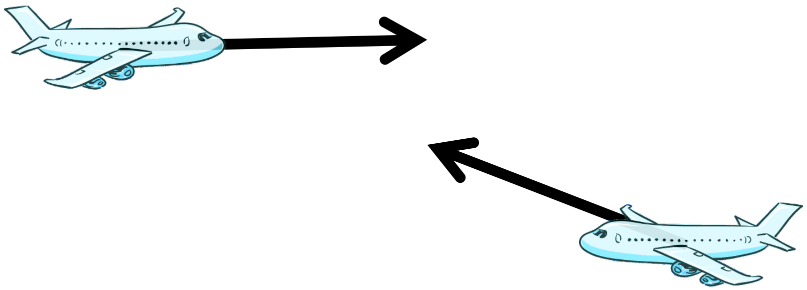
dTL^2: Differential Temporal Dynamic Logic with Nested Modalities for Hybrid Systems

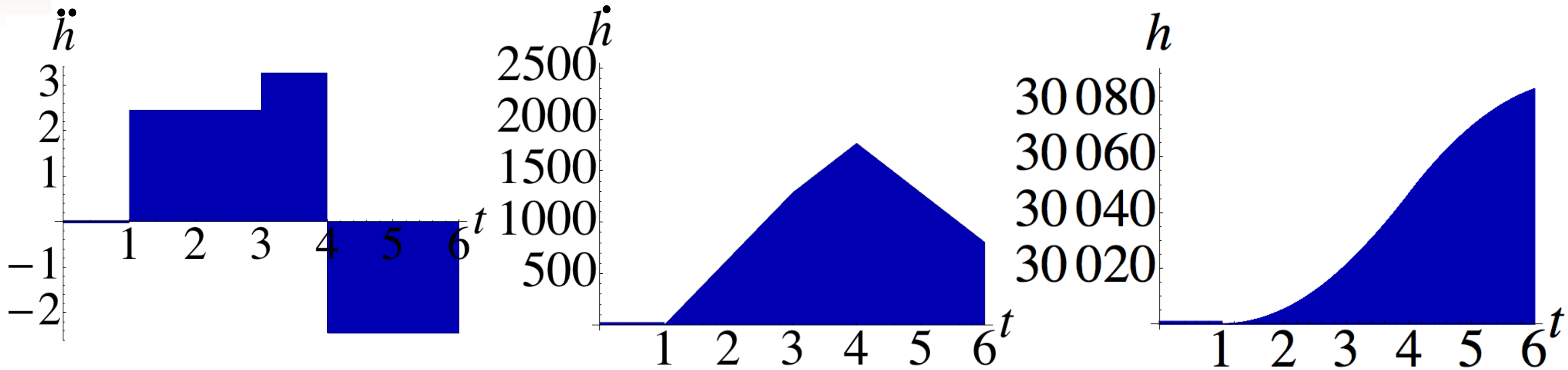
Jean-Baptiste Jeannin and André Platzer
Carnegie Mellon University

IJCAR, July 21st, 2014

Hybrid Systems

- Continuous Evolutions (differential equations, e.g. flight dynamics)
- Discrete Jumps (control decisions, e.g. pilot actions)

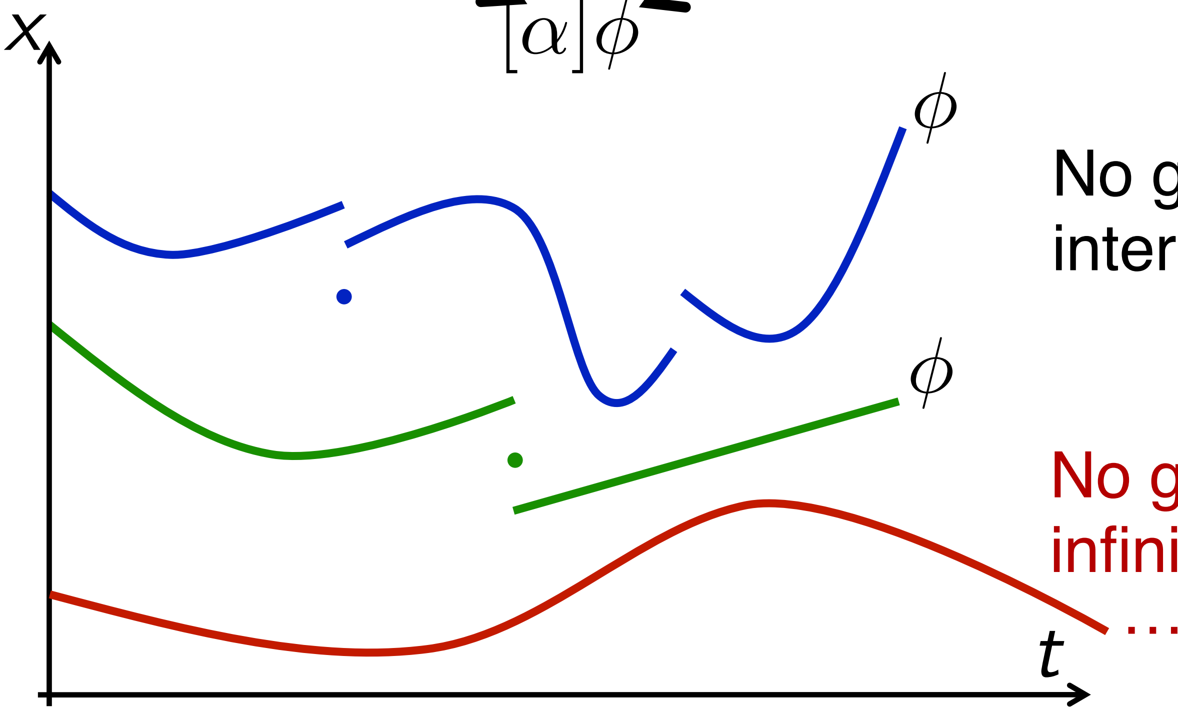




Differential Dynamic Logic

- used to reason about (nondeterministic) hybrid systems
- comes with a (relatively) complete axiomatization
- proves properties about the end state of the execution

