Abstractions of Hybrid Semantics

Patrick Cousot
NYU

ICALP, Wednesday July 6, 2022

Galois connections

Definition of a Galois connection

- $$\langle C,\ \sqsubseteq\rangle \xleftarrow[\alpha]{\gamma}\!\!\xrightarrow{} \langle A,\ \preccurlyeq\rangle \triangleq \begin{cases} \alpha \in C \stackrel{\nearrow}{\longrightarrow} A & \text{is increasing} \\ \gamma \in A \stackrel{\nearrow}{\longrightarrow} C & \text{is increasing} \\ \gamma \circ \alpha & \text{is an upper closure} \\ \alpha \circ \gamma & \text{is a lower closure} \end{cases}$$

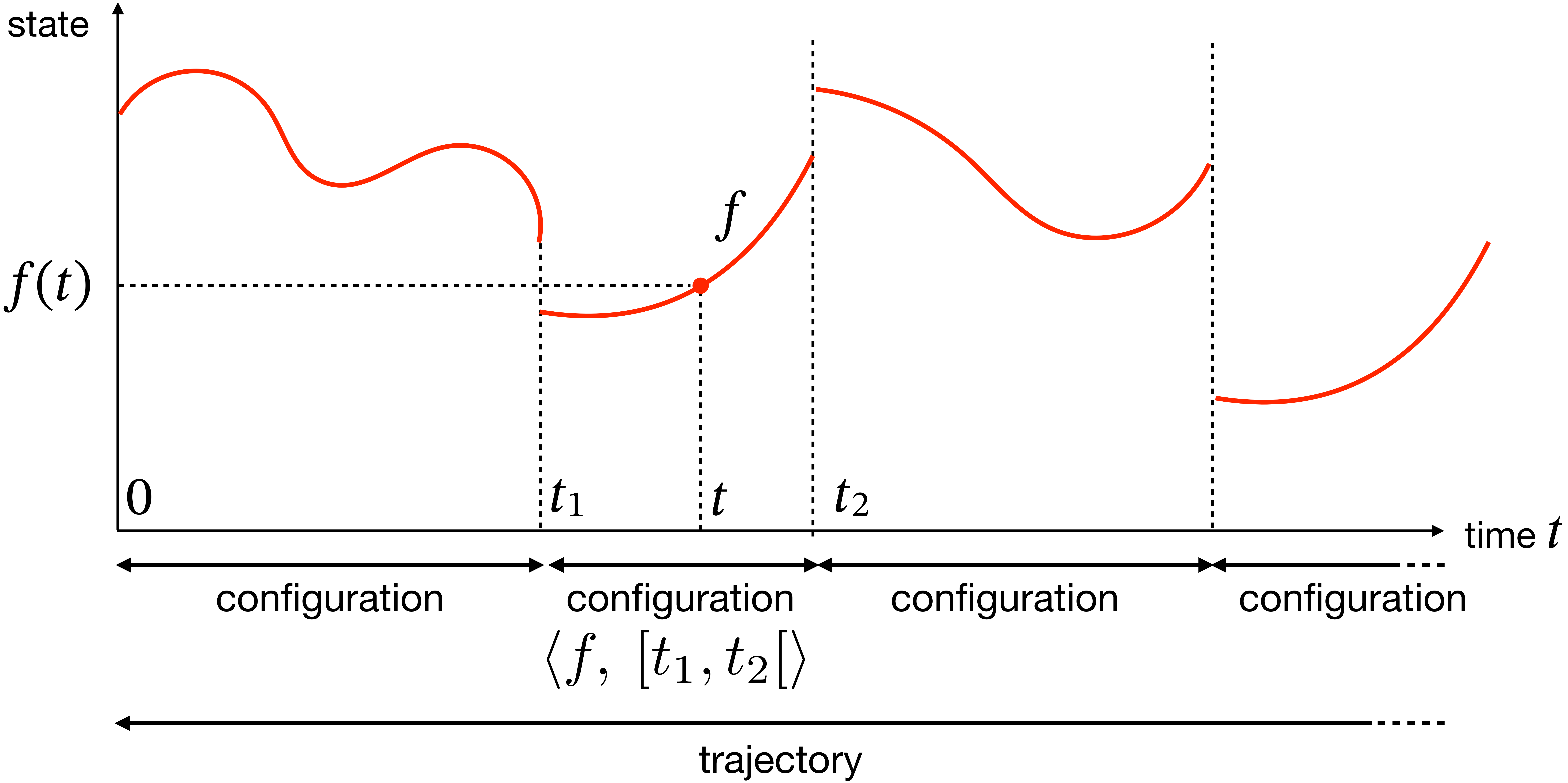
- equivalently

$$\forall x \in C\ .\ \forall y \in A\ .\ \alpha(x) \preccurlyeq y\ \Longleftrightarrow\ x \sqsubseteq \gamma(y)$$

- Galois retraction: α is surjective

Hybrid Semantics

Trajectory


state
$f(t)$
f
0
t_1
t
t_2
time t
configuration
configuration
configuration
configuration
$\langle f,\ [t_1, t_2[\rangle$
trajectory

Time, states, flows, time intervals

- Time: set $\mathbb{R}_{\geqslant 0}$ of all positive reals.
- Set of states: S
- Flows: $f \in \mathsf{F} \triangleq \mathbb{R}_{\geqslant 0} \nrightarrow \mathsf{S}$
- Time intervals: $i \in \mathsf{I} \triangleq \{[t_1, t_2[\mid t_1 \in \mathbb{R}_{\geqslant 0} \wedge t_2 \in \mathbb{R}_{\geqslant 0} \cup \{\infty\} \wedge t_1 + \zeta \leqslant t_2\}$

  (infinitesimal $\zeta > 0$, so non-zeno)

$$\mathsf{b}([t_1, t_2[) \triangleq t_1$$
$$\mathsf{e}([t_1, t_2[) \triangleq t_2$$

Configurations

- Configurations:

