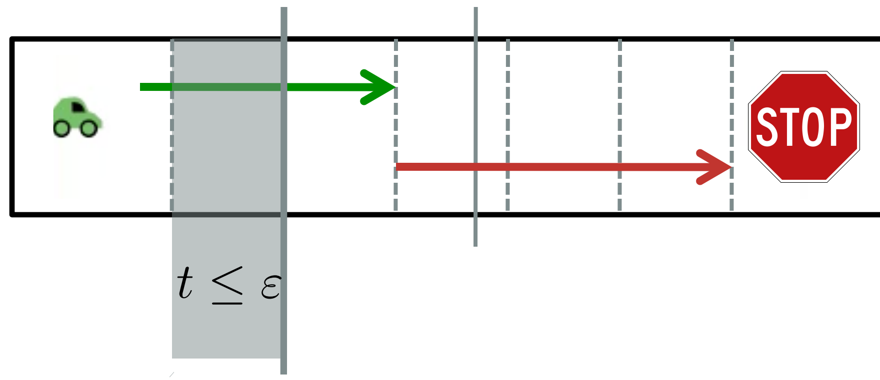
- Continuous sensing




$$(\mathtt{ctrl}_\mathtt{e};\ x' = \theta \,\&\, x + \frac{v^2}{2B} \leq S)^*$$

## Time-triggered

- Discrete sensing

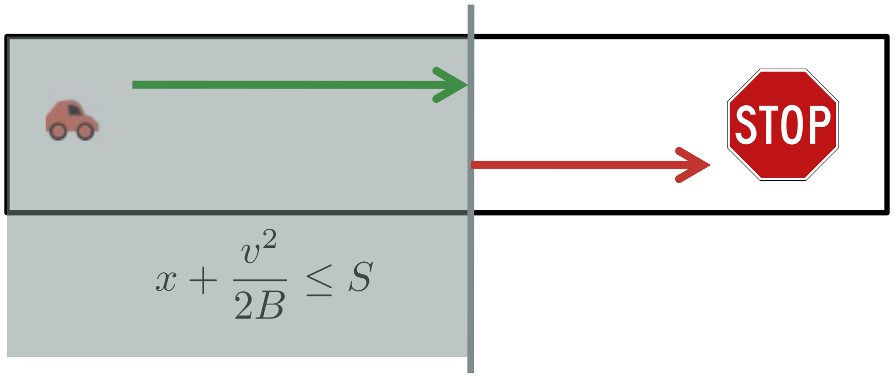



$$(\mathtt{ctrl}_\mathtt{t}; x' = \theta \,\&\, t \leq \varepsilon)^*$$

# Event-triggered vs. Time-triggered

## Event-triggered

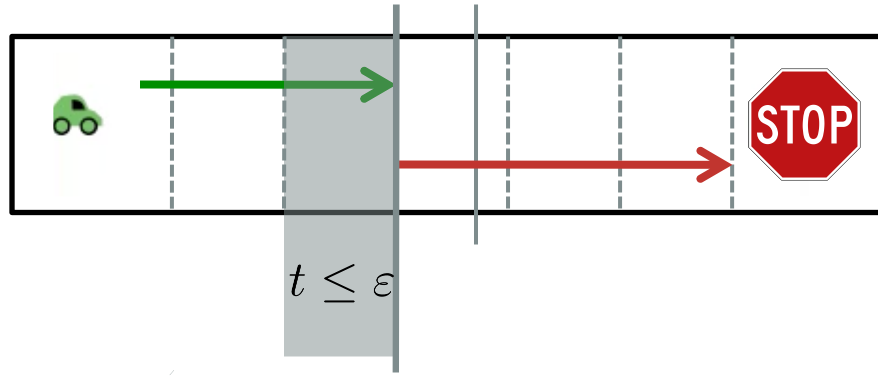
- Continuous sensing




$$(\mathtt{ctrl}_{\mathtt{e}};\ x' = \theta \,\&\, x + \frac{v^2}{2B} \leq S)^*$$

## Time-triggered

- Discrete sensing




$$(\mathtt{ctrl}_{\mathtt{t}};\, x' = \theta \,\&\, t \leq \varepsilon)^*$$

# Event-triggered vs. Time-triggered

## event-triggered

$$((?\mathtt{Safe}; a := *) \cup a := c;$$
$$x' = \theta \,\&\, E(x))^*$$

## time-triggered

$$((?\mathtt{Safe}_\varepsilon; a := *) \cup a := c;$$
$$x' = \theta \,\&\, t \leq \varepsilon)^*$$

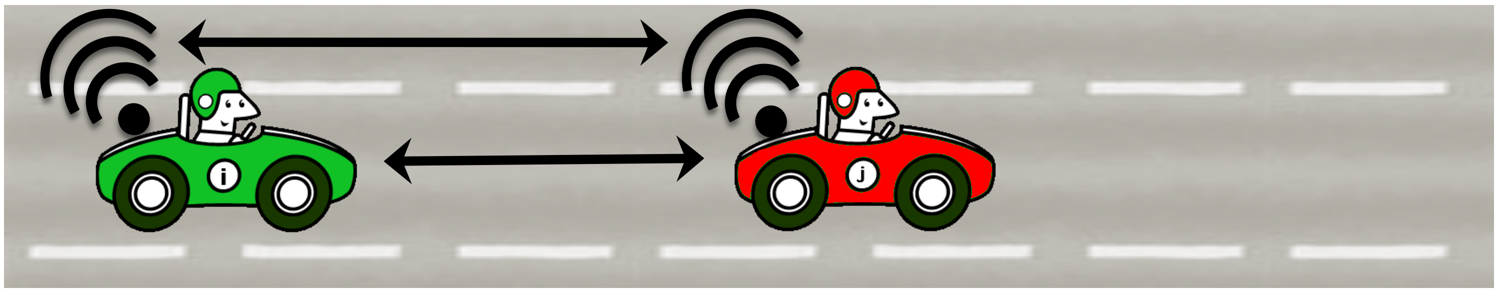
# dRL Proof Rules: Independence

$$\frac{}{\vdash (x := \theta_1; y := \theta_2) = (y := \theta_2; x := \theta_1)}(indep_{:=})$$

$$\frac{}{\vdash (x' = \theta_1; y' = \theta_2) = (y' = \theta_2; x' = \theta_1)}(indep')$$

$$\frac{}{\vdash (x := \theta_1; y' = \theta_2) = (y' = \theta_2; x := \theta_1)}(indep'_{:=})$$

# Motivation: Adaptive Cruise Control

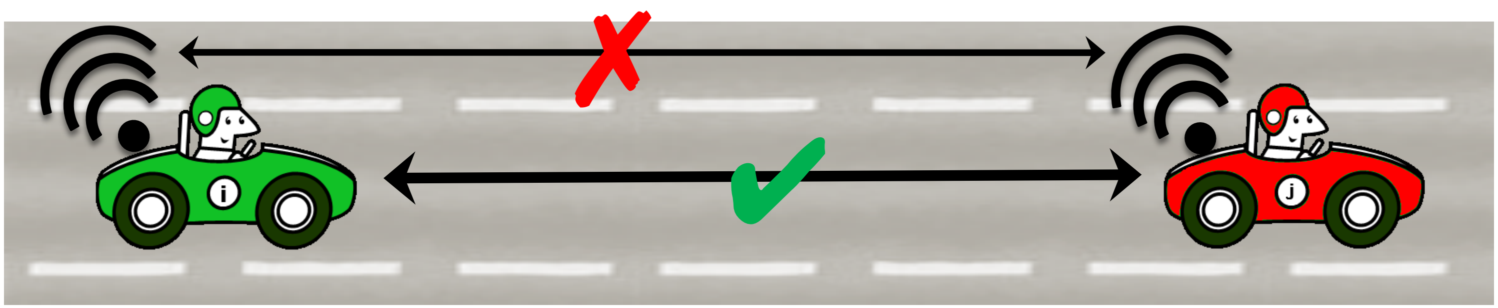


# Motivation: Adaptive Cruise Control


Low packet loss, small margin for error.

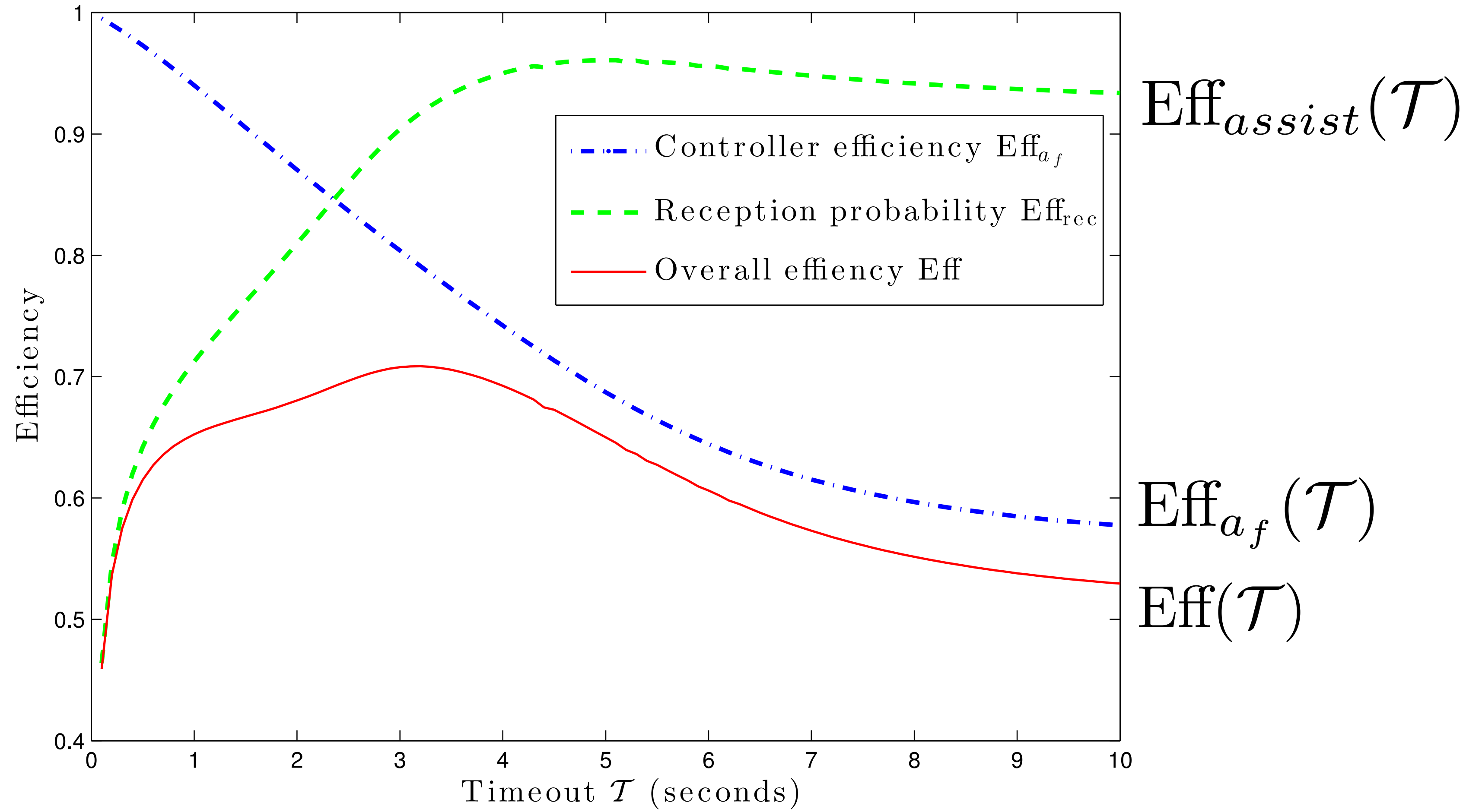
# Motivation: Adaptive Cruise Control


Low packet loss, small margin for error.




High packet loss, large margin for error.

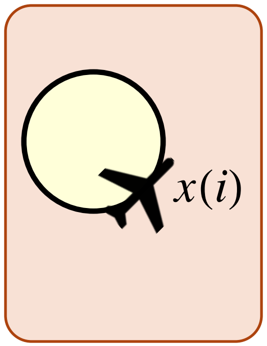
# Efficiency Analysis of ACC



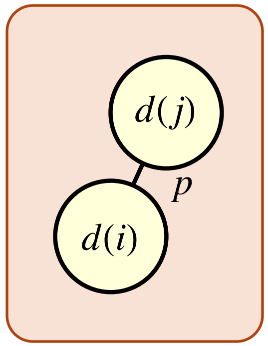
# Modular Proof for Distributed Aircraft

**To Prove:**

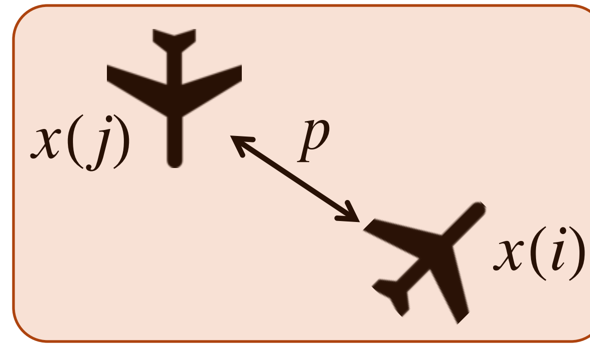
Safe separation of aircraft.