hybrid system → $[\alpha]\phi$ ← all behaviors of α satisfy ϕ at the end

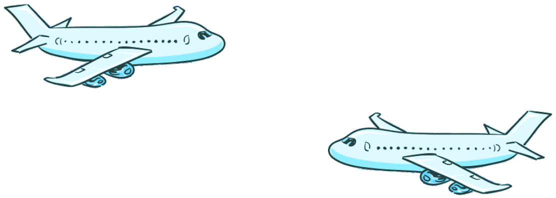


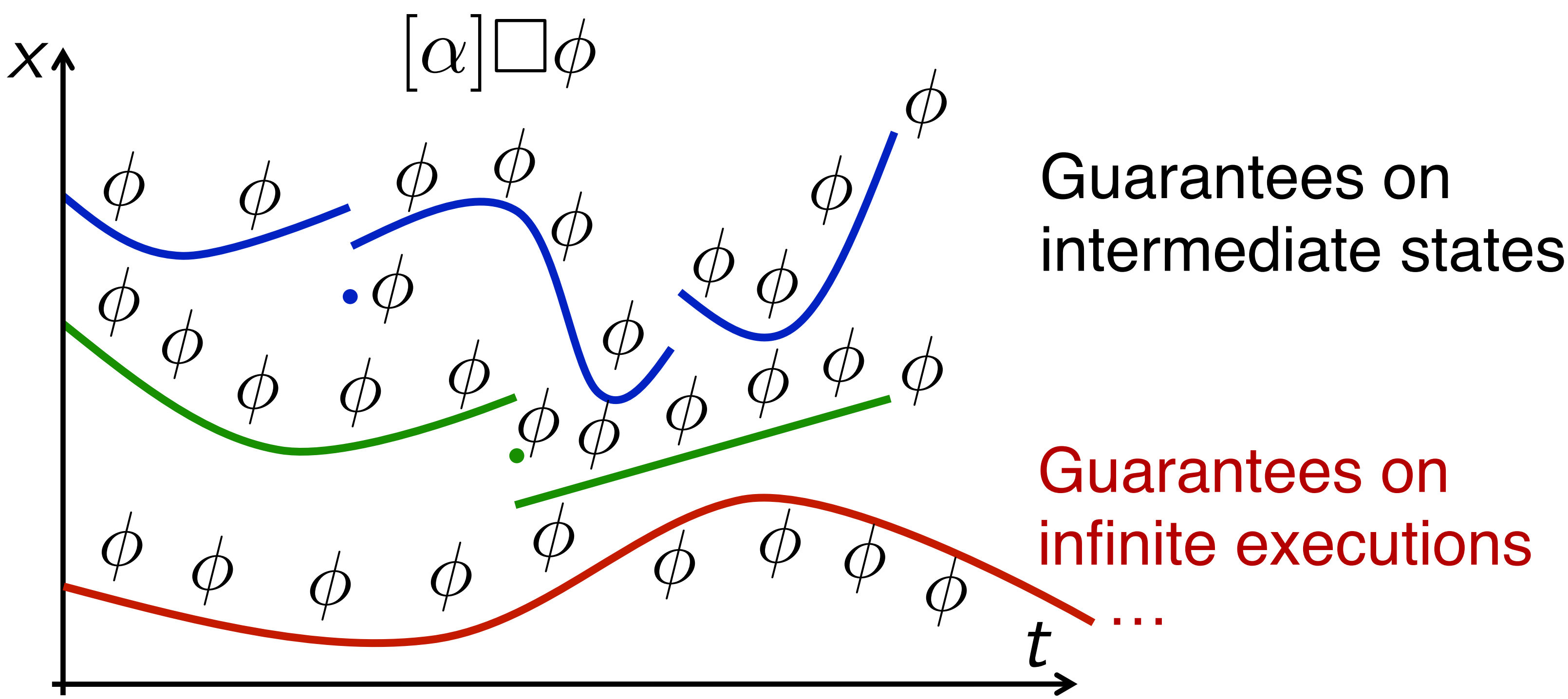
No guarantee on intermediate states

No guarantee on infinite executions

Differential Temporal Dynamic Logic

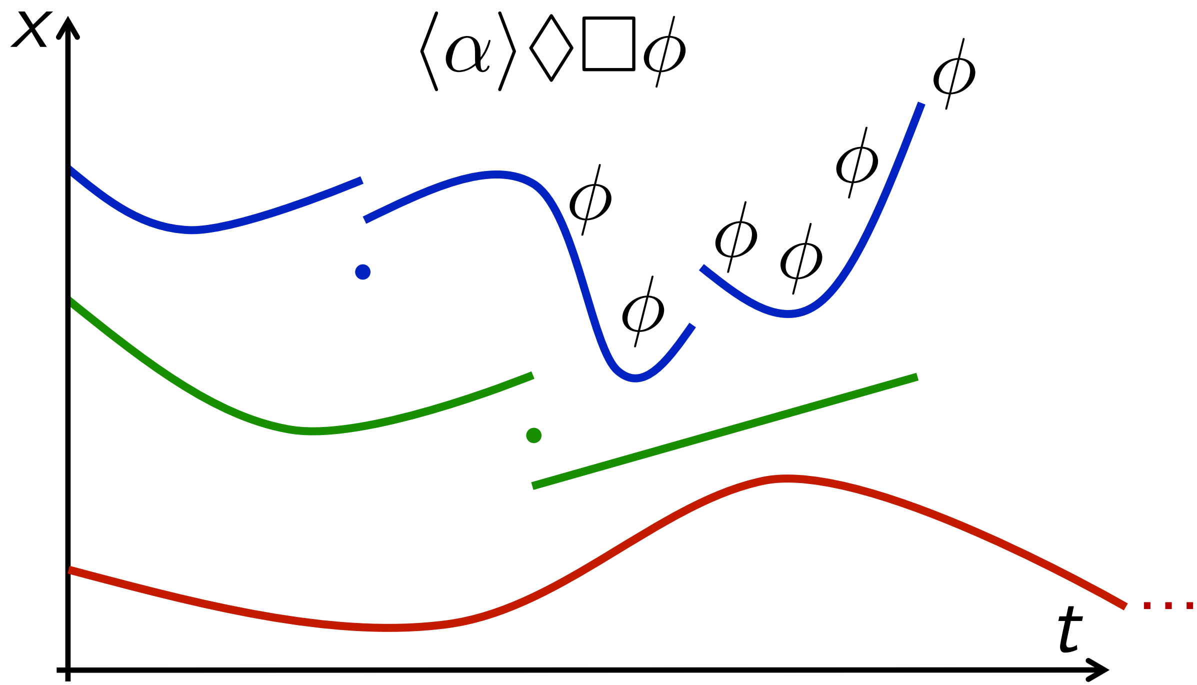
- What about property
  "these airplanes never collide"?
- We need some temporal reasoning





Nested Alternating Modalities

- What about property "this satellite can reach its orbit and then stay there"?
- We need nested alternating modalities
- A step towards dTL*, handling temporal formulas of CTL*



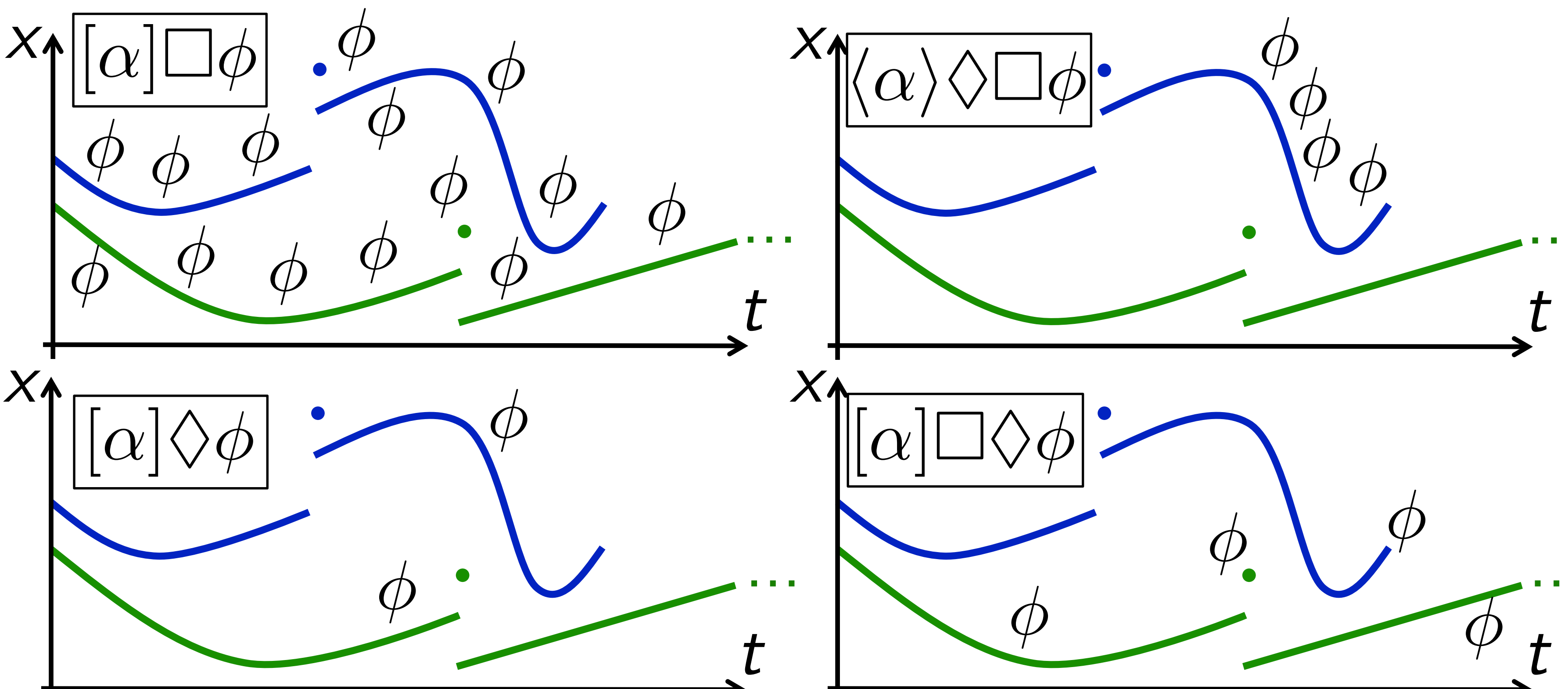
Temporal Properties of Hybrid Systems

State Property ϕ, ψ

- $\leq, \neg, \wedge, \vee, \forall, \exists$
- $[\alpha]\pi$ for all traces of α
- $\langle\alpha\rangle\pi$ there is a trace of α

Trace property π

- ϕ
- $\Box\pi$ for all suffix of σ
- $\Diamond\pi$ there is a suffix of σ



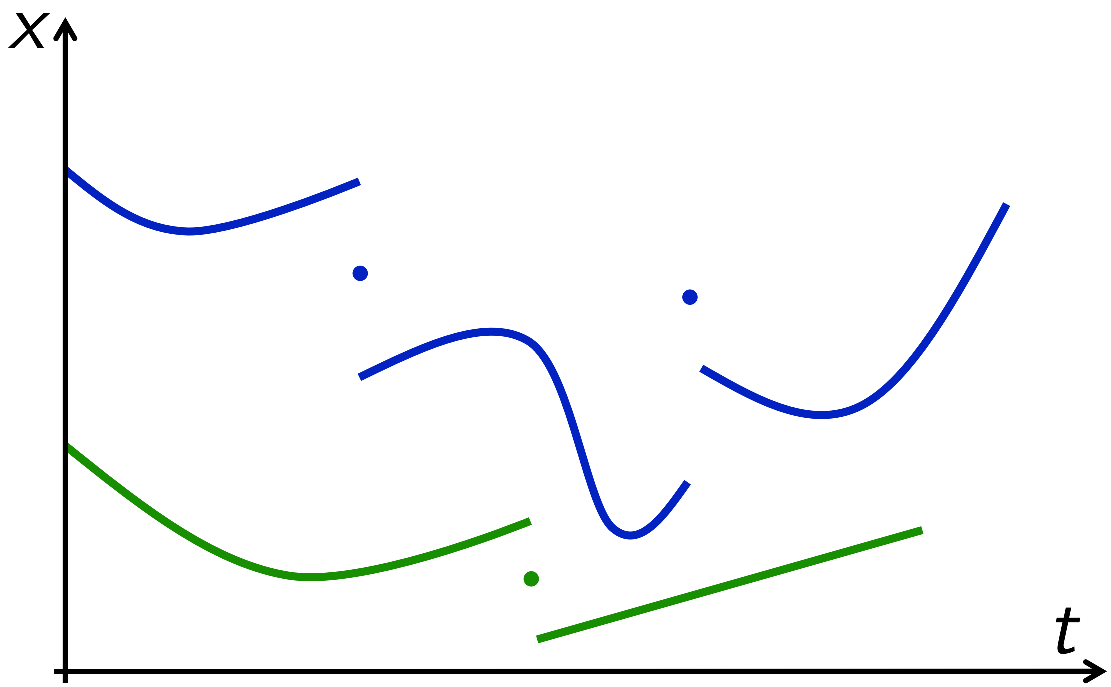
Hybrid Programs

They model systems and are non deterministic. They are:

- Discrete variable assignment $x := \theta$
- Test $?\chi$
- Differential Equation $x' = \theta \;\&\; \chi$
- Nondeterministic choice $\alpha \cup \beta$
- Sequential composition $\alpha; \beta$
- Nondeterministic repetition α^*

