Recitation 2

Logic and transition relations

$$d\mathcal{L} = \overbrace{FOL_{\mathbb{R}}}^{\text{Last week}} + HP + \underbrace{\text{Modalities}}_{[\cdot],\ \langle\cdot\rangle}$$

This week

Precondition

Safety Property

$$P \rightarrow [\alpha]\, Q$$

H.P.

Recap: $FOL_{\mathbb{R}}$

Terms $\quad e := c \mid x \mid e_1 + e_2 \mid e_1 \cdot e_2$

$c \in \mathbb{R}$

$\mathbb{Q}$

Formulas $\quad P, Q := e_1 \sim e_2 \mid \neg P \mid P \vee Q \mid \cdots \mid \exists x P \mid \forall x P$

$\sim \in \{=, <, >, \leq, \geq\}$

$\mid [\alpha] P \mid \langle \alpha \rangle P$

H.P. $\quad \alpha := x := e \mid ?Q \mid \{x' = f(x) \,\&\, Q\}$

$\mid \alpha ; \beta \mid \alpha \cup \beta \mid \alpha^*$

Semantics

$[\![\cdot]\!] : \text{Term} \to (\text{State} \to \mathbb{R})$

If $\omega(x) = 2$, then $\omega [\![x+1]\!] = 3$

$[\![\cdot]\!] : \text{Formula} \to \mathcal{P}(\text{State})$

$[\![x = 0]\!] = \{\omega \mid \omega(x) = 0\}$

$[\![\exists y,\ x = y^2]\!] = \{\omega \mid \omega(x) \geq 0\}$

$[\![\forall x \exists y\ x = y^2]\!] = \emptyset$ (unsat)

$[\![\exists y\ x + y = 0]\!] = \text{State}$ (valid)

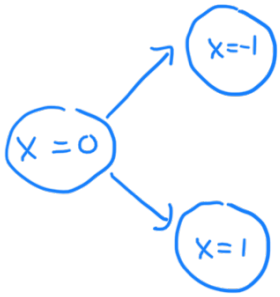
A semantics for Hybrid Programs

Attempt 1

$$[\![\cdot]\!] : HP \to (State \to State)$$

Does not handle nondeterminism!

Example: $x := x+1 \;\cup\; x := x-1$



Better definition

$$[\![\cdot]\!] : HP \to \underbrace{\mathcal{P}(State \times State)}_{\text{set of transitions}}$$

$$[\![\alpha]\!] = \left\{ (\omega, \nu) \;\middle|\; \begin{array}{l}\text{one can transition from} \\ \omega \text{ to } \nu \text{ by running } \alpha\end{array} \right\}$$

current state final state

Defining the semantics of H.Ps case by case

$$\alpha ::= \underbrace{x := e \mid ?Q \mid \{x' = f(x) \,\&\, Q\}}_{\text{atomic}} \mid \underbrace{\alpha ; \beta \mid \alpha \cup \beta \mid \alpha^*}_{\text{composite}}$$

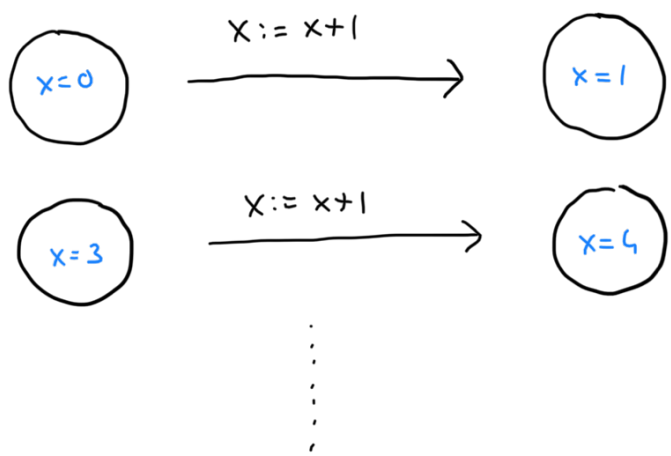
$$\boxed{x := e}$$

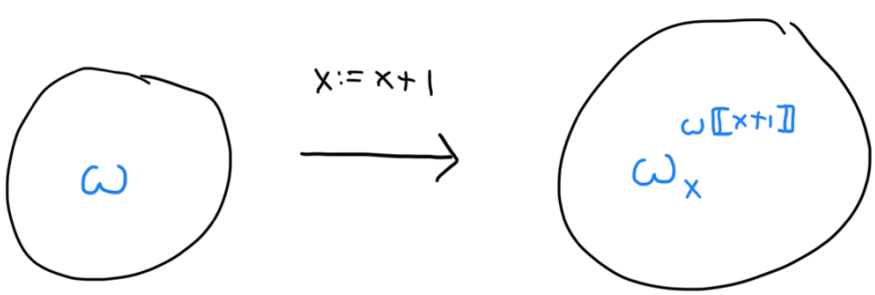
$$[\![x := e]\!] = \{ (\omega, \nu) \mid \omega = \nu \text{ except } \nu(x) = \omega[\![e]\!] \}$$

When is (ω, ν) a valid transition for $x := e$?