$\wedge$




$\Longrightarrow$




$$\forall i : \mathbb{A} \quad \|x(i) - d(i)\| \leq r \quad \wedge \quad \forall i \neq j : \mathbb{A} \quad \|d(i) - d(j)\| \geq 2r + p \quad \Longrightarrow \quad \forall i \neq j : \mathbb{A} \quad \|x(i) - x(j)\| \geq p$$

“How can we provide people with cyber-physical systems they can *bet their lives on*?”

-- Jeanette Wing

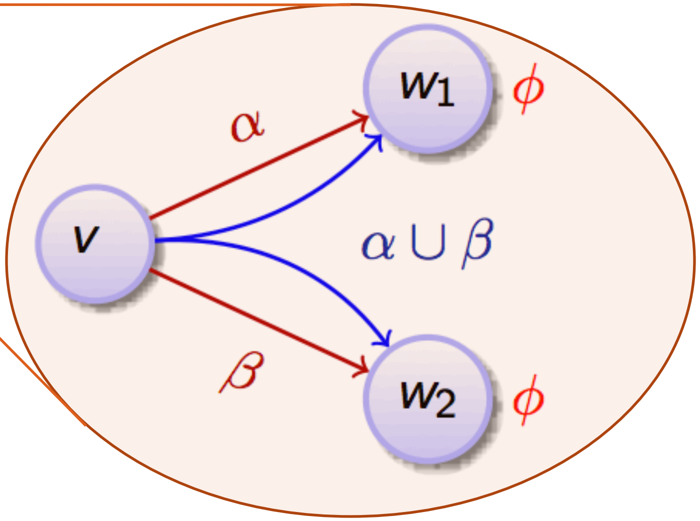
# Differential Dynamic Logic: Axiomatization

[:=] $[x := \theta]\phi(x) \leftrightarrow \phi(\theta)$

[?] $[?H]\phi \leftrightarrow (H \rightarrow \phi)$

['] $[x' = f(x)]\phi \leftrightarrow \forall t{\geq}0\, [x := y(t)]\phi \qquad (y'(t) = f(y))$

[∪] $[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$




[;] $[\alpha; \beta]\phi \leftrightarrow [\alpha][\beta]\phi$

[*] $[\alpha^*]\phi \leftrightarrow \phi \wedge [\alpha][\alpha^*]\phi$

K $[\alpha](\phi \rightarrow \psi) \rightarrow ([\alpha]\phi \rightarrow [\alpha]\psi)$

I $[\alpha^*](\phi \rightarrow [\alpha]\phi) \rightarrow (\phi \rightarrow [\alpha^*]\phi)$

[Platzer08]

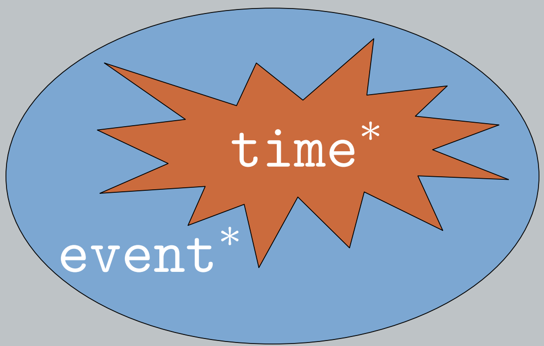
# Roadmap

## Differential Refinement Logic (dRL)

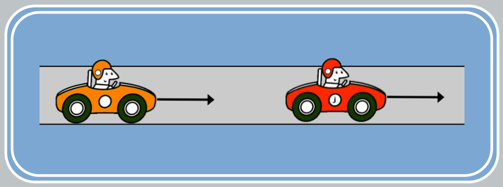
$$\alpha \leq \beta$$

- Proof rules
- Examples

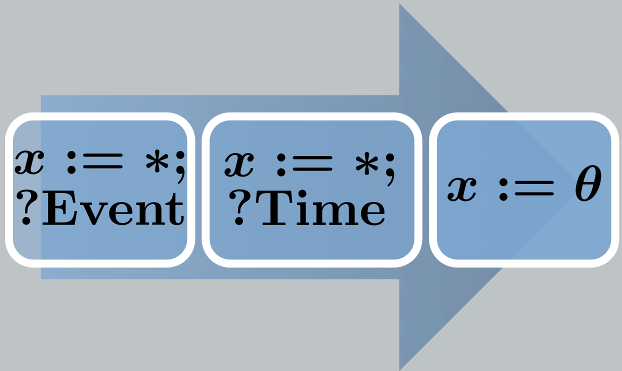
### Time-triggered vs. Event-triggered




### Verified Car Control



### Iterative System Design



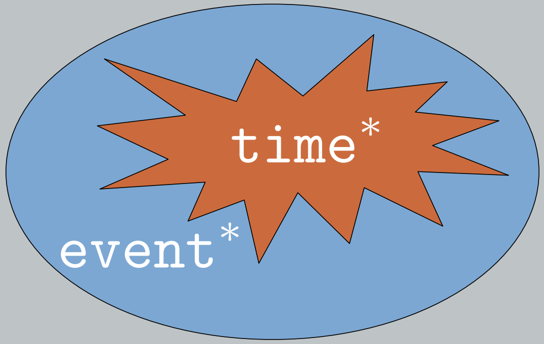
# Roadmap

## Differential Refinement Logic (dRL)

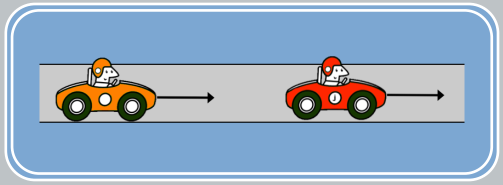
$$\alpha \leq \beta$$

- Proof rules
- Examples

### Time-triggered vs. Event-triggered




### Verified Car Control



### Iterative System Design

$x := *;$ $?\mathrm{Event}$ → $x := *;$ $?\mathrm{Time}$ → $x := \theta$

# Verifying a specific local lane controller

$$\texttt{safe}_* \equiv (?\mathbf{Safe}_\varepsilon;\ \ a_f := *;\ \ ?(-B \leq a_f \leq A))$$

# Verifying a specific local lane controller

$$\texttt{safe}_* \equiv (?\mathbf{Safe}_\varepsilon;\ a_f := *;\ ?(-B \le a_f \le A))$$

$$\texttt{safe}_\theta \equiv$$

$$a_f := K_p\left((x_l - x_f) - \left(\frac{\overline{v}^2}{2b} - \frac{\underline{v}^2}{2b} + (\frac{A}{b} + 1)(\frac{A}{2}\varepsilon^2 + \varepsilon\overline{v})\right)\right)$$

$$+ K_i(\overline{z}) + K_d(v_l - v_f)$$

# Verifying a specific local lane controller

$$\mathtt{safe}_* \equiv (?\mathbf{Safe}_\varepsilon;\ a_f := *;\ ?(-B \le a_f \le A))$$

$$\mathtt{safe}_{\boldsymbol{\theta}} \equiv$$

$$\boldsymbol{a_f := \theta}$$

# Verifying a specific local lane controller

$$\mathtt{safe}_* \equiv (?\mathbf{Safe}_\varepsilon;\ a_f := *;\ ?(-B \le a_f \le A))$$

$$\mathtt{safe}_{\boldsymbol{\theta}} \equiv \boldsymbol{a_f} := \boldsymbol{\theta}$$

# Verifying a specific local lane controller

$$\mathtt{safe}_* \equiv (?\mathbf{Safe}_\varepsilon;\ a_f := *;\ ?(-B \le a_f \le A))$$

$$-B \le \theta \le A \qquad \le \qquad (\theta > -b) \to \mathbf{Safe}_\varepsilon$$

$$\mathtt{safe}_{\boldsymbol{\theta}} \equiv \boldsymbol{a_f} := \boldsymbol{\theta}$$

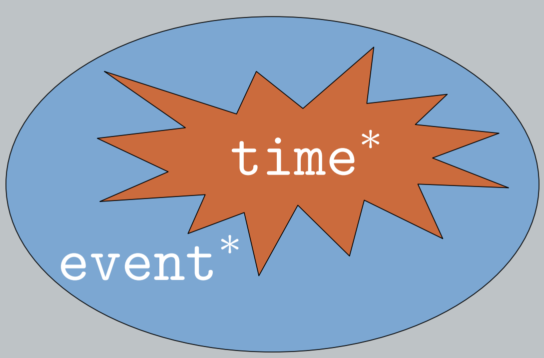
# Roadmap

## Differential Refinement Logic (dRL)

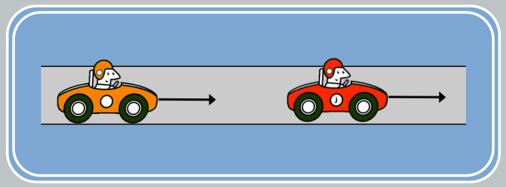
$$\boldsymbol{\alpha} \leq \boldsymbol{\beta}$$