Trace Semantics of Hybrid Programs

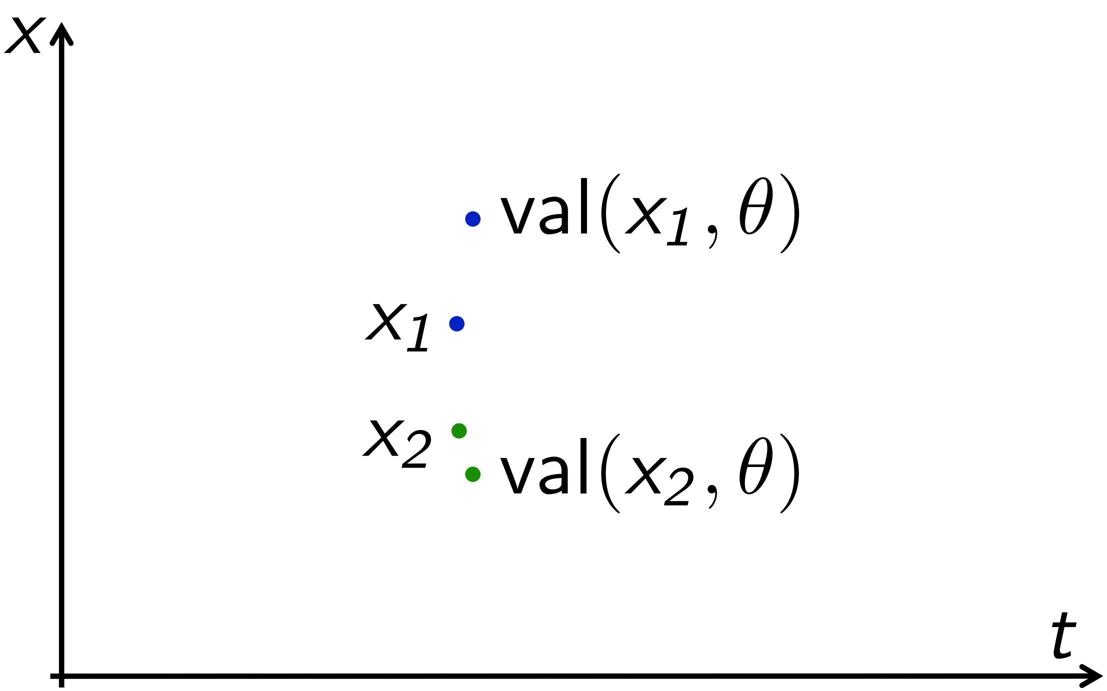
A trace σ represents the evolution of the variable over time, consisting of continuous evolutions and discrete jumps