- $\sigma(x) = \omega[\![e]\!]$
- $\sigma(y) = \omega(y) \qquad (x \neq y)$

With diagrams!





$$[\![x := e]\!] = \{ (\omega, \omega_x^{\omega[\![e]\!]}) \}$$

$$\boxed{?a}$$

$\omega \in [\![a]\!]$	$\omega \notin [\![a]\!]$
$\omega \circlearrowleft ?a$	$\times$

$$[\![?a]\!] = \{ (\omega, \omega) \mid \omega \in [\![a]\!] \}$$

Why tests?

$\rightarrow$ Constrain nondeterminism

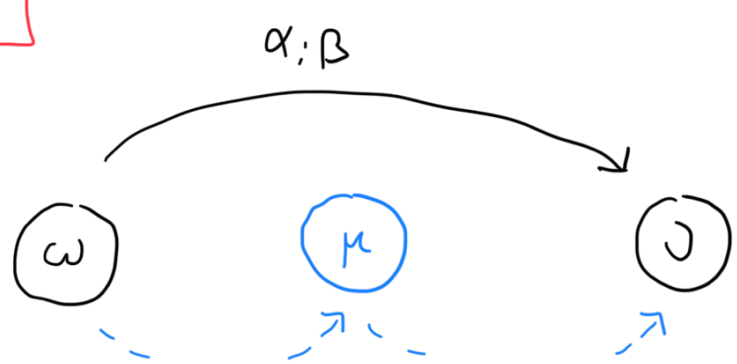
Example: $\underbrace{(?v \leq L;\ a := A)}_{\text{brake}} \cup \underbrace{(a := -B)}_{\text{accelerate}}$

$$\boxed{\{ x' = f(x) \ \& \ Q \}}$$

See later.

Composite Programs

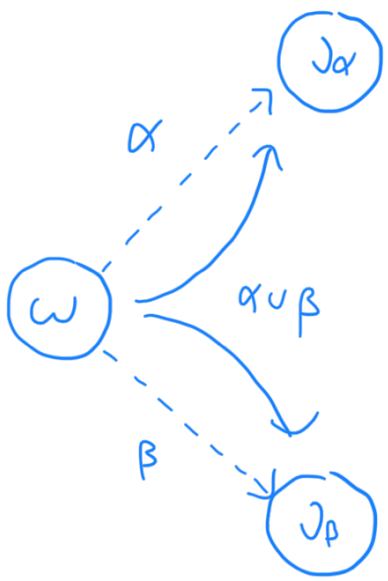
$$\boxed{\alpha ; \beta}$$



α β

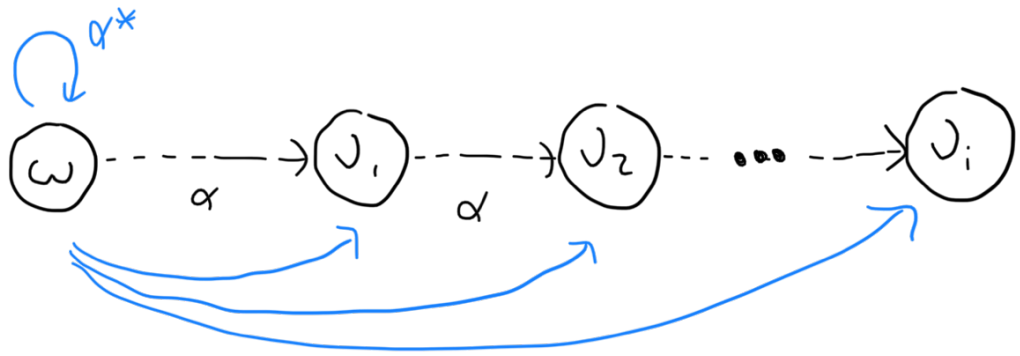
$$[\![\alpha ; \beta]\!] = \{ (\omega, \nu) \mid (\omega, \mu) \in [\![\alpha]\!], (\mu, \nu) \in [\![\beta]\!] \}$$

$$\boxed{\alpha \cup \beta}$$



$$[\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$$

$$\boxed{\alpha^*}$$



$$[\![\alpha^*]\!] = \bigcup_{i \in \mathbb{N}} [\![\alpha^i]\!] \quad \text{where} \quad \begin{cases} \alpha^0 = ?\ \text{true} \\ \alpha^{i+1} = \alpha^i ; \alpha \end{cases}$$