- Proof rules
- Examples

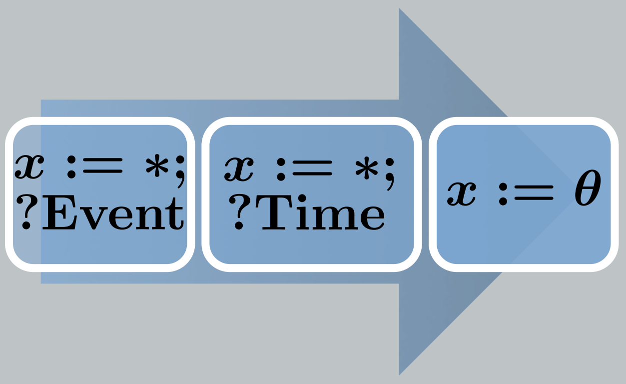
### Time-triggered vs. Event-triggered



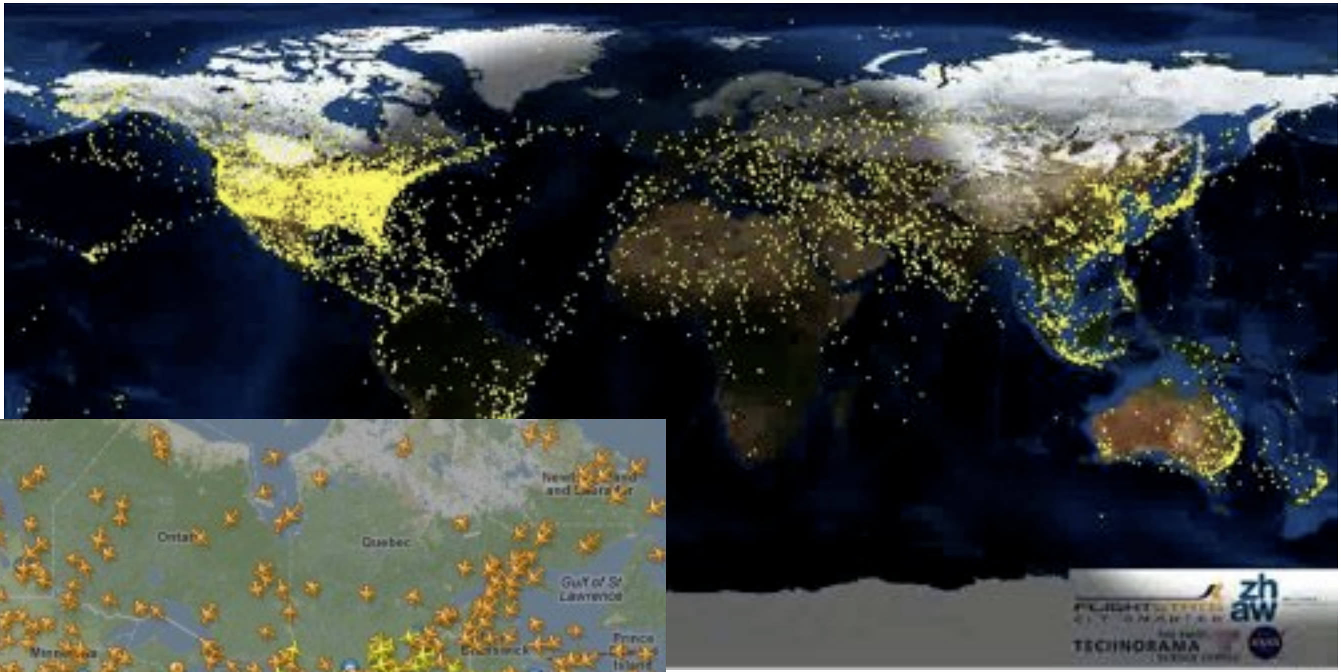

### Verified Car Control



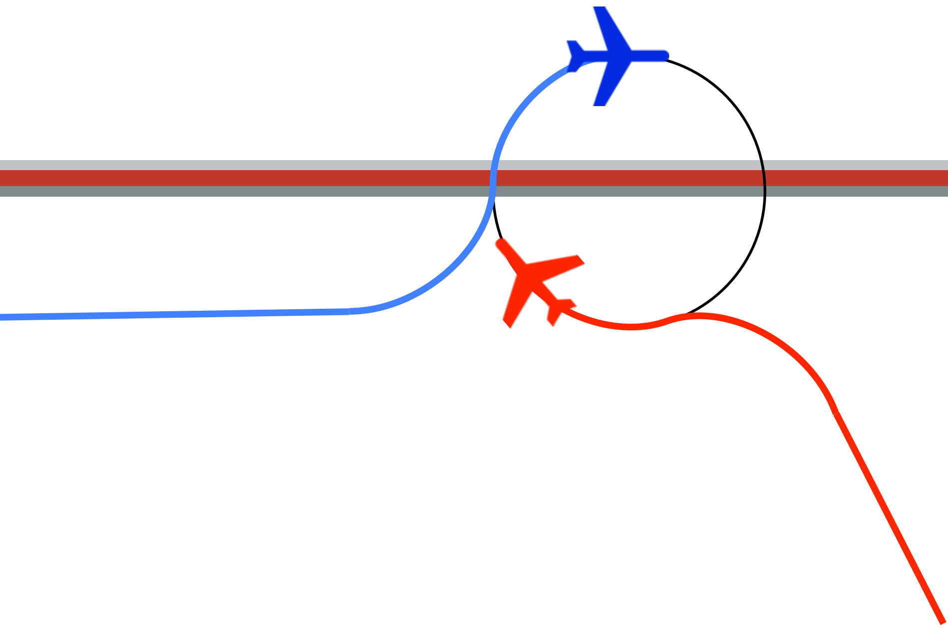
### Iterative System Design



# How Can We Prove Distributed Airspace?

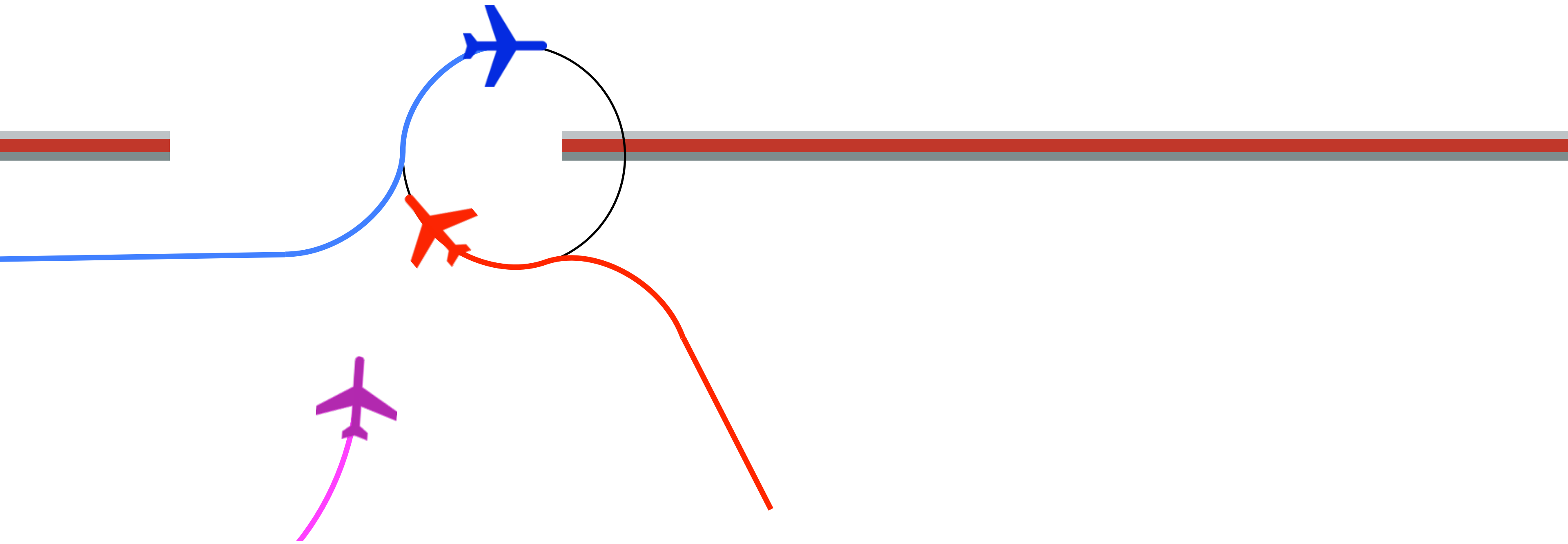


# How Can We Prove Distributed Airspace?



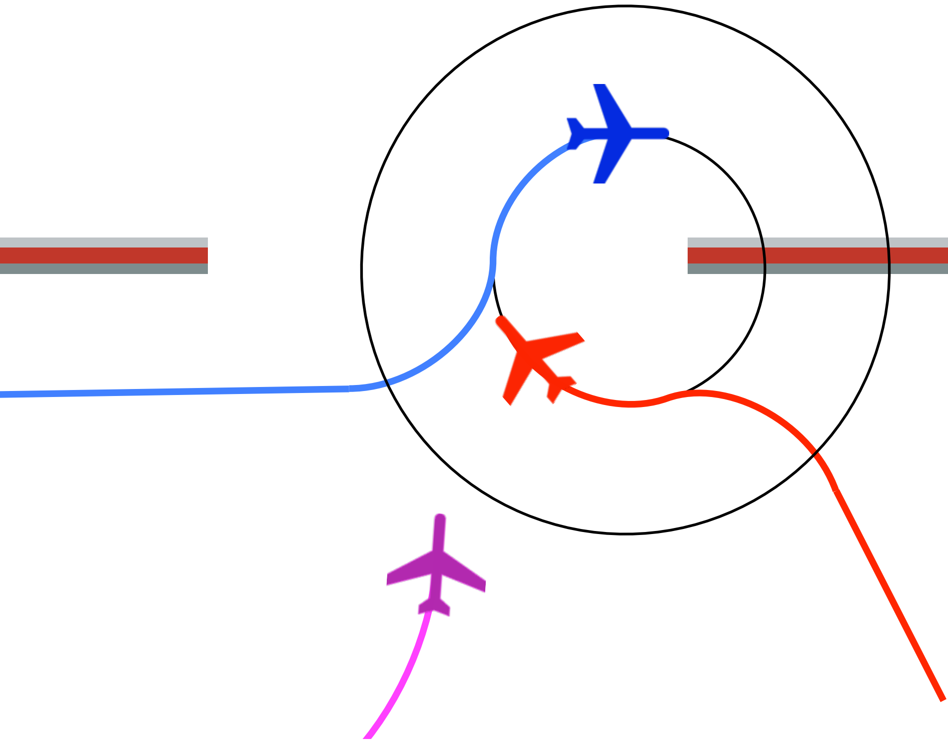
Sensor limits on aircraft are local.

# How Can We Prove Distributed Airspace?



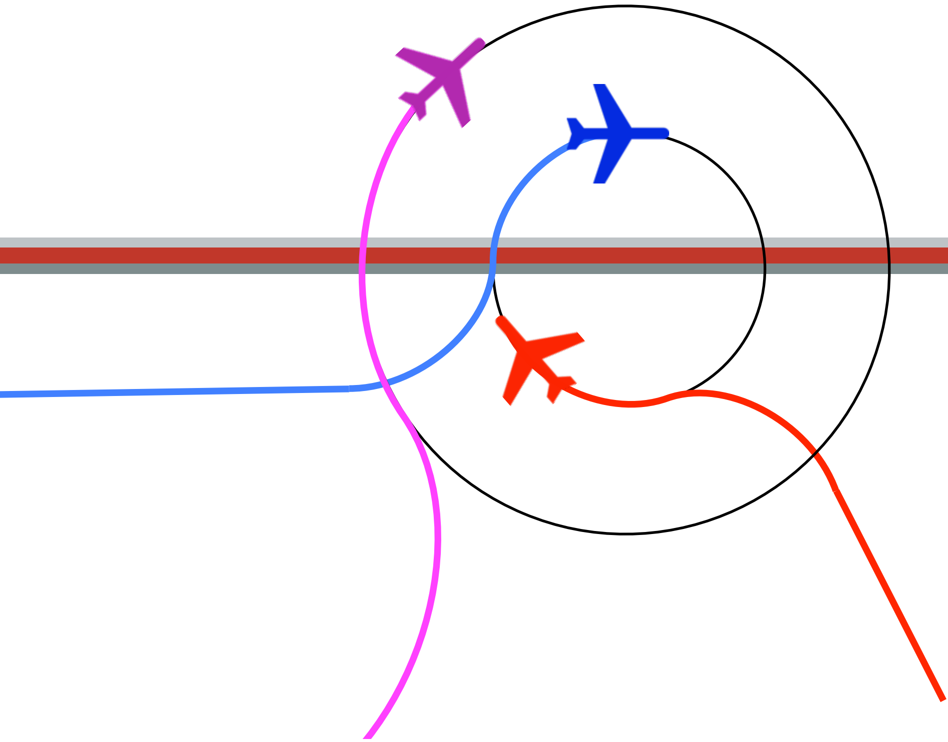
Sensor limits on aircraft are local.

# How Can We Prove Distributed Airspace?



Sensor limits on aircraft are local.

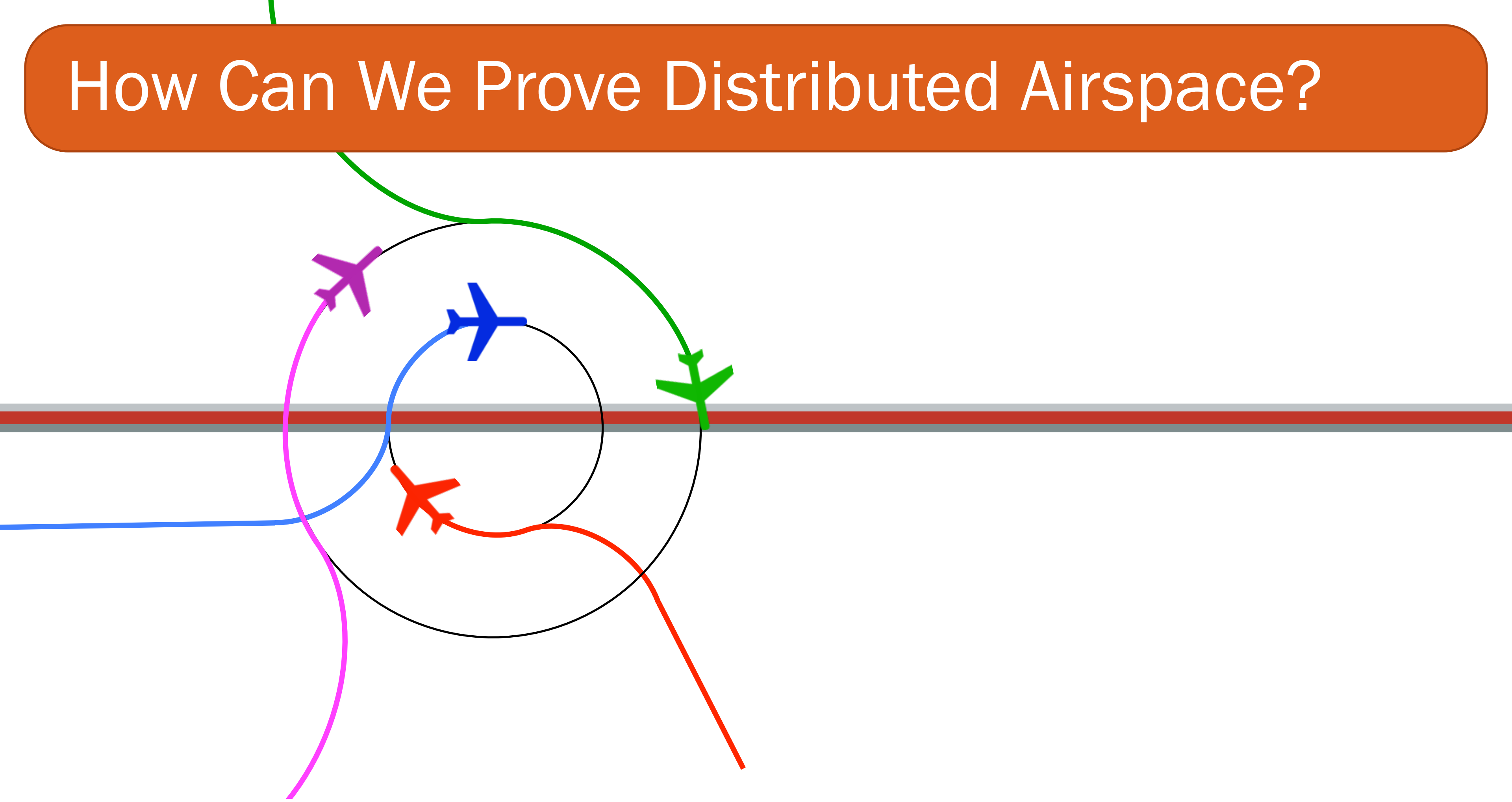
# How Can We Prove Distributed Airspace?