The trace semantics of a hybrid program is a set of traces

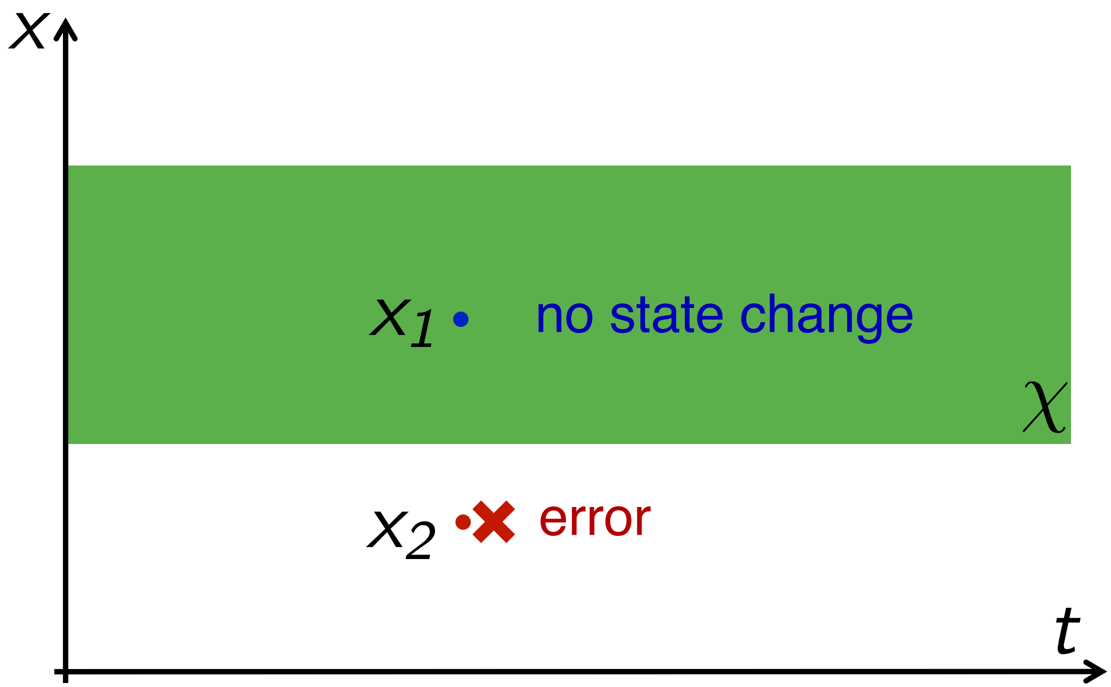
Trace Semantics of Hybrid Programs

Variable assignment $x := \theta$



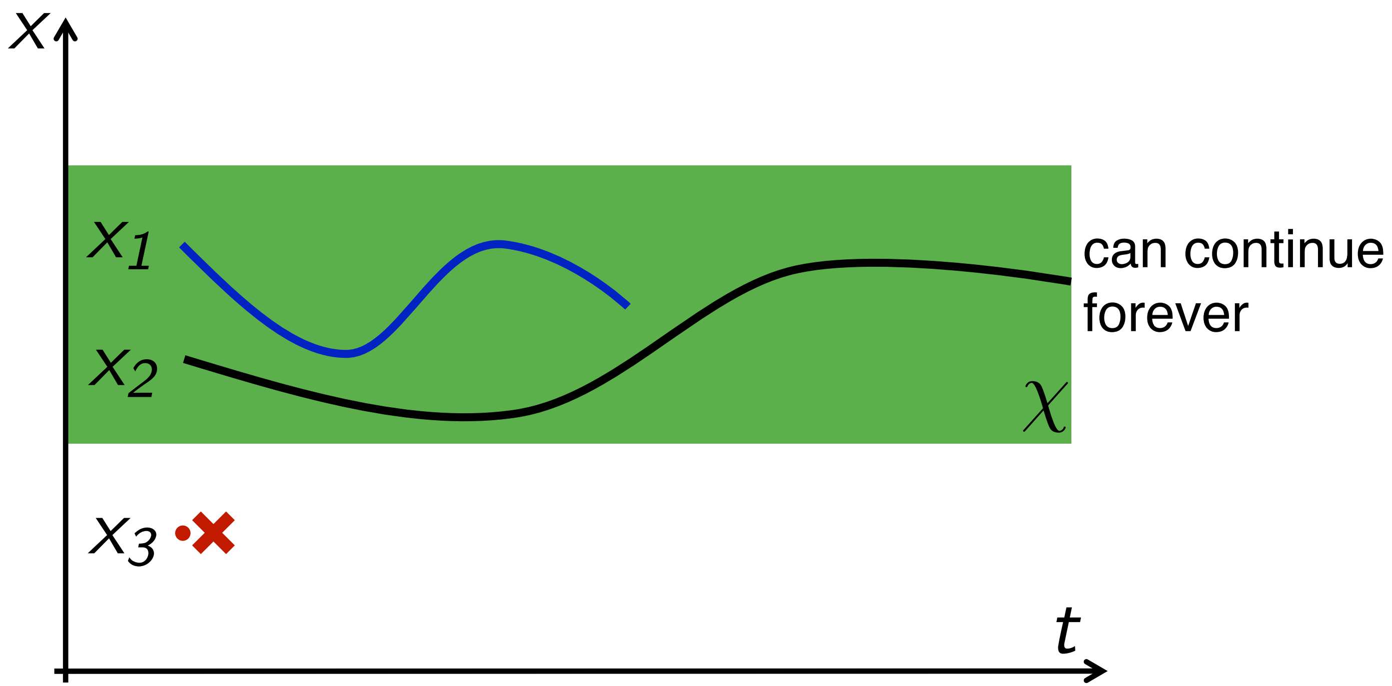
Trace Semantics of Hybrid Programs

Test $?\chi$



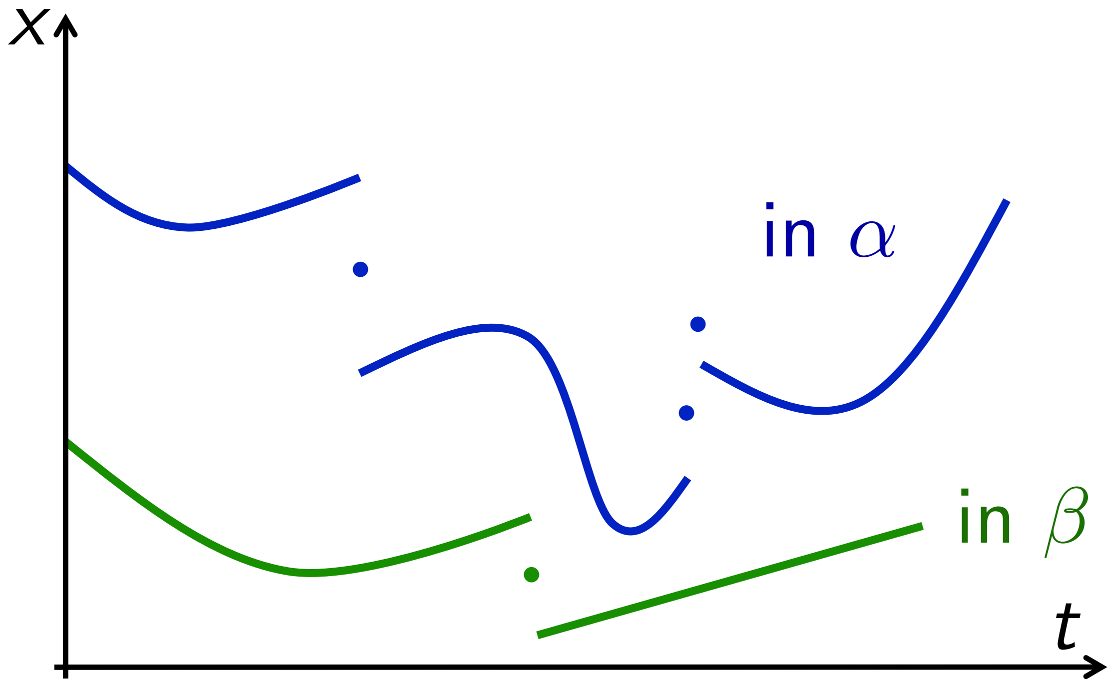
Trace Semantics of Hybrid Programs

Differential equation $x' = \theta \ \& \ \chi$



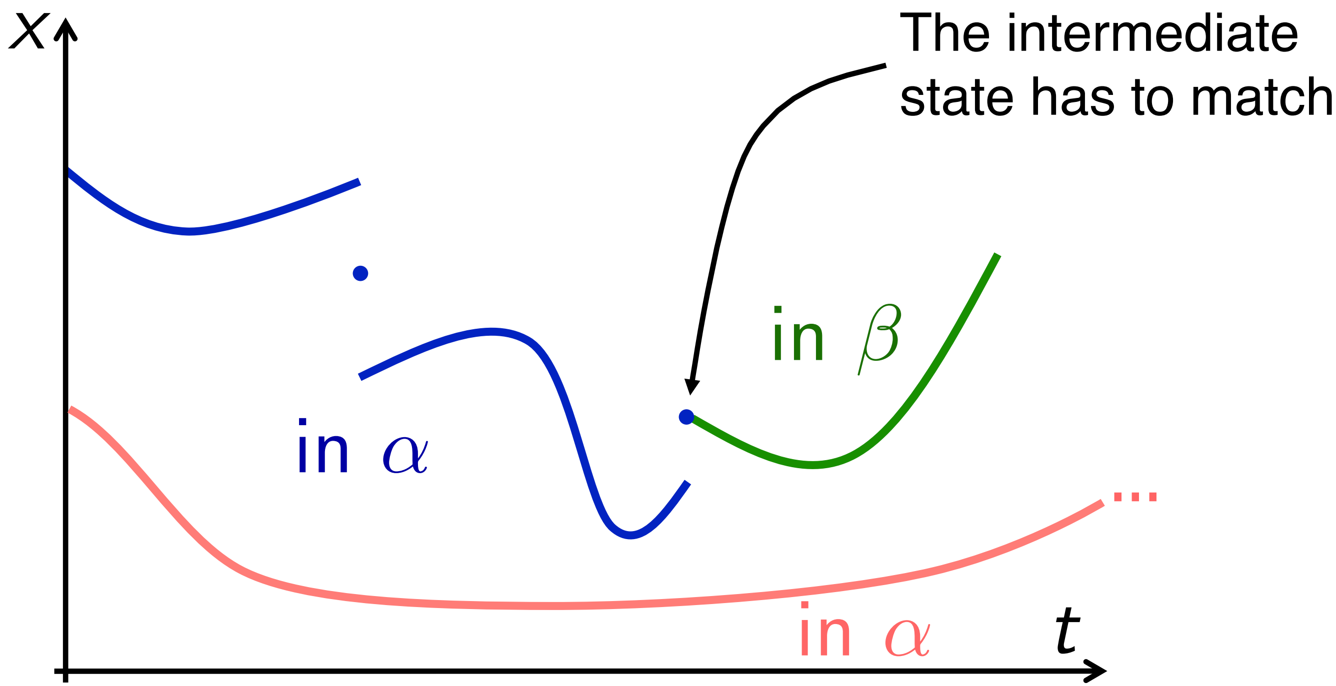
Trace Semantics of Hybrid Programs

Nondeterministic choice $\alpha \cup \beta$



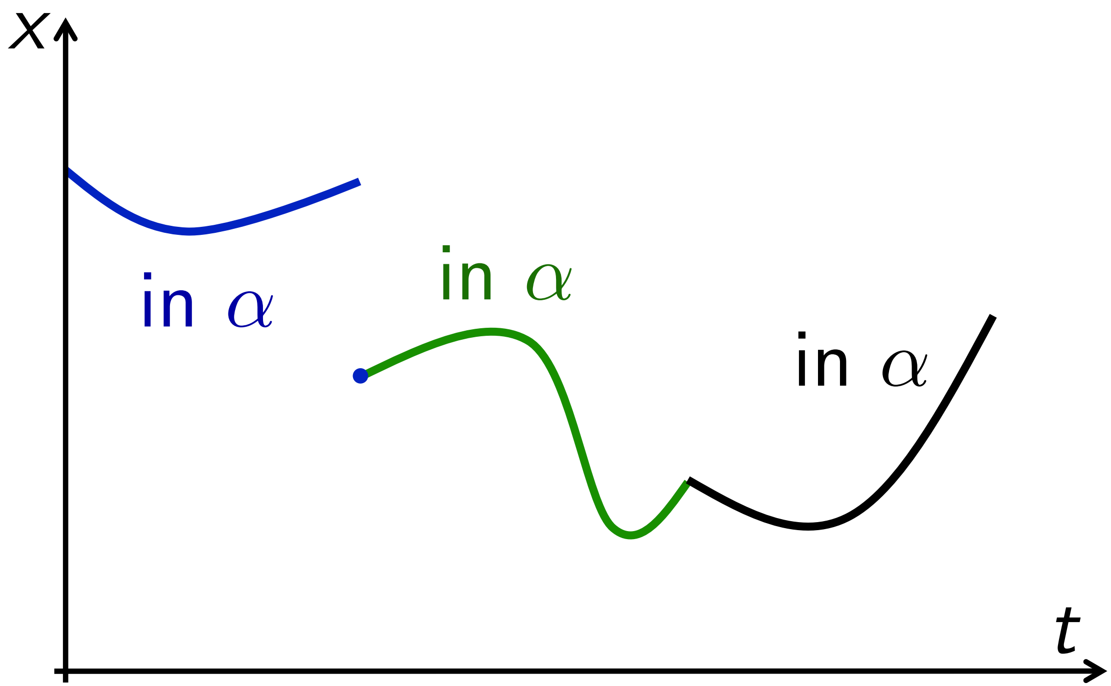
Trace Semantics of Hybrid Programs

Sequential composition $\alpha;\beta$



Trace Semantics of Hybrid Programs

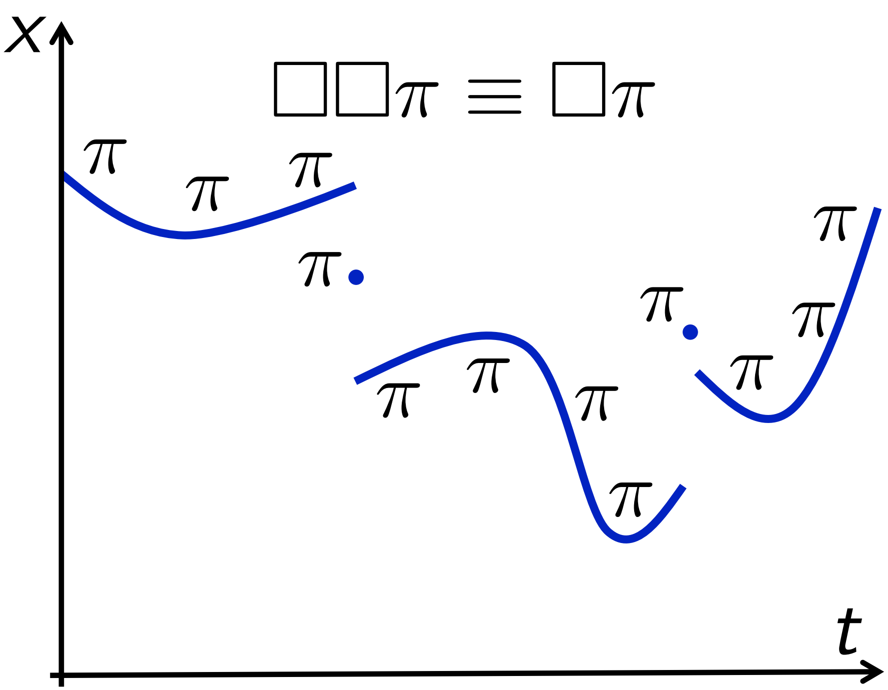
Nondeterministic repetition α^*

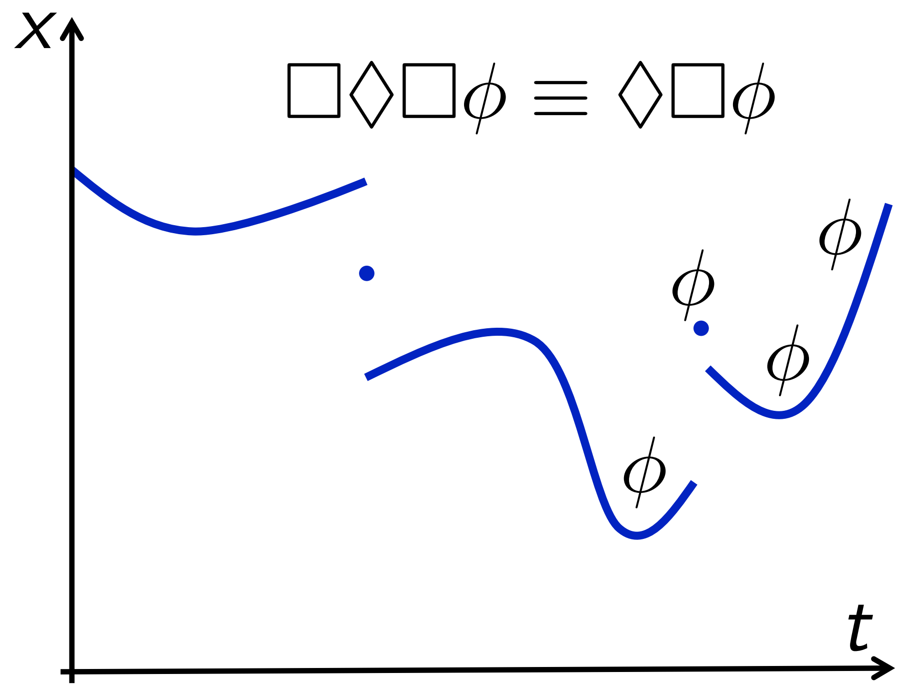


Simplification of Trace Formulas

$$\Diamond\Diamond\Diamond\Box\Diamond\Box\Box\phi$$
$$\equiv \Diamond\Box\Diamond\Box\phi$$
$$\equiv \Diamond\Diamond\Box\phi$$
$$\equiv \Diamond\Box\phi$$

$$\Box\Box\pi \equiv \Box\pi$$
$$\Diamond\Diamond\pi \equiv \Diamond\pi$$
$$\Box\Diamond\Box\phi \equiv \Diamond\Box\phi$$
$$\Diamond\Box\Diamond\phi \equiv \Box\Diamond\phi$$