$$c \in \mathsf{C} \triangleq \{\langle f,\ i\rangle \in \mathsf{F} \times \mathsf{I} \mid \forall t \in i \,.\, f(t) \in \mathsf{S}\}$$

- Final configurations are closed:

$$\begin{aligned}
\mathsf{cl}([t_1, t_2[) &\triangleq [t_1, t_2] \text{ if } t_2 \neq \infty \\
\mathsf{cl}([t_1, \infty[) &= [t_1, \infty[\\
\mathsf{cl}(\mathsf{I}) &\triangleq \{\mathsf{cl}(i) \mid i \in \mathsf{I}\} \\
c \in \mathsf{cl}(\mathsf{C}) &\triangleq \{\langle f,\ i\rangle \in \mathsf{F} \times \mathsf{cl}(\mathsf{I}) \mid \forall t \in i \,.\, f(t) \in \mathsf{S}\} \\
\mathsf{b}(c) &= \mathsf{b}(i) \\
\mathsf{e}(c) &= \mathsf{e}(i)
\end{aligned}$$

Trajectories, Hybrid semantics

- Trajectories:

$$\mathsf{T}^n_{\mathsf{C}} \triangleq \{\sigma \in [0,n] \to \mathsf{C} \mid \mathsf{b}(\sigma_0) = 0 \wedge \forall i \in [0,n[\;.\;\mathsf{e}(\sigma_i) = \mathsf{b}(\sigma_{i+1}) \wedge \sigma_n \in \mathsf{cl}(\mathsf{C})\}$$

finite trajectories $\sigma \in \mathsf{T}^n_{\mathsf{C}}$ of length $|\sigma| = n+1$, $n \in \mathbb{N}$

$$\mathsf{T}^+_{\mathsf{C}} \triangleq \bigcup_{n\in\mathbb{N}} \mathsf{T}^n_{\mathsf{C}}$$

finite nonempty trajectories

$$\mathsf{T}^\infty_{\mathsf{C}} \triangleq \{\sigma \in \mathbb{N} \to \mathsf{C} \mid \mathsf{b}(\sigma_0) = 0 \wedge \forall i \in \mathbb{N}\;.\;\mathsf{e}(\sigma_i) = \mathsf{b}(\sigma_{i+1})\}$$

infinite trajectories $\sigma \in \mathsf{T}^\infty_{\mathsf{C}}$ of length $|\sigma| = \infty$

$$\mathsf{T}^{+\infty}_{\mathsf{C}} \triangleq \mathsf{T}^+_{\mathsf{C}} \cup \mathsf{T}^\infty_{\mathsf{C}} \qquad \text{trajectories} \tag{15}$$