Sensor limits on aircraft are local.

Sometimes a maneuver may look safe locally...

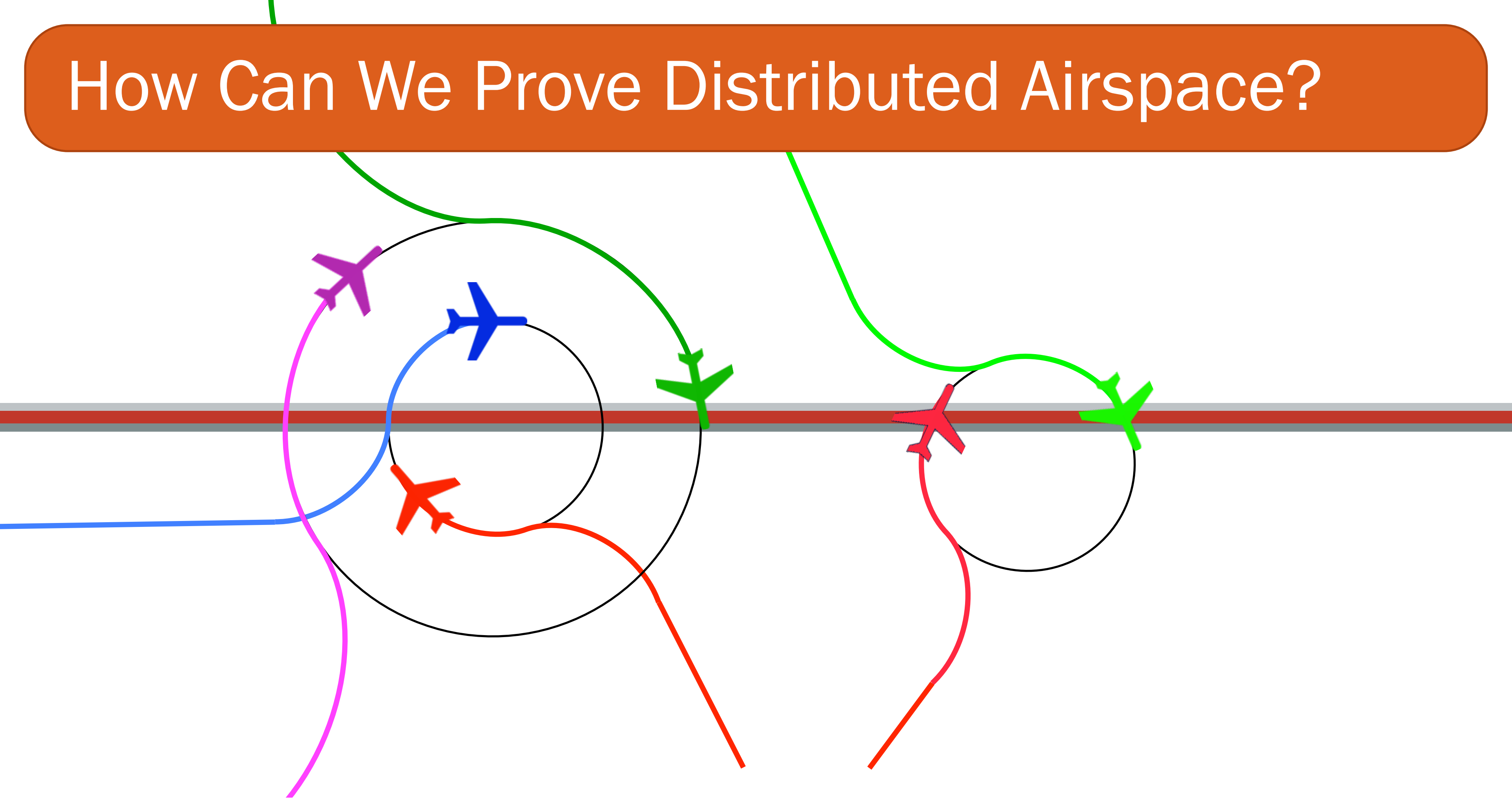
# How Can We Prove Distributed Airspace?



Sensor limits on aircraft are local.

Sometimes a maneuver may look safe locally…

# How Can We Prove Distributed Airspace?

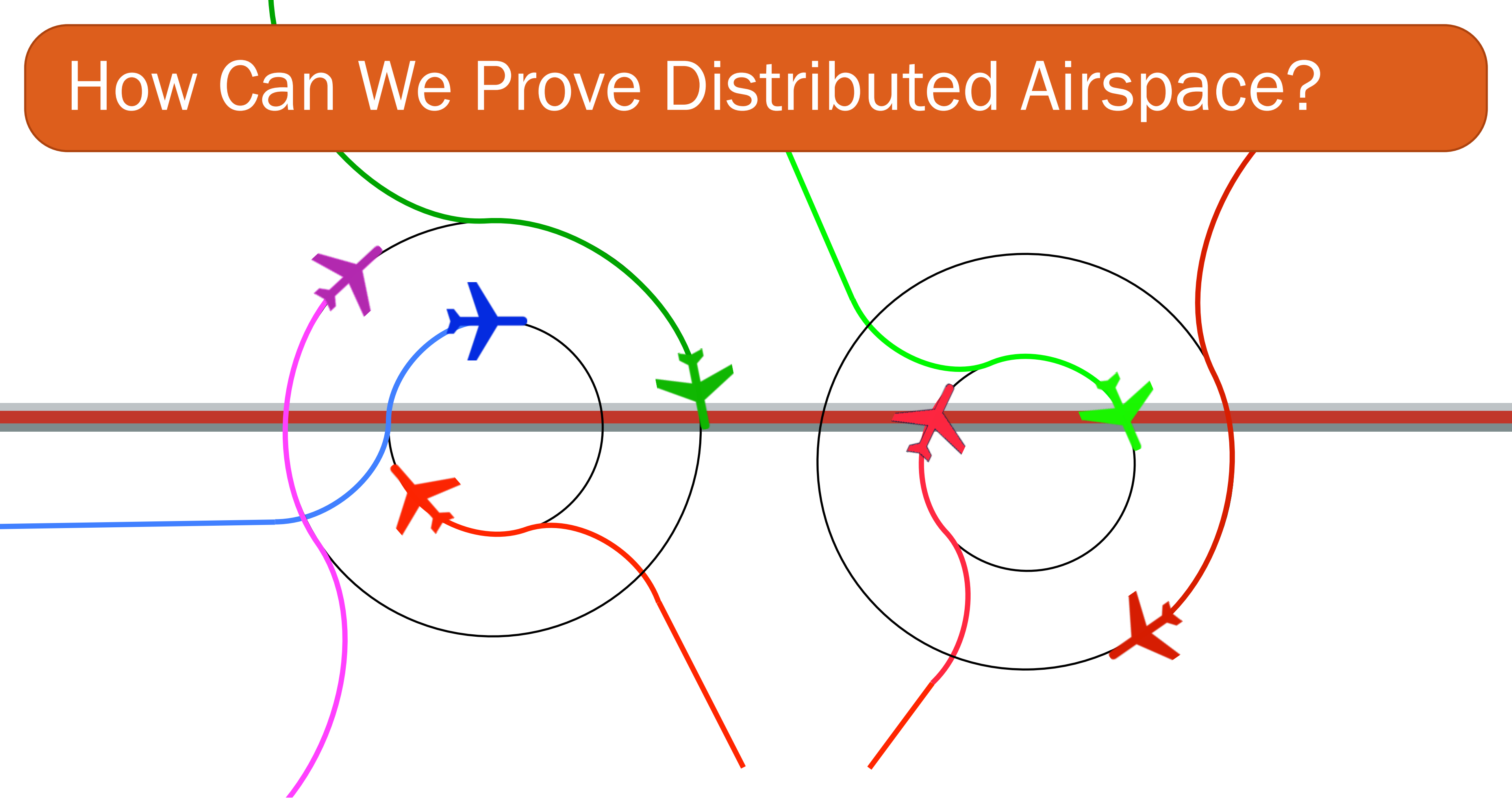


Sensor limits on aircraft are local.

Sometimes a maneuver may look safe locally…

But is a terrible idea when implemented globally.

# How Can We Prove Distributed Airspace?

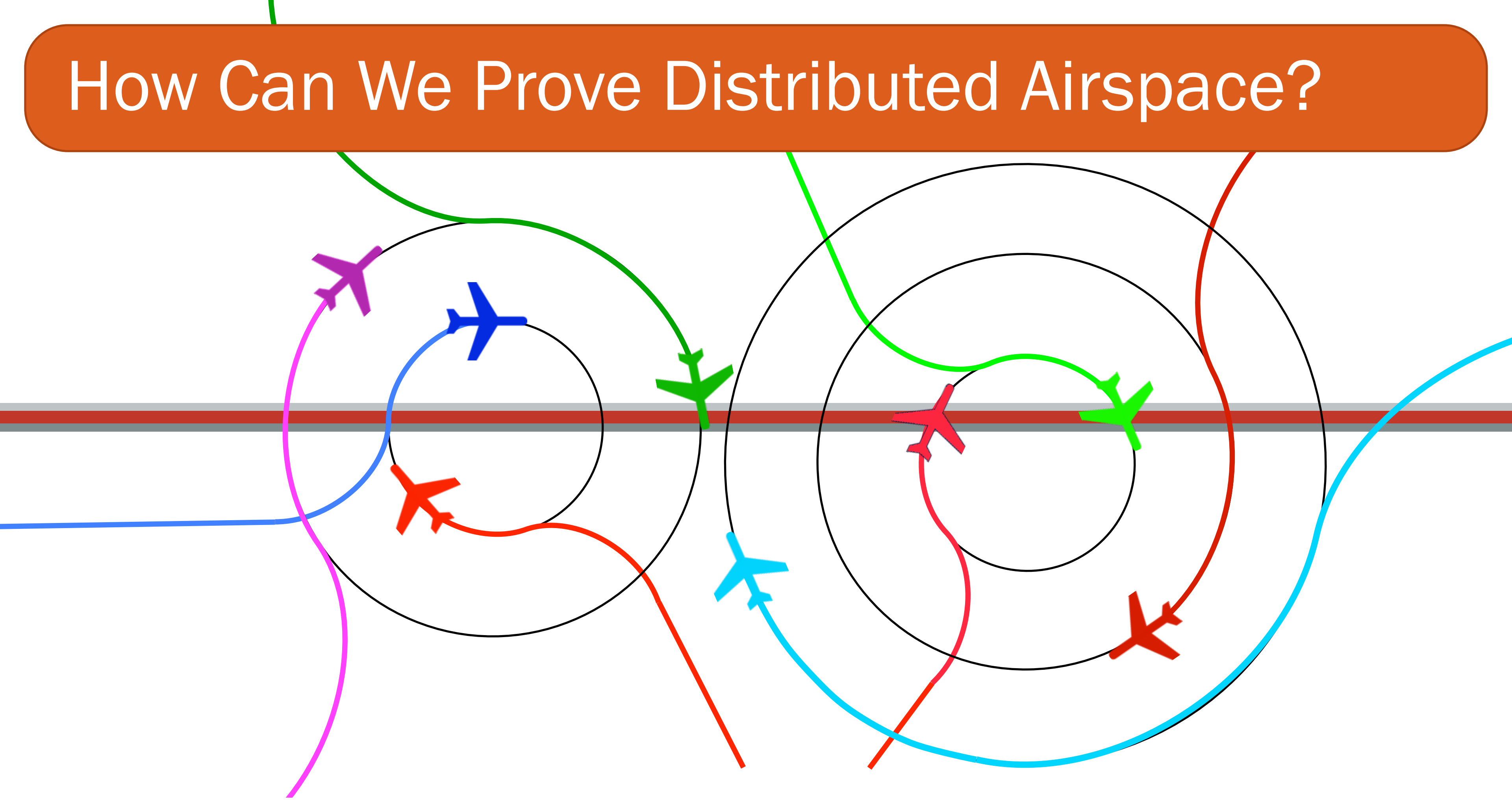


Sensor limits on aircraft are local.

Sometimes a maneuver may look safe locally…

But is a terrible idea when implemented globally.