Simplification of Trace Formulas

$$\begin{aligned} & \Diamond\Diamond\Diamond\Box\Diamond\Box\Box\phi \\ \equiv\ & \Diamond\Box\Diamond\Box\phi \\ \equiv\ & \Diamond\Diamond\Box\phi \\ \equiv\ & \Diamond\Box\phi \end{aligned}$$

$$\begin{aligned} \Box\Box\pi &\equiv \Box\pi \\ \Diamond\Diamond\pi &\equiv \Diamond\pi \\ \Box\Diamond\Box\phi &\equiv \Diamond\Box\phi \\ \Diamond\Box\Diamond\phi &\equiv \Box\Diamond\phi \end{aligned}$$

The only interesting temporal properties thus are

$$\Box\phi \qquad \Diamond\phi \qquad \Diamond\Box\phi \qquad \Box\Diamond\phi$$

and this corresponds to modal system S4.2

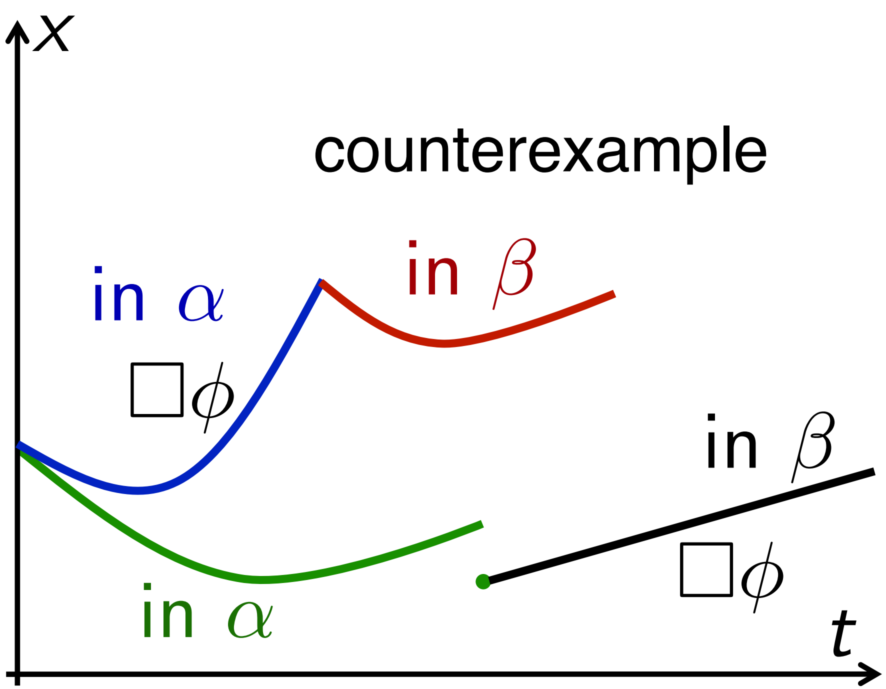
We focus on the study of $\Box\phi$ and particularly on $\langle\alpha\rangle\Box\phi$

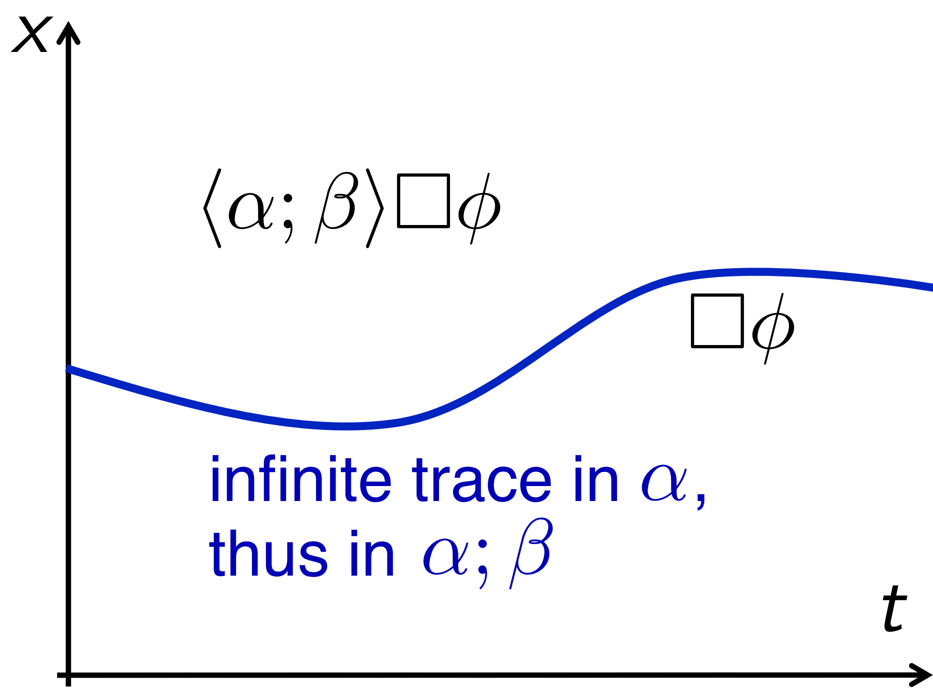
A Technical Issue: the Composition

$$\frac{\langle\alpha\rangle\Box\phi \land \langle\alpha\rangle\langle\beta\rangle\Box\phi}{\langle\alpha;\beta\rangle\Box\phi}$$ (unsound)

$\langle\alpha\rangle(\Box\phi \land \langle\beta\rangle\Box\phi)$ (OK if the trace of α terminates)

$\langle\alpha\rangle\Box\phi$ (if the trace of α does not terminate)





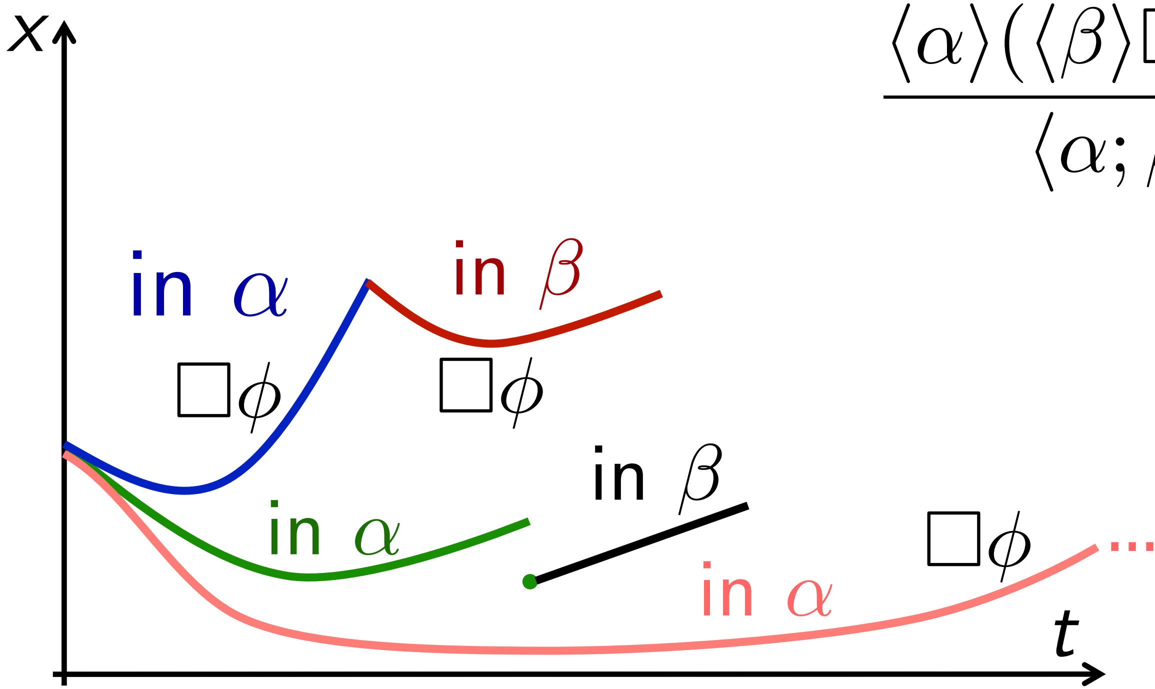
Solution: Introducing $\phi \sqcap \Box\psi$

$\sigma \vDash \phi \sqcap \Box\psi$ if and only if

- last $\sigma \vDash \phi$ and $\sigma \vDash \Box\psi$ — if σ terminates
- $\sigma \vDash \Box\psi$ — otherwise (infinite or error)

and $\Box\phi \equiv \text{true} \sqcap \Box\phi$

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



Solution: Introducing $\phi \sqcap \Box\psi$

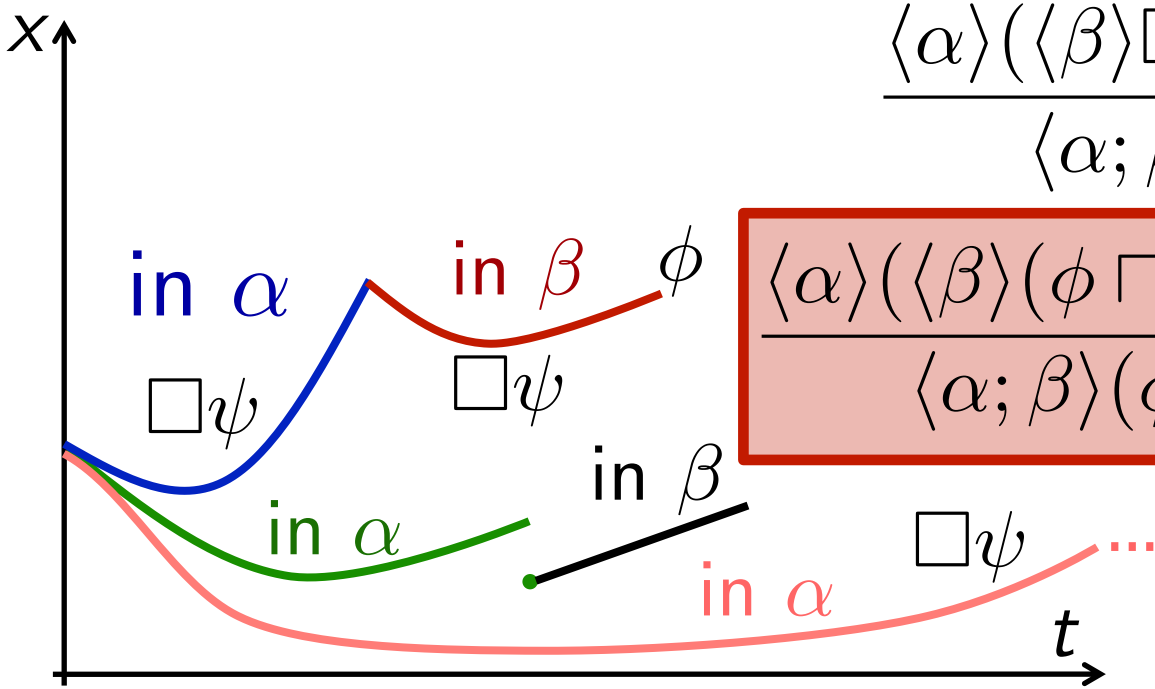
$\sigma \vDash \phi \sqcap \Box\psi$ if and only if