- Hybrid semantics:

$$\mathcal{S}_{\mathsf{C}} \in \wp(\mathsf{T}^{+\infty}_{\mathsf{C}})$$

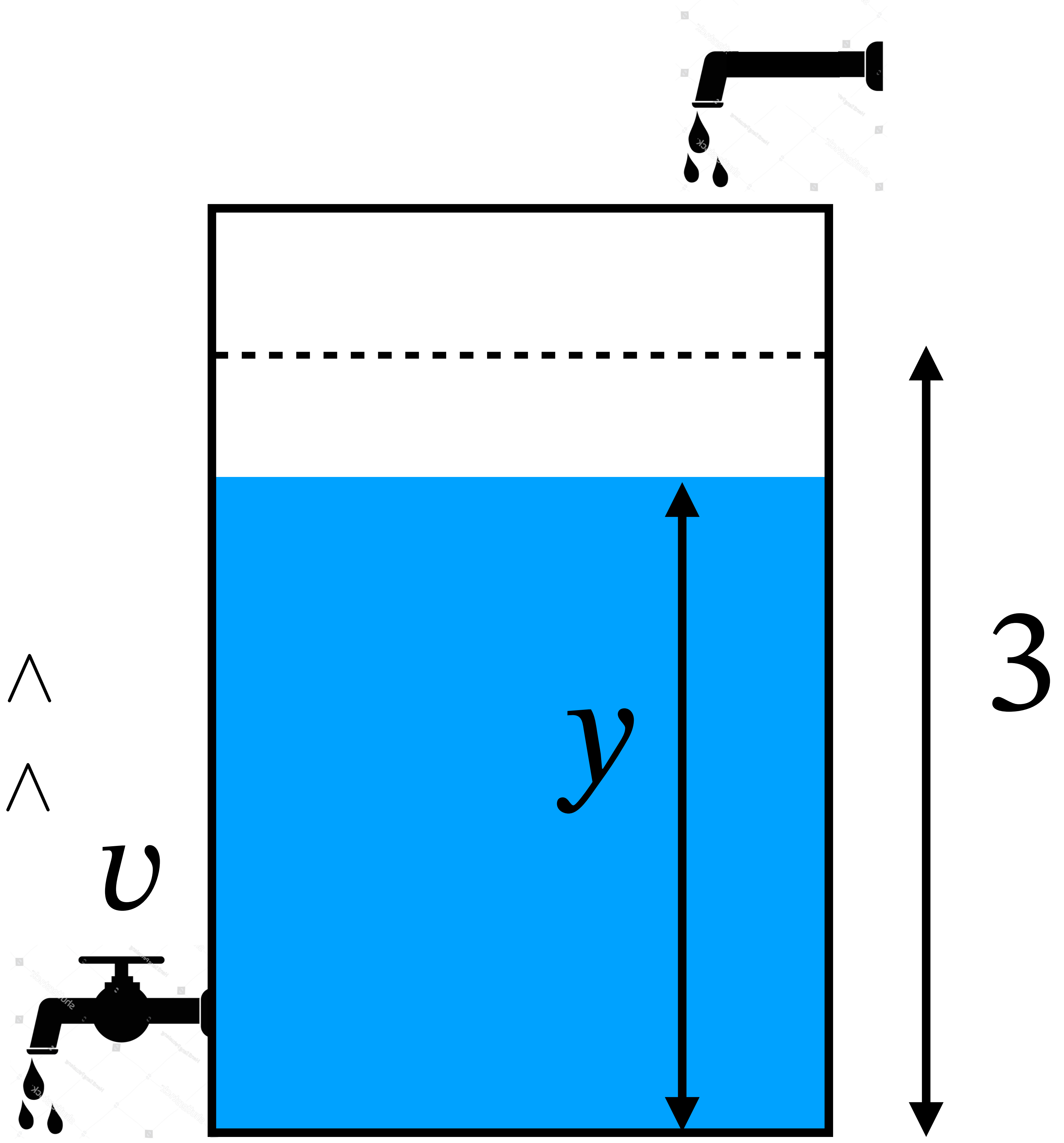
Example: water tank specification

y $\quad$ v

$$s \in \mathsf{S} \triangleq \mathbb{R} \times \{open, shut\}$$

$$\mathcal{S}^1 \triangleq \{\sigma \in \{0\} \to \mathsf{C} \mid \mathsf{e}(\sigma_0) = \infty \wedge P(\sigma_0)\}$$