# How Can We Prove Distributed Airspace?

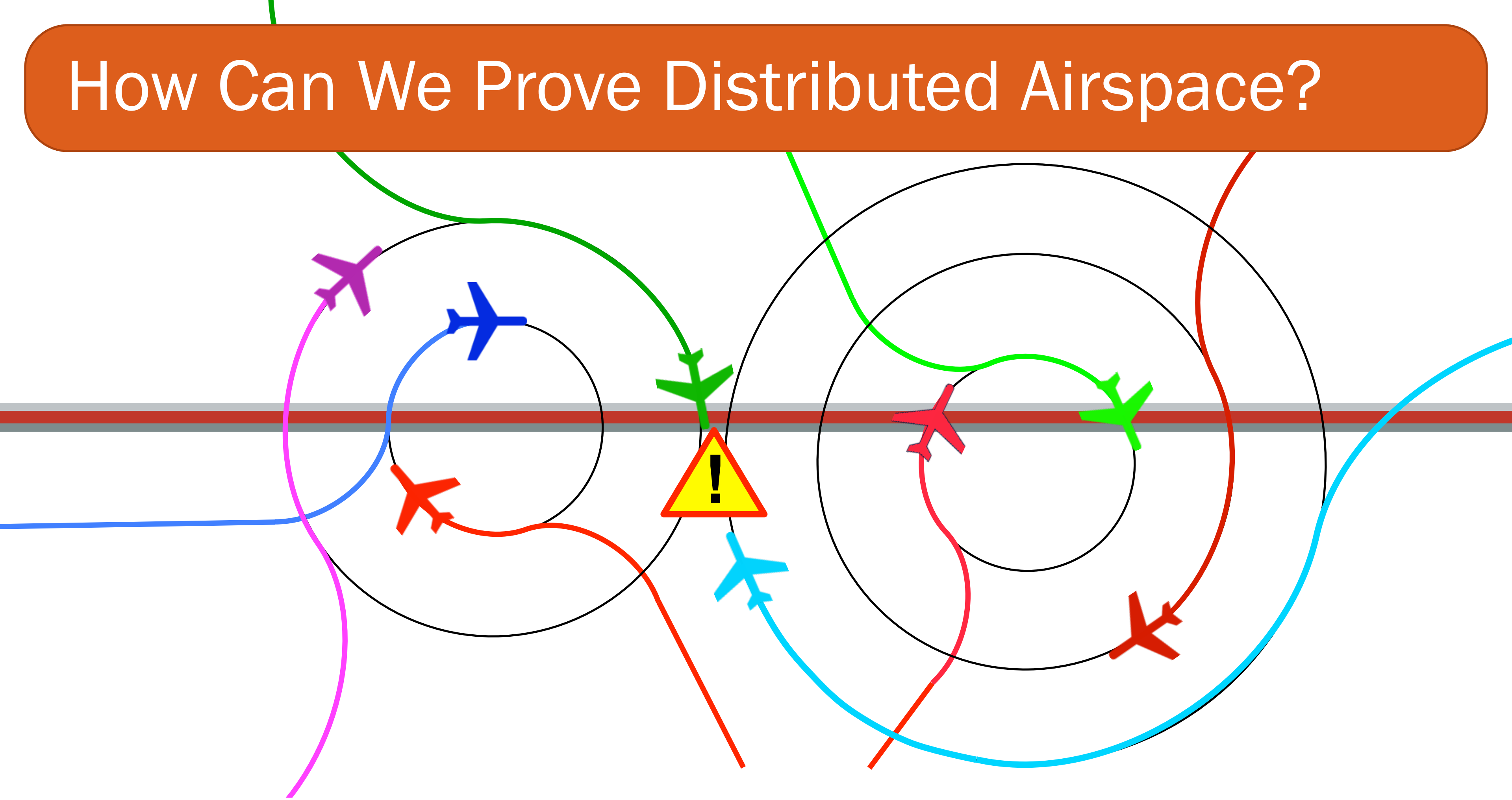


Sensor limits on aircraft are local.

Sometimes a maneuver may look safe locally…

But is a terrible idea when implemented globally.

# How Can We Prove Distributed Airspace?



Sensor limits on aircraft are local.

Sometimes a maneuver may look safe locally…

But is a terrible idea when implemented globally.

# Assumptions and Requirements

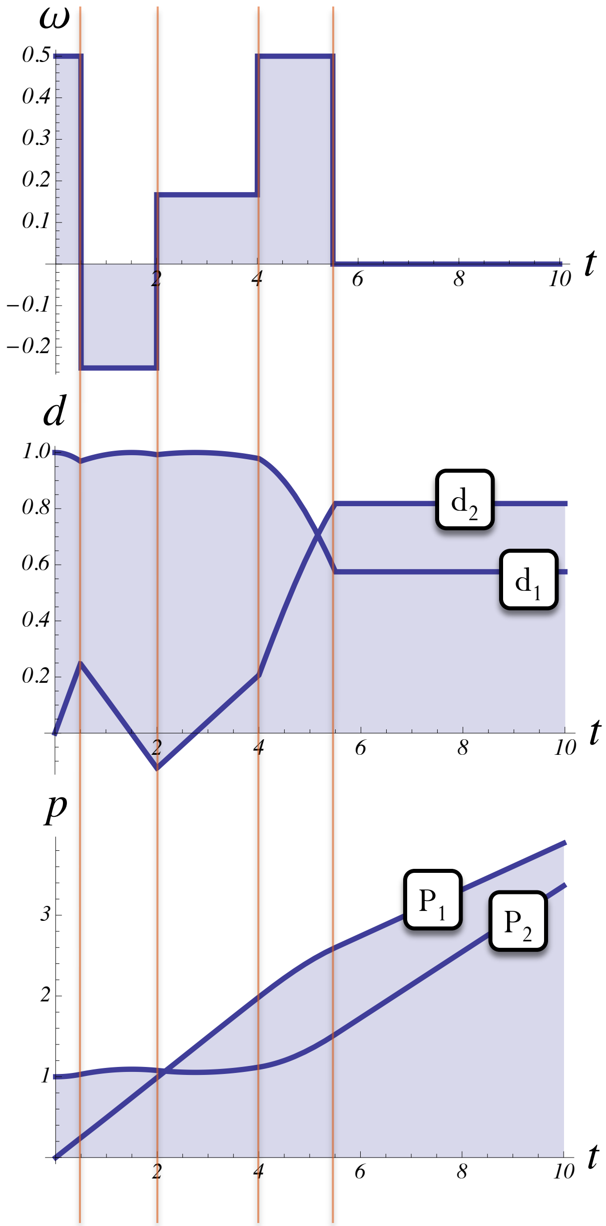
## Requirements

- **Safety**: At all times, the aircraft must be separated by distance greater than $p$.
- Aircraft trajectories must always be **flyable**.
- An **arbitrary number** of aircraft may enter the maneuver at any time.

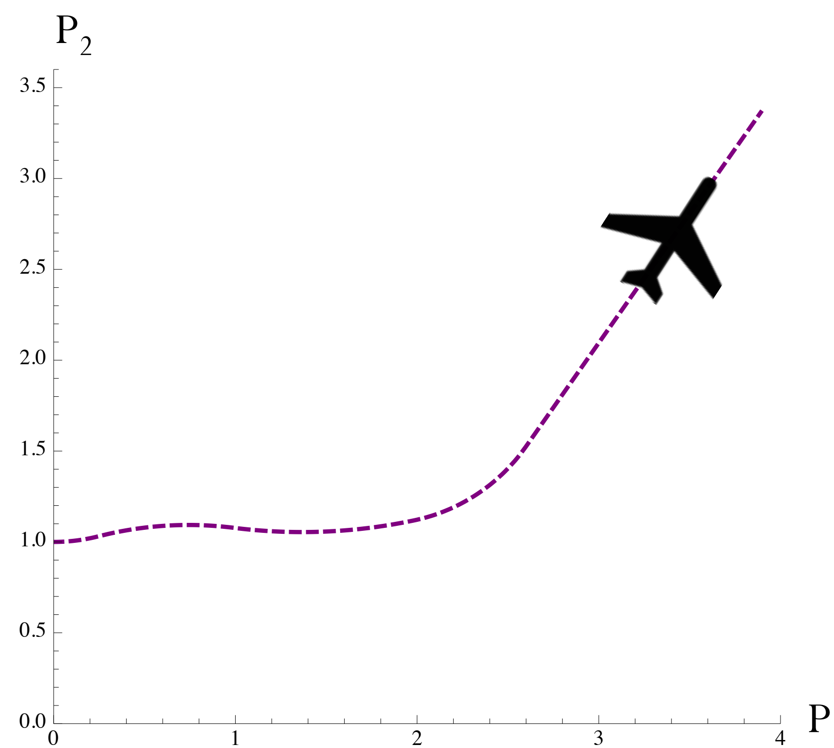
## Assumptions

- Aircraft maintain constant velocity.
- Sensors are accurate and have no delay.
- Collision avoidance maneuvers are executed on the 2D plane.

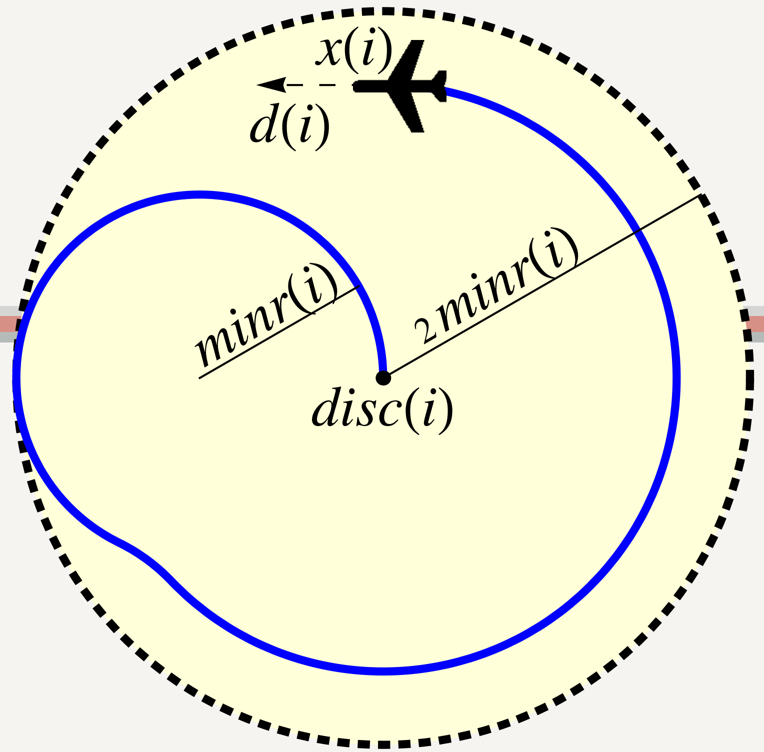
# Hybrid Dynamics




Aircraft are controlled by steering, through discrete changes in angular velocity $\omega$.



# Big Disc Control

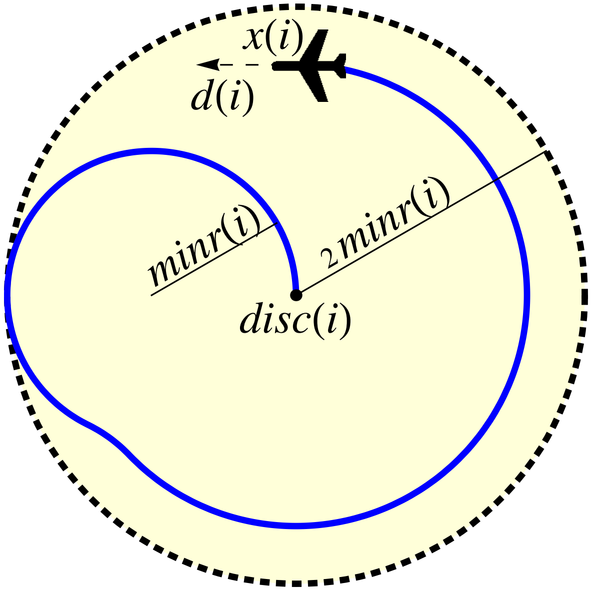



- Leaves maneuverability to pilot discretion.
- Requires large buffer disc.
- Requires aircraft to return to the center of the disc before completing avoidance maneuver.