- last $\sigma \vDash \phi$ and $\sigma \vDash \Box\psi$ — if σ terminates
- $\sigma \vDash \Box\psi$ — otherwise (infinite or error)

and $\Box\phi \equiv \text{true} \sqcap \Box\phi$

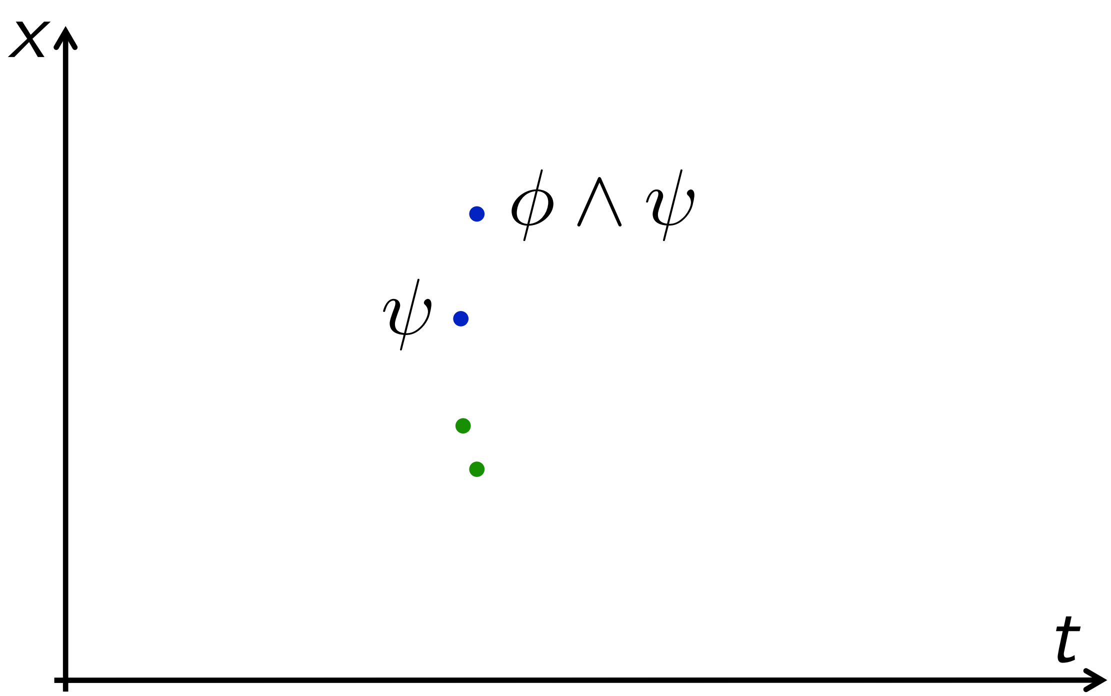
$$\frac{\langle\alpha\rangle(\langle\beta\rangle\Box\phi \sqcap \Box\phi)}{\langle\alpha;\beta\rangle\Box\phi}\ \langle;\rangle\Box$$

$$\frac{\langle\alpha\rangle(\langle\beta\rangle(\phi \sqcap \Box\psi) \sqcap \Box\psi)}{\langle\alpha;\beta\rangle(\phi \sqcap \Box\psi)}\ \langle;\rangle\sqcap$$



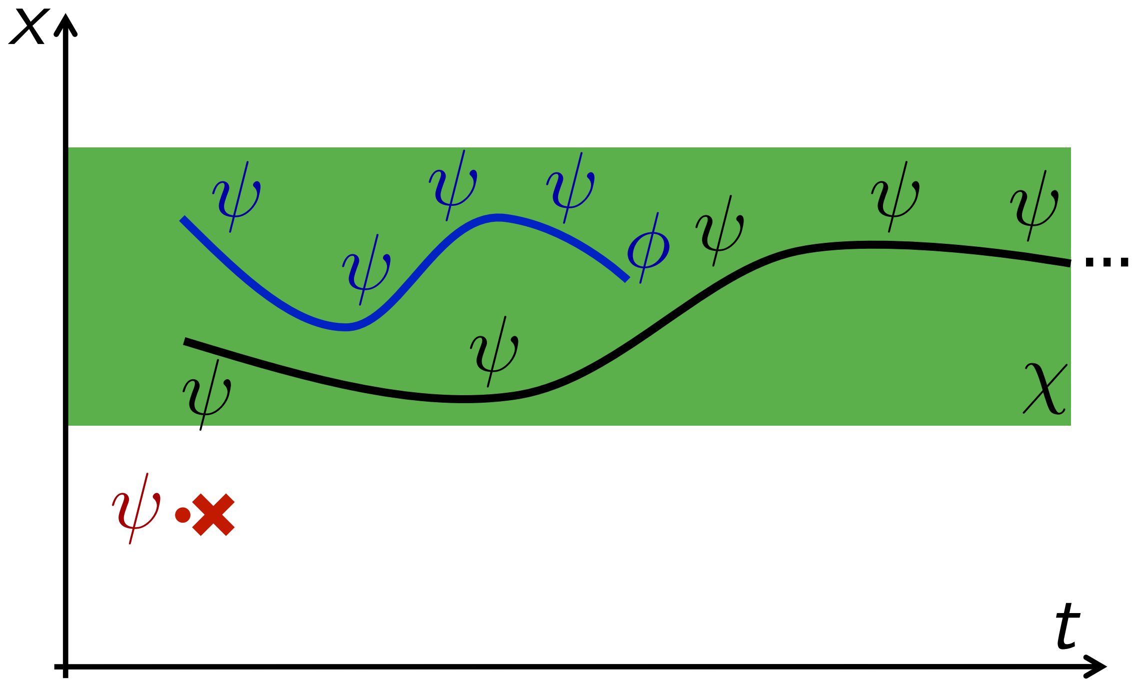
New Rules for $\phi \sqcap \Box\psi$

$$\frac{\psi \land \langle x := \theta\rangle(\phi \land \psi)}{\langle x := \theta\rangle(\phi \sqcap \Box\psi)}\ \langle{:=}\rangle\sqcap$$



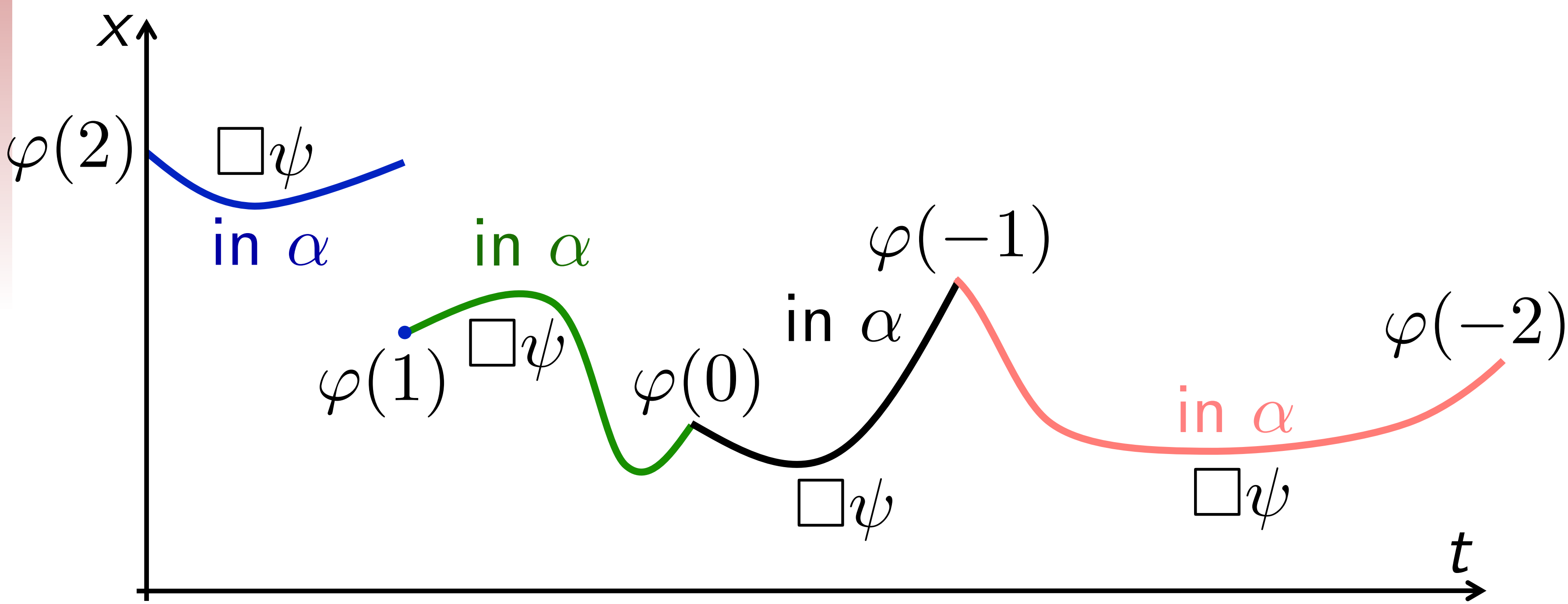
New Rules for $\phi \sqcap \Box\psi$

$$\frac{(\neg\chi \land \psi) \lor \langle x' = \theta \,\&\, (\chi \land \psi)\rangle\phi \lor [x' = \theta](\chi \land \psi)}{\langle x' = \theta \,\&\, \chi\rangle(\phi \sqcap \Box\psi)}$$