$$\begin{aligned}P(\sigma) \triangleq \forall t \in \mathbb{R}_{\geqslant 0} \;.\; 0 \leqslant \sigma(t).y \leqslant 3 \wedge \forall t_2 > t_1 \geqslant 0 \;.\\ \forall t \in [t_1, t_2] \;.\; \sigma(t).v = open \Longrightarrow \sigma(t_1).y > \sigma(t_2).y \wedge\\ \forall t \in [t_1, t_2] \;.\; \sigma(t).v = shut \Longrightarrow \sigma(t_1).y < \sigma(t_2).y \wedge\\ \forall t \in \mathbb{R}_{\geqslant 0} \;.\; \sigma(t).y = 0 \Longrightarrow \sigma(t + \zeta).y > 0\end{aligned}$$



Thomas A. Henzinger and Pei-Hsin Ho. A note on abstract interpretation strategies for hybrid automata. In *Hybrid Systems*, volume 999 of *Lecture Notes in Computer Science*, pages 252–264. Springer, 1994.

Time evolution law abstraction (as in dynamic systems)

- Duration:

$$\llbracket\sigma\rrbracket \triangleq \sum_{k=0}^{n} \mathsf{e}(\sigma_i) - \mathsf{b}(\sigma_i) = \mathsf{e}(\sigma_n) \qquad \text{when} \quad \sigma \in \mathsf{T}_{\mathsf{C}}^{n} \tag{16}$$

$$\triangleq \sum_{k=0}^{\infty} \mathsf{e}(\sigma_i) - \mathsf{b}(\sigma_i) = \infty \qquad \text{when} \quad \sigma \in \mathsf{T}_{\mathsf{C}}^{\infty} \qquad \text{(nonzeno hypothesis)}$$

- Time evaluation law (in dynamic systems theory): $\alpha_{tr}(\sigma) \in \mathbb{R}_{\geqslant 0} \to \mathsf{S}$

$$\mathsf{dom}(\alpha_{tr}(\sigma)) \triangleq [0, \llbracket\sigma\rrbracket] \qquad \text{(by convention, excluding } \infty \text{ if } \llbracket\sigma\rrbracket = \infty)$$

$$\alpha_{tr}(\sigma)(t) \triangleq f(t) \text{ such that } \exists k \in [0, |\sigma|[\,.\, \sigma_k = \langle f,\ i\rangle \wedge t \in i \tag{17}$$

$$\sigma_t \triangleq \alpha_{tr}(\sigma)(t) \qquad \text{(abbreviated notation)}$$

- Abstraction:

$$\langle \wp(\mathsf{T}_{\mathsf{C}}^{+\infty}),\ \subseteq\rangle \xleftrightarrow[\alpha_{tr}]{\gamma_t} \langle \wp(\mathbb{R}_{\geqslant 0} \to \mathsf{S}),\ \subseteq\rangle$$