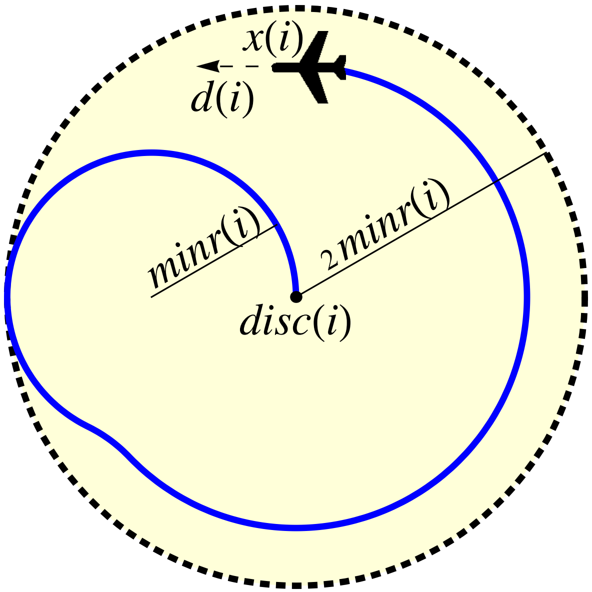
[LoosRP13]

# To Prove:

$$\mathtt{Init} \rightarrow [\mathtt{BigDisc}]\mathtt{Safe}$$



# Big Disc Control

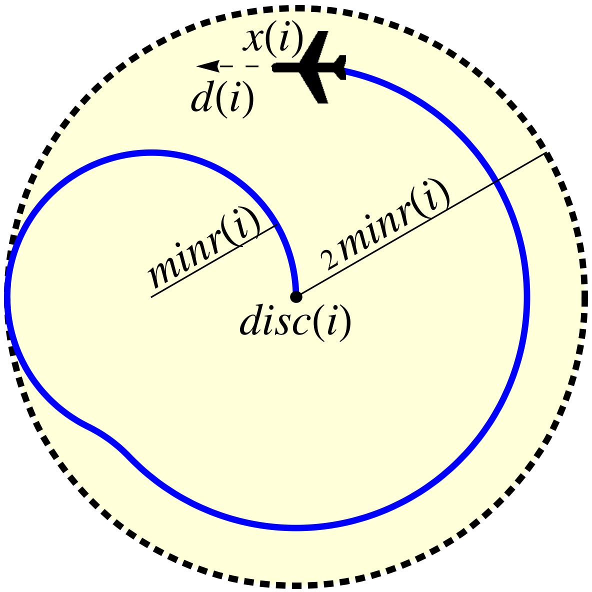



## To Prove:

$$\mathtt{Init} \rightarrow [\mathtt{BigDisc}]\mathtt{Safe}$$

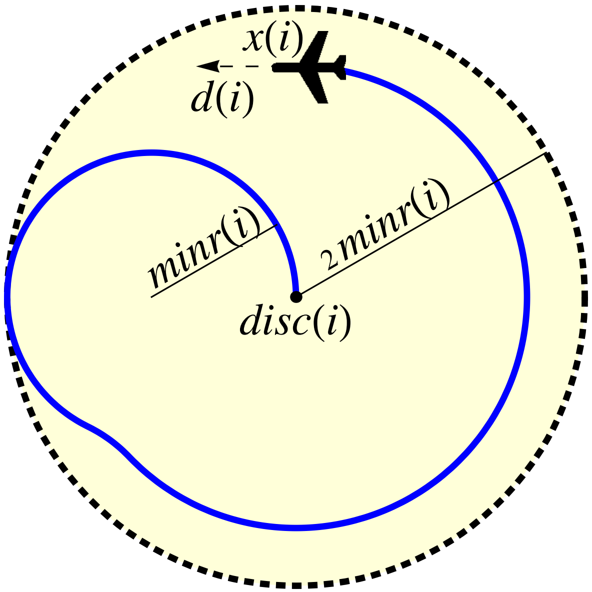
$$\mathtt{Safe} \equiv$$
$$(\forall i, j : \mathbb{A} \;\; i \neq j \rightarrow$$
$$\|x(i) - x(j)\| \geq p)$$

# Big Disc Control $\quad \mathtt{Init} \rightarrow [\mathtt{BigDisc}]\mathtt{Safe}$




$$
\begin{aligned}
\mathtt{BigDisc} &\equiv (\mathtt{Control} \cup \mathtt{Plant})^* \\
\mathtt{Control} &\equiv k := *_{\mathbb{A}};\ (\mathtt{CA} \cup \mathtt{NotCA}) \\
\mathtt{CA} &\equiv ?(ca(k) = 1);\ (\mathtt{Steer} \cup \mathtt{Exit}) \\
\mathtt{NotCA} &\equiv ?(ca(k) = 0);\ (\mathtt{Steer} \cup \mathtt{Flip} \cup \mathtt{Enter}) \\
\mathtt{Steer} &\equiv \omega(k) := *_{\mathbb{R}};\ ?(-\Omega(k) \leq \omega(k) \leq \Omega(k)) \\
\mathtt{Exit} &\equiv ?(disc(k) = x(k));\ ca(k) := 0 \\
\mathtt{Enter} &\equiv \omega(k) := side(k) \cdot \Omega(k);\ ca(k) := 1 \\
\mathtt{Flip} &\equiv side(k) := -side(k) \\
\mathtt{Plant} &\equiv \forall i : \mathbb{A} \Big( x(i)' = v(i) \cdot d(i),\ d(i)' = \omega(i) \cdot d(i)^{\perp}, \\
&\qquad disc(i)' = (1 - ca(i)) \cdot v(i) \cdot d(i)\ \&\ \mathtt{EvDom} \Big) \\
\mathtt{EvDom} &\equiv \forall j : \mathbb{A} \\
&\quad ((j \neq i \land (ca(i) = 0 \lor ca(j) = 0)) \rightarrow \mathsf{Sep}(i, j) \\
&\quad \land \|disc(i) - (x(i) + minr(i) \cdot side(i) \cdot d(i)^{\perp})\| \\
&\qquad \leq minr(i)) \\
\mathsf{Sep}(i, j) &\equiv \|disc(i) - disc(j)\| \geq 2minr(i) + 2minr(j) + p
\end{aligned}
$$

# Big Disc Control $\mathtt{Init} \to [\mathtt{BigDisc}]\mathtt{Safe}$



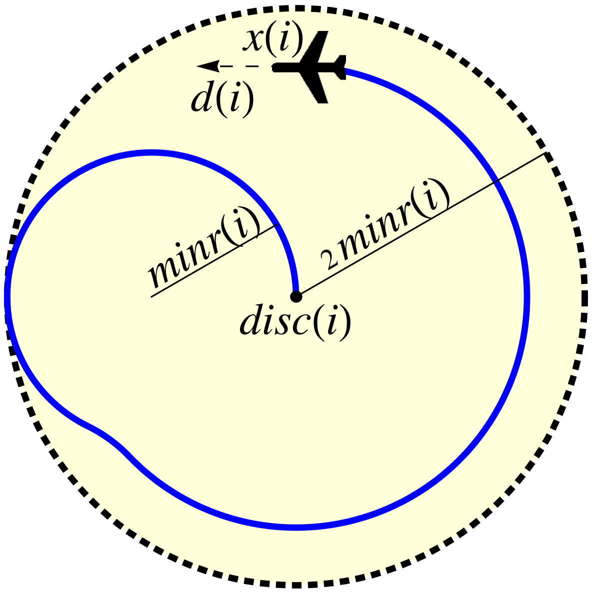

$$\mathtt{Plant} \equiv \forall i : \mathbb{A} \left( \boxed{x(i)' = v(i) \cdot d(i),\ d(i)' = \omega(i) \cdot d(i)^{\perp},} \right.$$
$$\left. disc(i)' = (1 - ca(i)) \cdot v(i) \cdot d(i)\ \&\ \mathtt{EvDom} \right)$$

Dubins Model
for 2D motion

[Dubins57]

# Big Disc Control

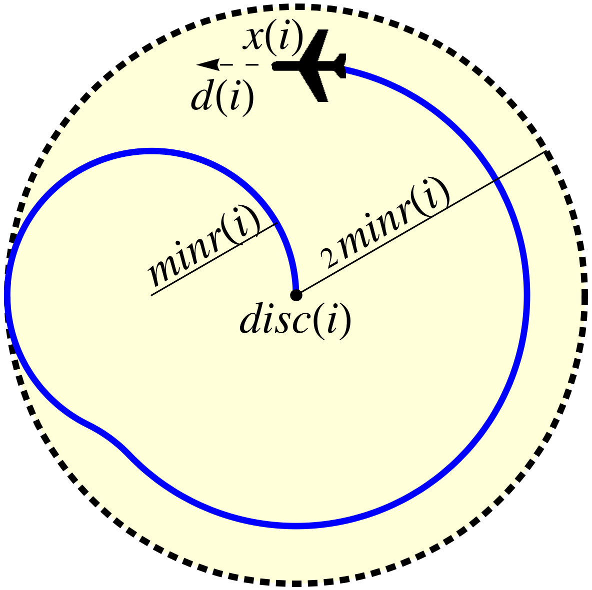
$\mathtt{Init} \to [\mathtt{BigDisc}]\mathtt{Safe}$




$$\mathtt{Plant} \equiv \forall i : \mathbb{A}\Big(x(i)' = v(i)\cdot d(i),\ d(i)' = \omega(i)\cdot d(i)^{\perp},$$
$$\boxed{disc(i)' = (1 - ca(i))\cdot v(i)\cdot d(i)}\ \&\ \mathtt{EvDom}\Big)$$

The disc does not move when in a collision avoidance maneuver

# Big Disc Control $\texttt{Init} \rightarrow [\texttt{BigDisc}]\texttt{Safe}$



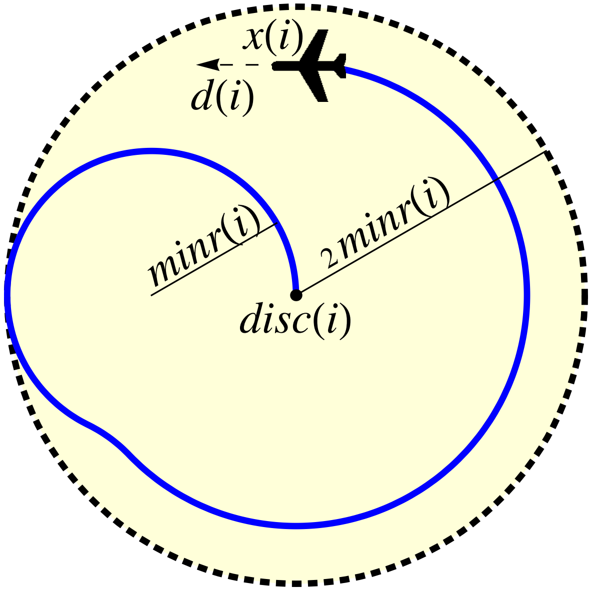

$$\texttt{Plant} \equiv \boxed{\forall i : \mathbb{A}} \Big( x(i)' = v(i) \cdot d(i),\ d(i)' = \omega(i) \cdot d(i)^{\perp},\ disc(i)' = (1 - ca(i)) \cdot v(i) \cdot d(i)\ \&\ \texttt{EvDom} \Big)$$

All aircraft evolve simultaneously

# Big Disc Control

$\text{Init} \rightarrow [\text{BigDisc}]\text{Safe}$

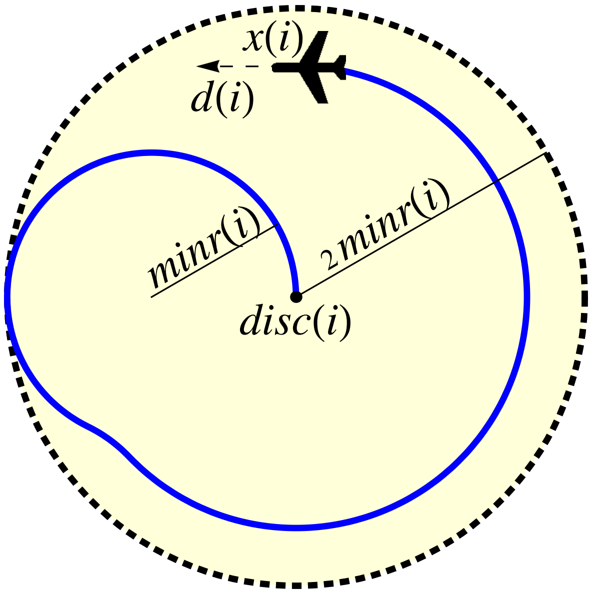
$\text{BigDisc} \equiv (\text{Control} \cup \text{Plant})^*$




$$\text{Plant} \equiv \forall i : \mathbb{A}\Big(x(i)' = v(i) \cdot d(i),\ d(i)' = \omega(i) \cdot d(i)^{\perp},$$
$$disc(i)' = (1 - ca(i)) \cdot v(i) \cdot d(i)\ \&\ \text{EvDom}\Big)$$

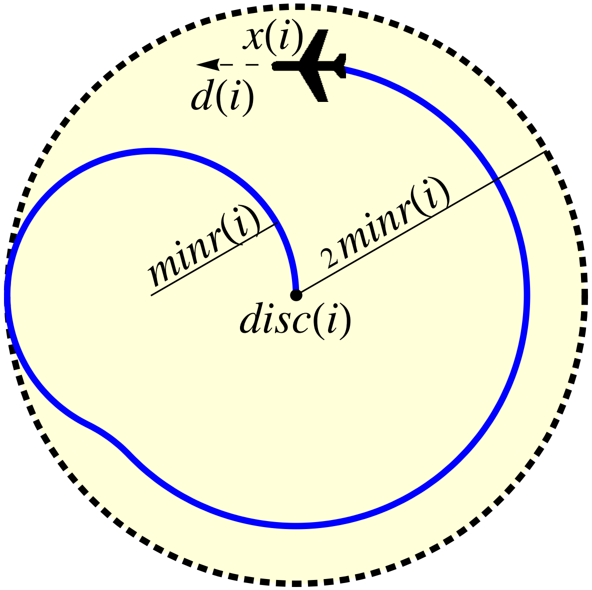
# Big Disc Control $\texttt{Init} \rightarrow [\texttt{BigDisc}]\texttt{Safe}$

$$\begin{aligned}
\texttt{BigDisc} &\equiv (\texttt{Control} \cup \texttt{Plant})^* \\
\texttt{Control} &\equiv \boxed{k := *_{\mathbb{A}};}\ (\texttt{CA} \cup \texttt{NotCA}) \\
\texttt{CA} &\equiv ?(ca(k) = 1);\ (\texttt{Steer} \cup \texttt{Exit}) \\
\texttt{NotCA} &\equiv ?(ca(k) = 0);\ (\texttt{Steer} \cup \texttt{Flip} \cup \texttt{Enter}) \\
\texttt{Steer} &\equiv \omega(k) := *_{\mathbb{R}};\ ?(-\Omega(k) \leq \omega(k) \leq \Omega(k)) \\
\texttt{Exit} &\equiv ?(disc(k) = x(k));\ ca(k) := 0 \\
\texttt{Enter} &\equiv \omega(k) := side(k) \cdot \Omega(k);\ ca(k) := 1 \\
\texttt{Flip} &\equiv side(k) := -side(k) \\
\texttt{Plant} &\equiv \forall i : \mathbb{A} \Big( x(i)' = v(i) \cdot d(i),\ d(i)' = \omega(i) \cdot d(i)^{\perp}, \\
&\qquad disc(i)' = (1 - ca(i)) \cdot v(i) \cdot d(i)\ \&\ \texttt{EvDom} \Big)
\end{aligned}$$