New Rules for $\phi \sqcap \Box\psi$

$$\frac{\forall^{\alpha}\forall r > 0\ (\varphi(r) \rightarrow \langle\alpha\rangle(\varphi(r-1) \sqcap \Box\psi))}{(\exists r\ \varphi(r)) \wedge \psi \rightarrow \langle\alpha^*\rangle((\exists r \leq 0\ \varphi(r)) \sqcap \Box\psi)}$$



Similarly $\phi \sqcup \Diamond\psi$, $\phi \blacktriangleleft \Box\Diamond\psi$, $\phi \blacktriangleleft \Diamond\Box\psi$

Remember: $\sigma \vDash \phi \sqcap \Box\psi$ if and only if

- last $\sigma \vDash \phi$ and $\sigma \vDash \Box\psi$ — if σ terminates
- $\sigma \vDash \Box\psi$ — otherwise (infinite or error)

$\sigma \vDash \phi \sqcup \Diamond\psi$ if and only if

- last $\sigma \vDash \phi$ or $\sigma \vDash \Diamond\psi$ — if σ terminates
- $\sigma \vDash \Diamond\psi$ — otherwise (infinite or error)

$\sigma \vDash \phi \blacktriangleleft \Box\Diamond\psi$ if and only if

- last $\sigma \vDash \phi$ — if σ terminates
- $\sigma \vDash \Box\Diamond\psi$ — otherwise (infinite or error)

$\sigma \vDash \phi \blacktriangleleft \Diamond\Box\psi$ is defined similarly

Meta-Results

Theorem

The dTL^2 calculus is sound, i.e., derivable state formulas are valid

Theorem

The dTL^2 calculus restricted to star-free programs is complete relative to FOD, i.e., every valid dTL^2 formula with only star-free programs can be derived from FOD tautology

FOD = first order real arithmetic augmented with formulas expressing properties of differential equations

Related work

- [Beckert and Schlager 2001, Platzer 2007]
  - the basis for this work
  - only formulas of the form $[\alpha]\Box\phi$ and $\langle\alpha\rangle\Diamond\phi$
- Process logic [Parikh 1978, Pratt 1979, Harel et al. 1982]
  - well-studied but limited to the discrete case
  - different approach: $[\alpha]\Diamond\phi$ is a trace formula rather than a state formula
- [Davoren and Nerode 2000, Davoren et al. 2004]
  - calculi for temporal reasoning of hybrid systems
  - propositional only
  - but no specific rule for differential equations

Conclusion and Future Work

- We have extended Differential Temporal Dynamic Logic to handle formulas of the form

$$[\alpha]\Diamond\phi \qquad \langle\alpha\rangle\Box\phi \qquad [\alpha]\Box\Diamond\phi \qquad \langle\alpha\rangle\Box\Diamond\phi$$

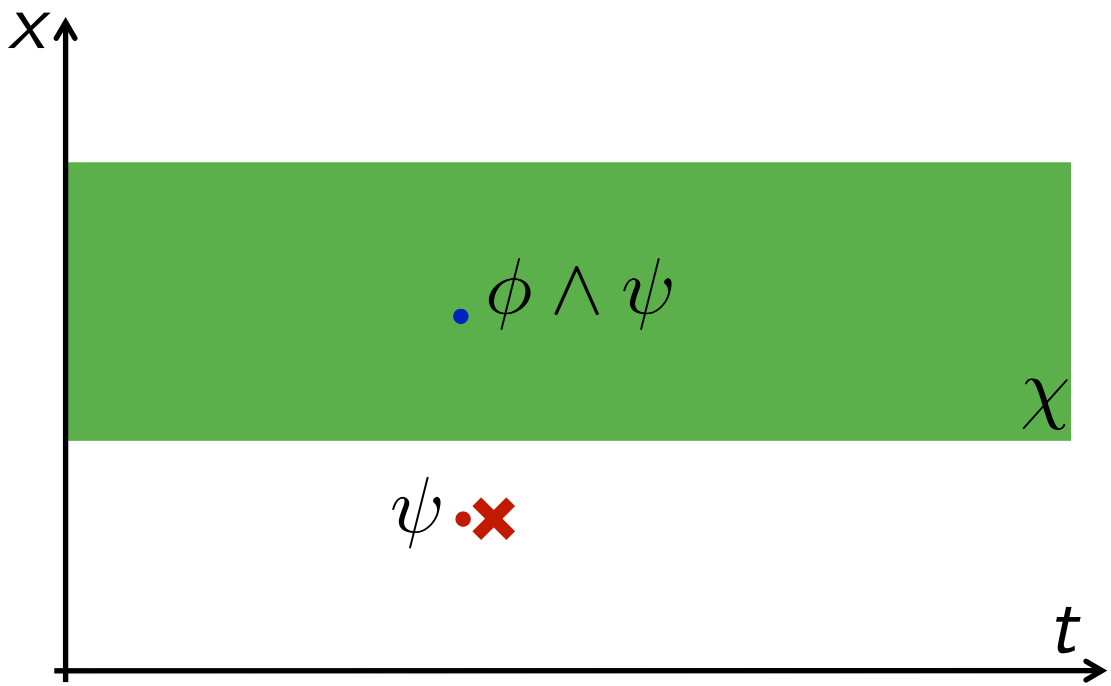
  solving open problems posed in [Beckert and Schleger 2001] and [Platzer 2007]
- We prove soundness and relative completeness for star-free expressions

Future work:

- Extensions: Until operator, nested $\wedge$ and $\Diamond$
- This is a step towards dTL*, handling formulas of CTL*

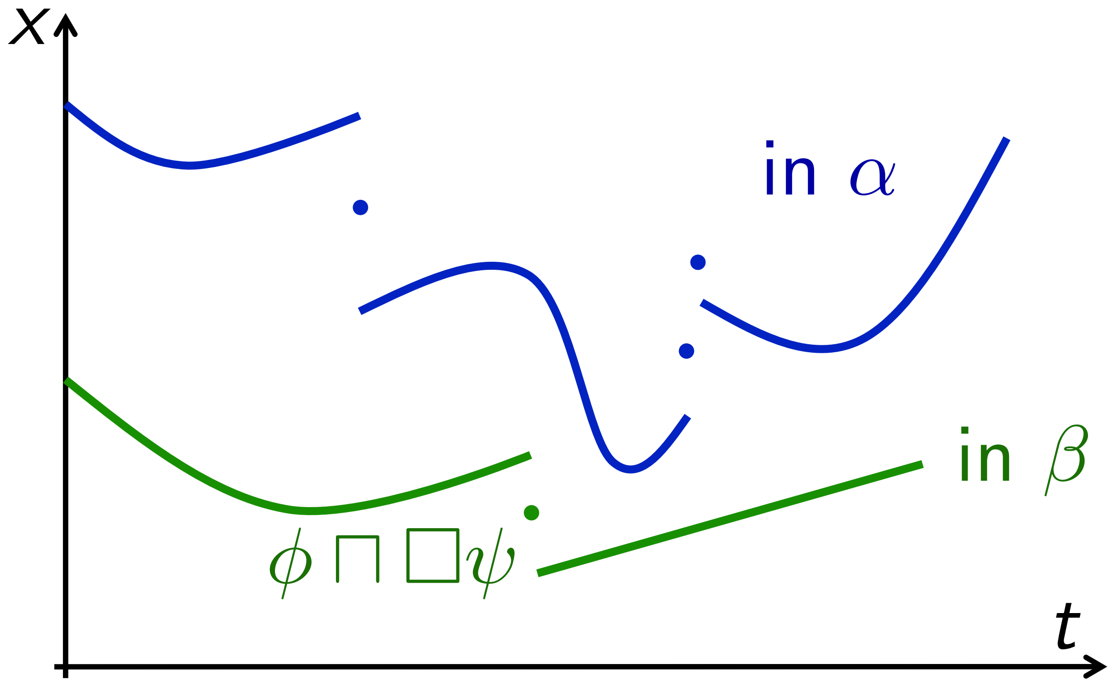
New Rules for $\phi \sqcap \Box\psi$

$$\frac{(\neg\chi \vee \phi) \wedge \psi}{\langle ?\chi\rangle(\phi \sqcap \Box\psi)}\ \langle ?\rangle\sqcap$$



New Rules for $\phi \sqcap \Box\psi$

$$\frac{\langle\alpha\rangle(\phi \sqcap \Box\psi) \lor \langle\beta\rangle(\phi \sqcap \Box\psi)}{\langle\alpha \cup \beta\rangle(\phi \sqcap \Box\psi)} \langle\cup\rangle\sqcap$$



Differential (Temporal) Dynamic Logic

- is based on dynamic logic augmented with continuous evolutions, and has been used to verify trains, highways and airplanes. It can express properties

$$[\alpha]\phi \qquad \langle\alpha\rangle\phi$$

- has been extended with differential temporal dynamic logic, expressing properties

$$[\alpha]\Box\phi \qquad \langle\alpha\rangle\Diamond\phi$$

- but we would like to be able to express more powerful properties, for example

$$[\alpha]\Diamond\phi \qquad \langle\alpha\rangle\Box\phi \qquad [\alpha]\Box\Diamond\phi \qquad \langle\alpha\rangle\Box\Diamond\phi$$