Exercise

What is $[\![x := 0 ; ((x := x+1)^* \cup (x := x-1)^*)]\!]$?

$$\| $$

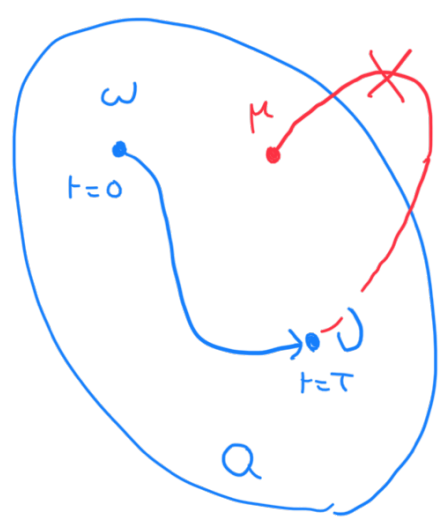
$$\{ (\omega, \omega_x^n) \mid n \in \mathbb{Z} \}$$

Semantics of ODEs

$$\boxed{\{x' = f(x) \;\&\; Q\}}$$

$(\omega, \nu) \in [\![x' = f(x) \;\&\; Q]\!]$

$\iff$ There exists T s.t.



Formally:

$(\omega, \nu) \in [\![\{ x' = e_1, y' = e_2 \ \& \ Q \}]\!]$ iff

there exists $T \geq 0$ s.t.

there exists $\varphi : [0,T] \to \text{State}$ s.t.

- $\varphi(0) = \omega$
- $\varphi(T) = \nu$
- $\varphi'(t)(x) = \varphi(t)[\![e_1]\!]$ $\quad (t \in [0,T])$
- $\varphi'(t)(y) = \varphi(t)[\![e_2]\!]$ $\quad (t \in [0,T])$
- $\varphi(t) \in [\![Q]\!]$ $\quad (t \in [0,T])$

Exercise

$$x = 0 \xrightarrow[\ ?\ ]{\{x' = 1 \ \& \ x \leq 1 \ \vee \ x \geq 2\}} x = 3$$

Modalities

$$[\![\underbrace{[\alpha]P}]\!] = \{ \omega \mid v \in [\![P]\!] \text{ for all } (\omega, v) \in [\![\alpha]\!] \}$$

↳ P holds after all runs of α

$$[\![\underbrace{\langle\alpha\rangle P}]\!] = \{ \omega \mid v \in [\![P]\!] \text{ for } \underline{\text{some}} \ (\omega, v) \in [\![\alpha]\!] \}$$

↳ there exists a run of α after which P holds.

Exercises

$$[\![[?x>0]\, 0=1]\!] = \{ \omega \mid \omega(x) \leq 0 \}$$

Satisfiable

But $x \leq 0 \rightarrow [?x>0]\, 0=1$ valid !

$$[\![\langle ?x>0 \rangle\, 0=1]\!] = \emptyset$$

Unsat

$$[\![[\{ x' = 1 \ \& \ x \leq 5 \}] \ x \leq 5]\!] = \text{State}$$

(valid)

$$[\![\langle \{ x' = 1 \ \& \ x \leq 5 \} \rangle \ 0 = 0]\!] = \{ \omega \mid \omega(x) \leq 5 \}$$

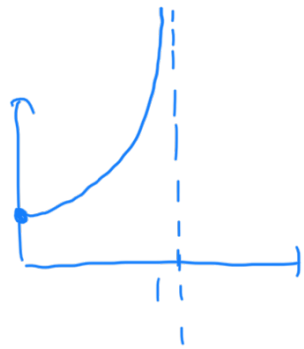
(satisfiable)

BONUS

$$\langle \{ x' = x^2, \ t' = 1 \} \rangle \ t \geq 5$$

Satisfiable but not valid:

$\omega(x) = 1, \quad \omega(t) = 0 \quad \Rightarrow \quad x(t) = \frac{1}{1-t}$



With KeYmaera X

[[illegible] & x≥0] [illegible]