# Big Disc Control $\mathtt{Init} \rightarrow [\mathtt{BigDisc}]\mathtt{Safe}$

$$\mathtt{BigDisc} \equiv (\mathtt{Control} \cup \mathtt{Plant})^*$$
$$\mathtt{Control} \equiv k := *_{\mathbb{A}};\ (\mathtt{CA} \cup \mathtt{NotCA})$$
$$\mathtt{CA} \equiv ?(ca(k) = 1);\ (\mathtt{Steer} \cup \mathtt{Exit})$$
$$\mathtt{NotCA} \equiv ?(ca(k) = 0);\ (\mathtt{Steer} \cup \mathtt{Flip} \cup \mathtt{Enter})$$
$$\mathtt{Steer} \equiv \omega(k) := *_{\mathbb{R}};\ ?(-\Omega(k) \leq \omega(k) \leq \Omega(k))$$
$$\mathtt{Exit} \equiv ?(disc(k) = x(k));\ ca(k) := 0$$
$$\mathtt{Enter} \equiv \omega(k) := side(k) \cdot \Omega(k);\ ca(k) := 1$$
$$\mathtt{Flip} \equiv side(k) := -side(k)$$
$$\mathtt{Plant} \equiv \forall i : \mathbb{A}\ \Big(x(i)' = v(i) \cdot d(i),\ d(i)' = \omega(i) \cdot d(i)^{\perp},\ disc(i)' = (1 - ca(i)) \cdot v(i) \cdot d(i)\ \&\ \boxed{\mathtt{EvDom}}\Big)$$
$$\mathtt{EvDom} \equiv \forall j : \mathbb{A}\ ((j \neq i \land (ca(i) = 0 \lor ca(j) = 0)) \rightarrow \mathsf{Sep}(i, j) \land \|disc(i) - (x(i) + minr(i) \cdot side(i) \cdot d(i)^{\perp})\| \leq minr(i))$$
$$\mathsf{Sep}(i, j) \equiv \|disc(i) - disc(j)\| \geq 2minr(i) + 2minr(j) + p$$




-Ensures aircraft control can engage CA maneuver.

- Aircraft can flyably remain within disc

# Big Disc Control $\texttt{Init} \to [\texttt{BigDisc}]\texttt{Safe}$

$$\texttt{BigDisc} \equiv (\texttt{Control} \cup \texttt{Plant})^*$$

$$\texttt{Control} \equiv k := *_{\mathbb{A}};\ (\texttt{CA} \cup \texttt{NotCA})$$

$$\texttt{CA} \equiv ?(ca(k) = 1);\ (\texttt{Steer} \cup \texttt{Exit})$$

$$\texttt{NotCA} \equiv ?(ca(k) = 0);\ (\texttt{Steer} \cup \texttt{Flip} \cup \texttt{Enter})$$

$$\texttt{Steer} \equiv \omega(k) := *_{\mathbb{R}};\ ?(-\Omega(k) \leq \omega(k) \leq \Omega(k))$$

$$\texttt{Exit} \equiv ?(disc(k) = x(k));\ ca(k) := 0$$

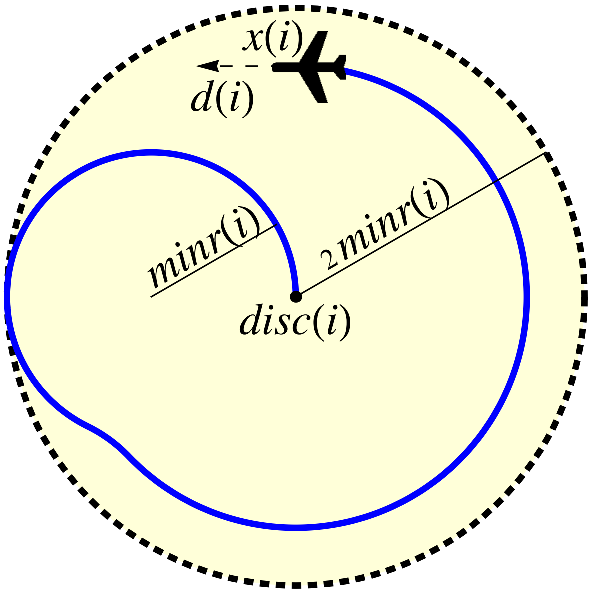
$$\texttt{Enter} \equiv \omega(k) := side(k) \cdot \Omega(k);\ ca(k) := 1$$

$$\texttt{Flip} \equiv side(k) := -side(k)$$

$$\texttt{Plant} \equiv \forall i : \mathbb{A} \Big( x(i)' = v(i) \cdot d(i),\ d(i)' = \omega(i) \cdot d(i)^{\perp},\ disc(i)' = (1 - ca(i)) \cdot v(i) \cdot d(i)\ \&\ \texttt{EvDom} \Big)$$

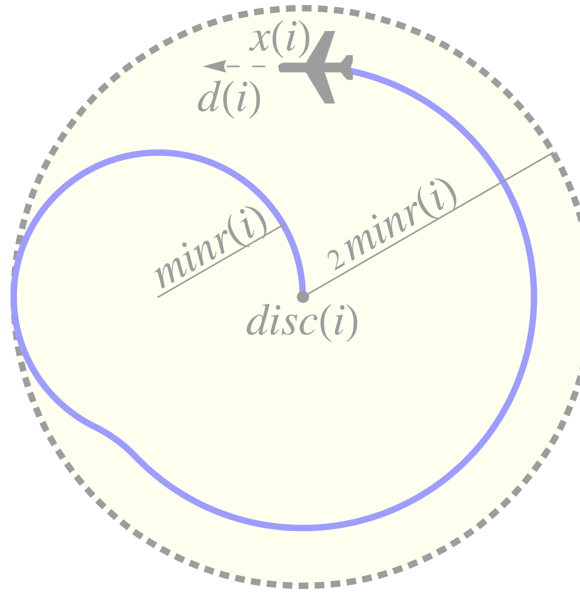
$$\texttt{EvDom} \equiv \forall j : \mathbb{A}\ \big((j \neq i \land (ca(i) = 0 \lor ca(j) = 0)) \to \mathsf{Sep}(i, j)\ \land \|disc(i) - (x(i) + minr(i) \cdot side(i) \cdot d(i)^{\perp})\| \leq minr(i)\big)$$

$$\mathsf{Sep}(i, j) \equiv \|disc(i) - disc(j)\| \geq 2minr(i) + 2minr(j) + p$$



# Big Disc Control

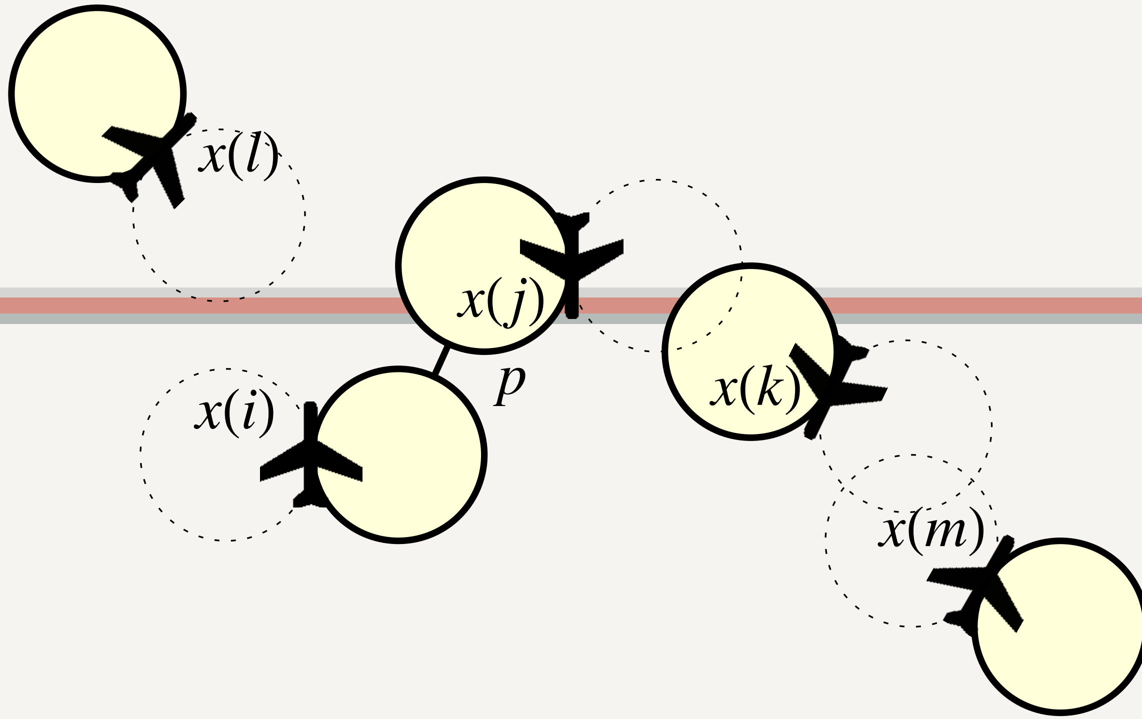
$\mathtt{Init} \rightarrow [\mathtt{BigDisc}]\mathtt{Safe}$




$$
\begin{aligned}
\mathtt{BigDisc} &\equiv (\mathtt{Control} \cup \mathtt{Plant})^* \\
\mathtt{Control} &\equiv k := *_{\mathbb{A}};\ (\mathtt{CA} \cup \mathtt{NotCA}) \\
\mathtt{CA} &\equiv ?(ca(k) = 1);\ (\mathtt{Steer} \cup \mathtt{Exit}) \\
\mathtt{NotCA} &\equiv ?(ca(k) = 0);\ (\mathtt{Steer} \cup \mathtt{Flip} \cup \mathtt{Enter}) \\
\mathtt{Steer} &\equiv \omega(k) := *_{\mathbb{R}};\ ?(-\Omega(k) \le \omega(k) \le \Omega(k)) \\
\mathtt{Exit} &\equiv ?(disc(k) = x(k));\ ca(k) := 0 \\
\mathtt{Enter} &\equiv \omega(k) := side(k) \cdot \Omega(k);\ ca(k) := 1 \\
\mathtt{Flip} &\equiv side(k) := -side(k) \\
\mathtt{Plant} &\equiv \forall i : \mathbb{A}\ \big(x(i)' = v(i) \cdot d(i),\ d(i)' = \omega(i) \cdot d(i)^{\perp}, \\
&\qquad disc(i)' = (1 - ca(i)) \cdot v(i) \cdot d(i)\ \&\ \mathtt{EvDom}\big) \\
\mathtt{EvDom} &\equiv \forall j : \mathbb{A} \\
&\quad ((j \neq i \wedge (ca(i) = 0 \vee ca(j) = 0)) \rightarrow \mathsf{Sep}(i, j) \\
&\qquad \wedge \|disc(i) - (x(i) + minr(i) \cdot side(i) \cdot d(i)^{\perp})\| \\
&\qquad\qquad \le minr(i)) \\
\mathsf{Sep}(i, j) &\equiv \|disc(i) - disc(j)\| \ge 2minr(i) + 2minr(j) + p
\end{aligned}
$$

**✔ Verified in KeYmaeraD**

# Small Discs Control




- Deterministic control makes it well suited for UAVs.
- Smaller discs allow aircraft to fly closer together.
- Aircraft may exit maneuver as soon as it is safe to do so.