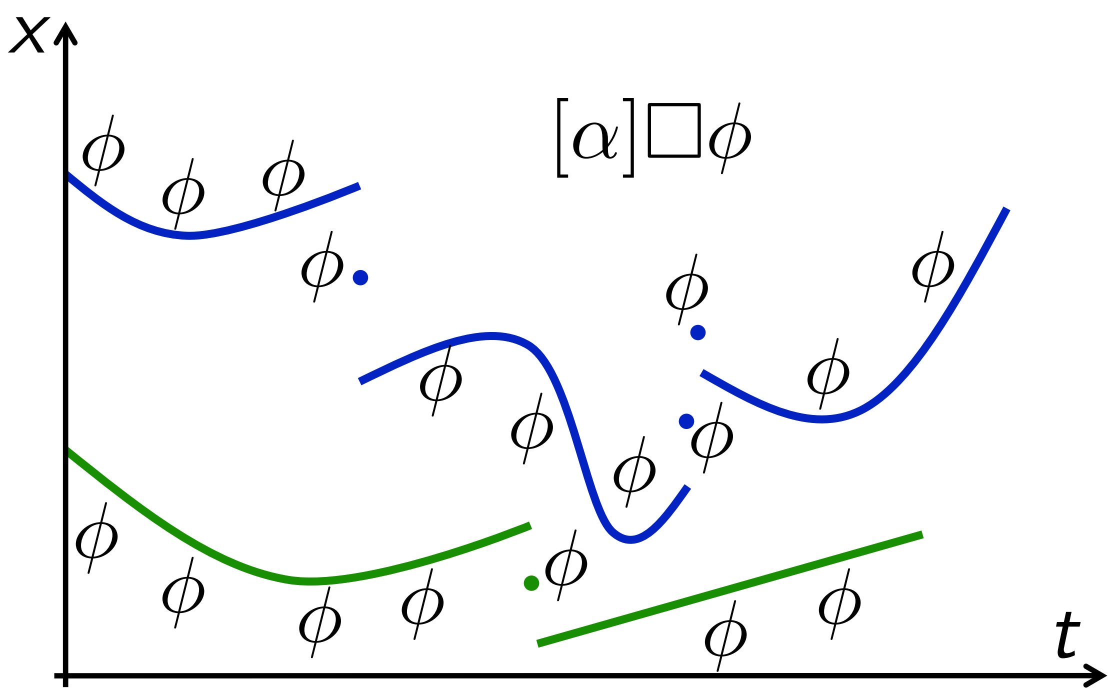
Temporal Properties of Hybrid Programs

State Property ϕ, ψ

- $\leq, \neg, \wedge, \vee, \forall, \exists$
- $[\alpha]\pi$ for all traces of α
- $\langle\alpha\rangle\pi$ there is a trace of α

Trace property π

- ϕ
- $\Box\pi$ for all suffix of σ
- $\Diamond\pi$ there is a suffix of σ



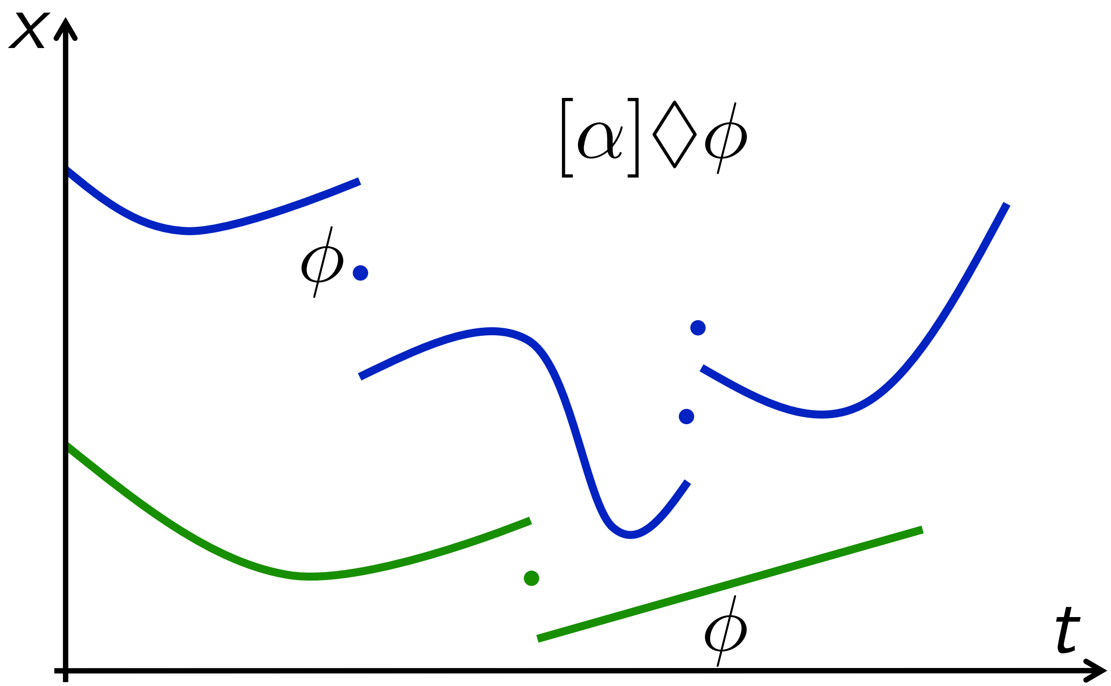
Temporal Properties of Hybrid Programs

State Property ϕ, ψ

- $\leq, \neg, \wedge, \vee, \forall, \exists$
- $[\alpha]\pi$ for all traces of α
- $\langle\alpha\rangle\pi$ there is a trace of α

Trace property π

- ϕ
- $\Box\pi$ for all suffix of σ
- $\Diamond\pi$ there is a suffix of σ



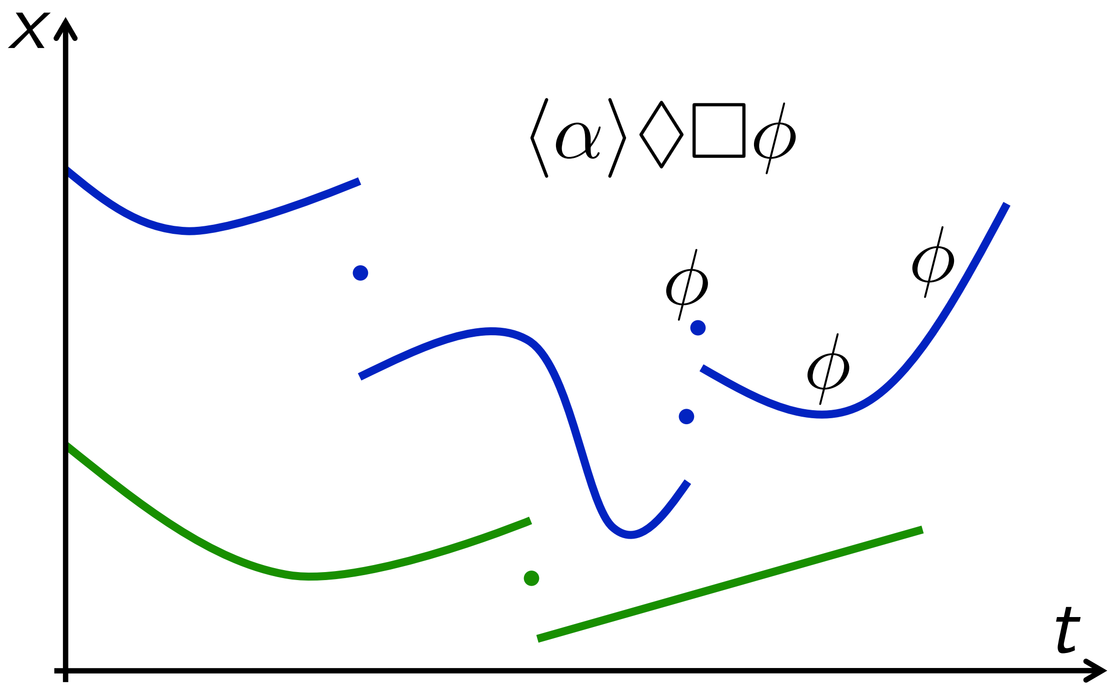
Temporal Properties of Hybrid Programs

State Property ϕ, ψ

- $\leq, \neg, \wedge, \vee, \forall, \exists$
- $[\alpha]\pi$ for all traces of α
- $\langle\alpha\rangle\pi$ there is a trace of α

Trace property π

- ϕ
- $\Box\pi$ for all suffix of σ
- $\Diamond\pi$ there is a suffix of σ



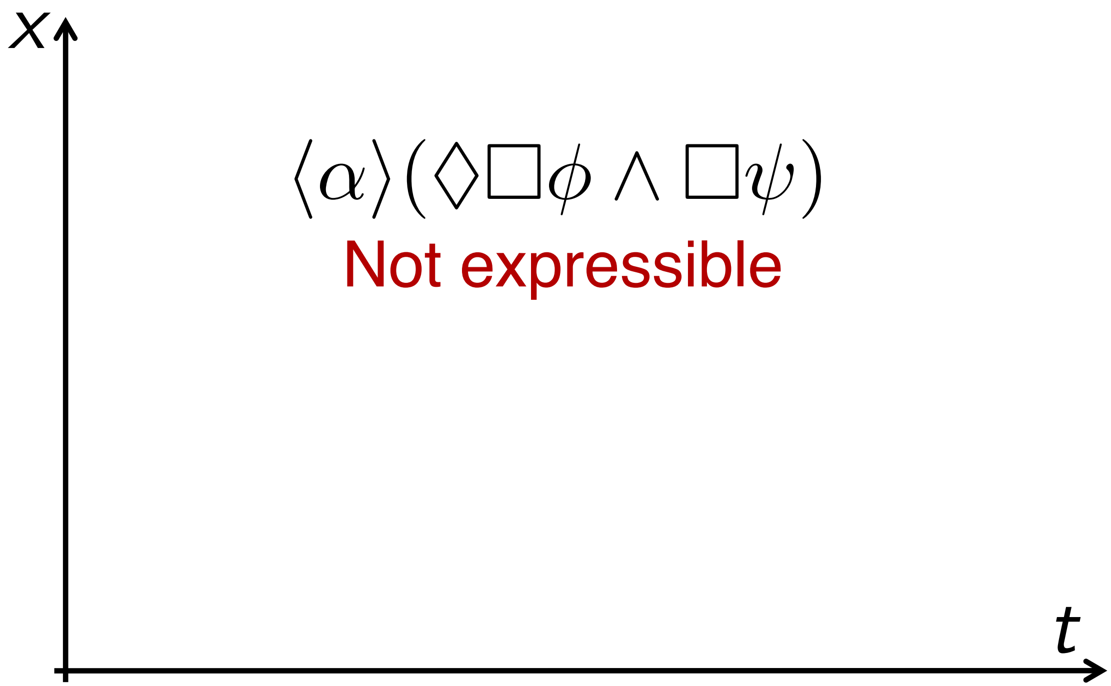
Temporal Properties of Hybrid Programs

State Property ϕ, ψ

- $\leq, \neg, \wedge, \vee, \forall, \exists$
- $[\alpha]\pi$ for all traces of α
- $\langle\alpha\rangle\pi$ there is a trace of α

Trace property π

- ϕ
- $\Box\pi$ for all suffix of σ
- $\Diamond\pi$ there is a suffix of σ



$$\langle\alpha\rangle(\Diamond\Box\phi \wedge \Box\psi)$$

Not expressible