[PallottinoSBF07, LoosRP13]

# Small Discs Control

$$\texttt{SmallDiscs} \equiv (\texttt{Control} \cup \texttt{Plant})^*$$

$$\texttt{Control} \equiv k := *_{\mathbb{A}};\ (\texttt{CA} \cup \texttt{NotCA})$$

$$\texttt{CA} \equiv ?(ca(k) = 1);\ (\texttt{Exit} \cup \texttt{Skip})$$

$$\texttt{NotCA} \equiv ?(ca(k) = 0);\ (\texttt{Steer} \cup \texttt{Flip} \cup \texttt{Enter})$$

$$\texttt{Skip} \equiv ?true$$

$$\texttt{Steer} \equiv \omega(k) := *_{\mathbb{R}};\ ?(-\Omega(k) \le \omega(k) \le \Omega(k))$$

$$\texttt{Exit} \equiv ca(k) := 0$$

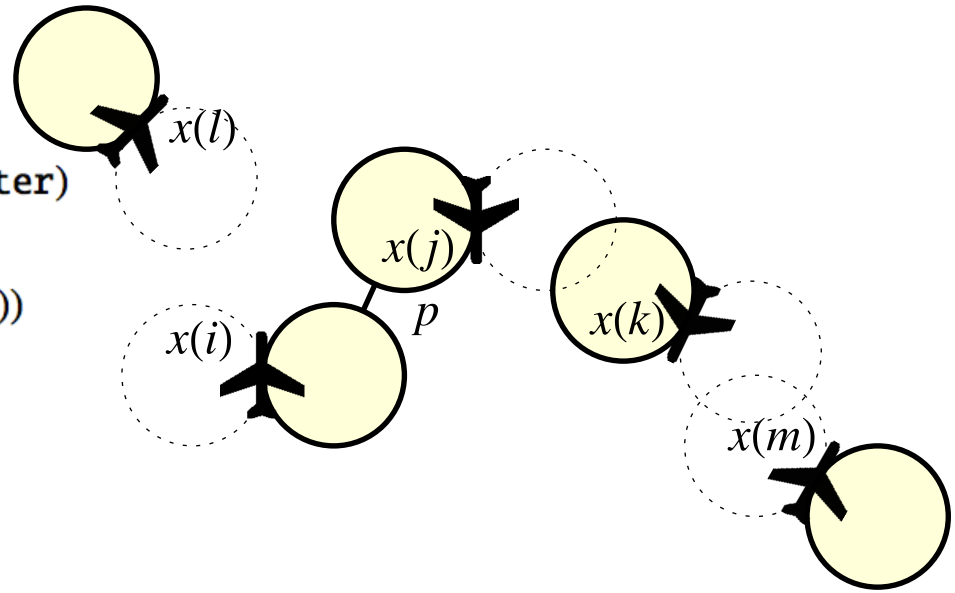
$$\texttt{Enter} \equiv (\omega(k) := side(k) \cdot \Omega(k));\ ca(k) := 1$$

$$\texttt{Flip} \equiv ?(\forall j : \mathbb{A}\ (j \ne k \to \ \mathsf{FlipSep}(j,k)));\ side(k) := -side(k)$$

$$\mathsf{FlipSep}(i,j) \equiv \|(x(i) + minr(i) \cdot side(i) \cdot d(i)^{\perp}) - (x(j) - minr(j) \cdot side(j) \cdot d(j)^{\perp})\| \ge minr(i) + minr(j) + p$$

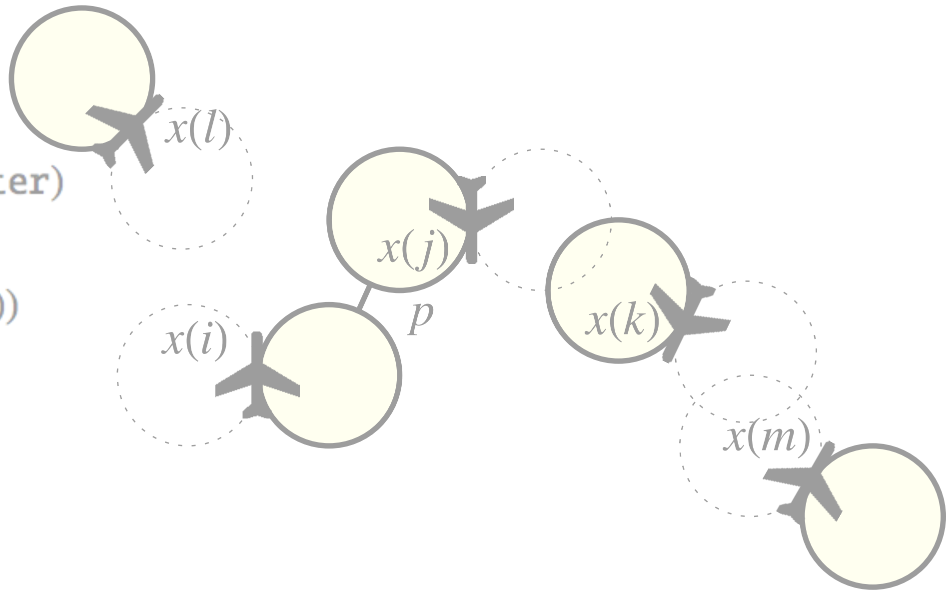
$$\texttt{Plant} \equiv \forall i : \mathbb{A}\ \Big(x(i)' = v(i) \cdot d(i),\ d(i)' = \omega(i) d(i)^{\perp}\ \&\ \forall j : \mathbb{A}\ ((j \ne i \land (ca(i) = 0 \lor ca(j) = 0)) \to \mathsf{Sep}(i,j))\Big)$$

$$\mathsf{Sep}(i,j) \equiv \|(x(i) + minr(i) \cdot side(i) \cdot d(i)^{\perp}) - (x(j) + minr(j) \cdot side(j) \cdot d(j)^{\perp})\| \ge minr(i) + minr(j) + p$$



# Small Discs Control

$$
\begin{aligned}
\texttt{SmallDiscs} &\equiv (\texttt{Control} \cup \texttt{Plant})^* \\
\texttt{Control} &\equiv k := *_{\mathbb{A}};\ (\texttt{CA} \cup \texttt{NotCA}) \\
\texttt{CA} &\equiv ?(ca(k) = 1);\ (\texttt{Exit} \cup \texttt{Skip}) \\
\texttt{NotCA} &\equiv ?(ca(k) = 0);\ (\texttt{Steer} \cup \texttt{Flip} \cup \texttt{Enter}) \\
\texttt{Skip} &\equiv ?true \\
\texttt{Steer} &\equiv \omega(k) := *_{\mathbb{R}};\ ?(-\Omega(k) \le \omega(k) \le \Omega(k)) \\
\texttt{Exit} &\equiv ca(k) := 0 \\
\texttt{Enter} &\equiv (\omega(k) := side(k) \cdot \Omega(k));\ ca(k) := 1 \\
\texttt{Flip} &\equiv ?(\forall j : \mathbb{A}\ (j \neq k \rightarrow \ \mathsf{FlipSep}(j, k)));\\
&\quad\ side(k) := -side(k) \\
\mathsf{FlipSep}(i, j) &\equiv \|(x(i) + minr(i) \cdot side(i) \cdot d(i)^{\perp}) \\
&\quad - (x(j) - minr(j) \cdot side(j) \cdot d(j)^{\perp})\| \\
&\quad \ge minr(i) + minr(j) + p \\
\texttt{Plant} &\equiv \forall i : \mathbb{A}\ \Big(x(i)' = v(i) \cdot d(i),\ d(i)' = \omega(i) d(i)^{\perp} \\
&\quad \&\ \forall j : \mathbb{A}\ ((j \neq i \wedge (ca(i) = 0 \vee ca(j) = 0)) \\
&\qquad\qquad \rightarrow \mathsf{Sep}(i, j))\Big) \\
\mathsf{Sep}(i, j) &\equiv \|(x(i) + minr(i) \cdot side(i) \cdot d(i)^{\perp}) \\
&\quad - (x(j) + minr(j) \cdot side(j) \cdot d(j)^{\perp})\| \\
&\quad \ge minr(i) + minr(j) + p
\end{aligned}
$$

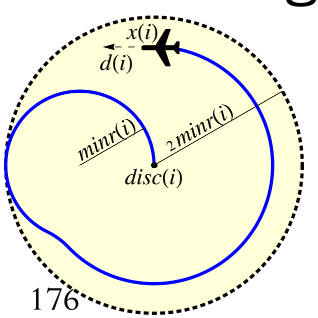


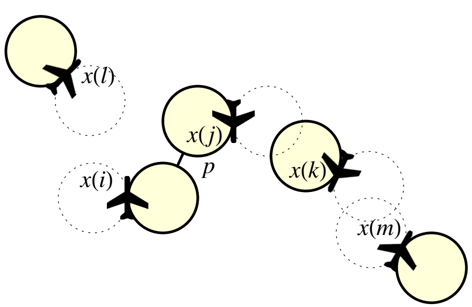

✔ **Verified in KeYmaeraD**

# Conclusions

## Challenges

- CPS needs verification
- Infinite, continuous, and evolving state space, $\mathbb{R}^\infty$
- Continuous dynamics
- Discrete control decisions
- Distributed dynamics
- Arbitrary number of aircraft
- Emergent behaviors




## Contributions

- Theorem proving is powerful for verifying distributed dynamics
- Non-linear flight paths and flyable maneuvers
- Compositionality – using small problems to solve the big ones
- Hierarchical proofs
- Undergraduates can understand and verify hybrid systems!

# Complete Proof Theory of Hybrid Systems

**Theorem (Continuous Relative Completeness) (J.Autom.Reas. 2008)**

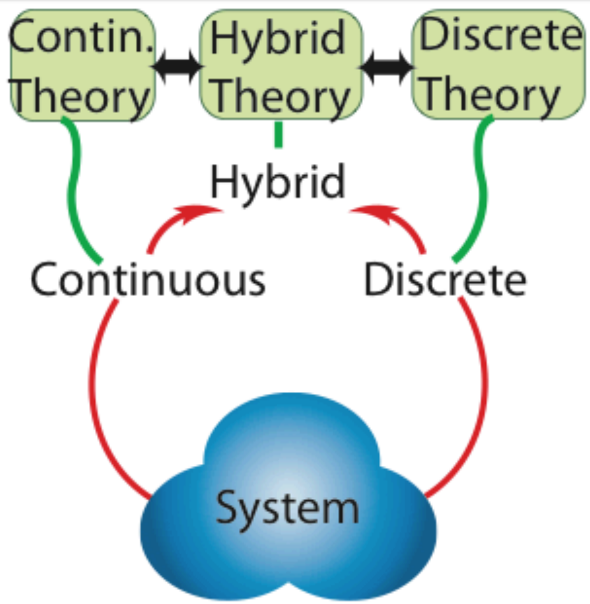
*d$\mathcal{L}$ calculus is a sound & complete axiomatization of hybrid systems relative to differential equations.*

Proof 15pp

**Theorem (Discrete Relative Completeness) (LICS'12)**

*d$\mathcal{L}$ calculus is a sound & complete axiomatization of hybrid systems relative to discrete dynamics.*

Proof +10pp



# References (page 1)

**Sarah M. Loos**, David Renshaw, and André Platzer. Formal Verification of Distributed Aircraft Controllers. In Calin Belta and Franjo Ivancic, editors, Hybrid Systems: Computation and Control (HSCC), 2013.

André Platzer and Jan-David Quesel. KeYmaera: A hybrid theorem prover for hybrid systems. In Alessandro Armando, Peter Baumgartner, and Gilles Dowek, editors, *IJCAR*, volume 5195 of *LNCS*, pages 171-178. Springer, 2008

Platzer, André. "Differential dynamic logic for hybrid systems." Journal of Automated Reasoning 41.2 (2008): 143-189.

Nikos Aréchiga, **Sarah M. Loos**, André Platzer, and Bruce H. Krogh. Using theorem provers to guarantee closed-loop system properties. In the American Control Conference, ACC, Montréal, Canada, 2012.

Stefan Mitsch, **Sarah M. Loos**, and André Platzer. Towards Formal Verification of Freeway Traffic Control. In the International Conference on Cyber-Physical Systems, ICCPS, Beijing, China, 2012.

Lucia Pallottino, Vincenzo Giovanni Scordio, Antonio Bicchi, and Emilio Frazzoli. "Decentralized cooperative policy for conflict resolution in multivehicle systems." *Robotics, IEEE Transactions on* 23, no. 6, pages 1170-1183, 2007.

# References (page 2)

Akshay Rajhans, Ajinkya Bhave, **Sarah M. Loos**, Bruce H. Krogh, André Platzer, and David Garlan. Using parameters in architectural views to support heterogeneous design and verification. In the IEEE Conference on Decision and Control and European Control Conference. 2011.

**Sarah M. Loos** and André Platzer. Safe Intersections: At the Crossing of Hybrid Systems and Verification. In the International IEEE Conference on Intelligent Transportation Systems, ITSC 2011, Washington, D.C., USA, Proceedings, 2011.

David Renshaw, **Sarah M. Loos**, and André Platzer. Distributed theorem proving for distributed hybrid systems. In the International Conference on Formal Engineering Methods, ICFEM'11, Durham, United Kingdom, Proceedings, LNCS. Springer, 2011.

**Sarah M. Loos**, André Platzer, and Ligia Nistor. Adaptive cruise control: Hybrid, distributed, and now formally verified. In the 17th International Symposium on Formal Methods, FM, Limerick, Ireland, Proceedings, LNCS. Springer, 2011.

André Platzer. Quantified differential dynamic logic for distributed hybrid systems. In Computer Science Logic. Volume 6247 of LNCS. Springer, 2010.

Dubins, L.E. On curves of minimal length with a constraint on average curvature, and with prescribed initial and terminal positions and tangents. Am J Math 79(3), pages 497–516, 1957.