Hybrid transition system

Hybrid transition system

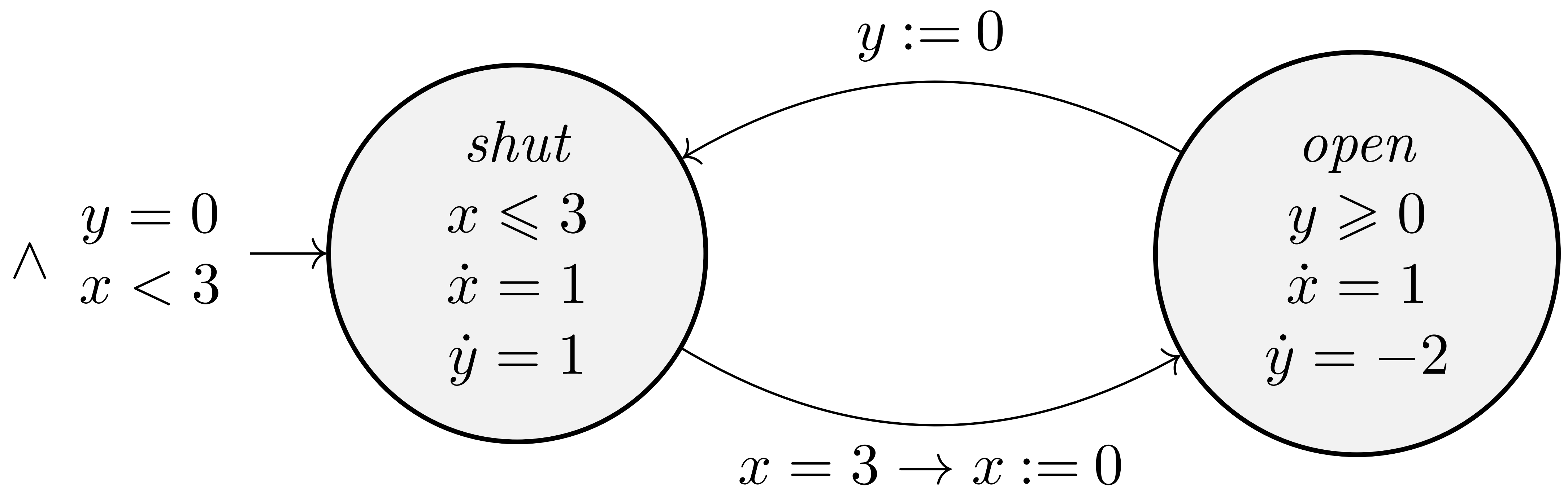
- Transition system: $\langle \mathsf{C},\ \mathsf{C}^0,\ \tau \rangle$
  - configurations C
  - initial configurations C^0
  - $\tau \in \wp(\mathsf{C} \times (\mathsf{C} \cup \mathsf{cl}(\mathsf{C})))$

- initial configurations $\qquad \mathsf{C}^0 \subseteq \{c \in \mathsf{C} \mid \mathsf{b}(c) = 0\}$ (22)

  consecutiveness $\qquad \forall \langle c,\ c' \rangle \in \tau \,.\, c \in \mathsf{C} \wedge \mathsf{e}(c) = \mathsf{b}(c')$

  closeness of final configurations $\qquad \forall c \,.\, (\forall c' \,.\, \langle c,\ c' \rangle \notin \tau) \iff c \in \mathsf{cl}(\mathsf{C})$

Example: water tank automaton



$$\mathsf{S} \triangleq \{open, shut\} \times \mathbb{R} \times \mathbb{R}$$

$$\mathsf{C}^{shut} \triangleq \{\langle f,\ [t_1, t_2[\rangle \mid \exists x, y\ .\ \forall t \in [t_1, t_2]\ .\ f(t) = \langle shut,\ x(t),\ y(t)\rangle \wedge (t = t_1 \Longrightarrow y(t) = 0) \wedge x(t) \leqslant 3 \wedge (x(t) = 3 \Longrightarrow t = t_2) \wedge \dot{x}(t) = 1 \wedge \dot{y}(t) = 1\}$$

$$\mathsf{C}^{open} \triangleq \{\langle f,\ [t_1, t_2[\rangle \mid \exists x, y\ .\ \forall t \in [t_1, t_2]\ .\ f(t) = \langle open,\ x(t),\ y(t)\rangle \wedge (t = t_1 \Longrightarrow x(t) = 0) \wedge y(t) \geqslant 0 \wedge (y(t) = 0 \Longrightarrow t = t_2) \wedge \dot{x}(t) = 1 \wedge \dot{y}(t) = -2\}$$

$$\mathsf{C} \triangleq \mathsf{C}^{shut} \cup \mathsf{C}^{open}$$

$$\mathsf{C}^0 \triangleq \{\langle f,\ [0, t[\rangle \in \mathsf{C}^{shut} \mid t > 0 \wedge \exists x < 3\ .\ f(0) = \langle shut,\ x,\ 0\rangle\}$$

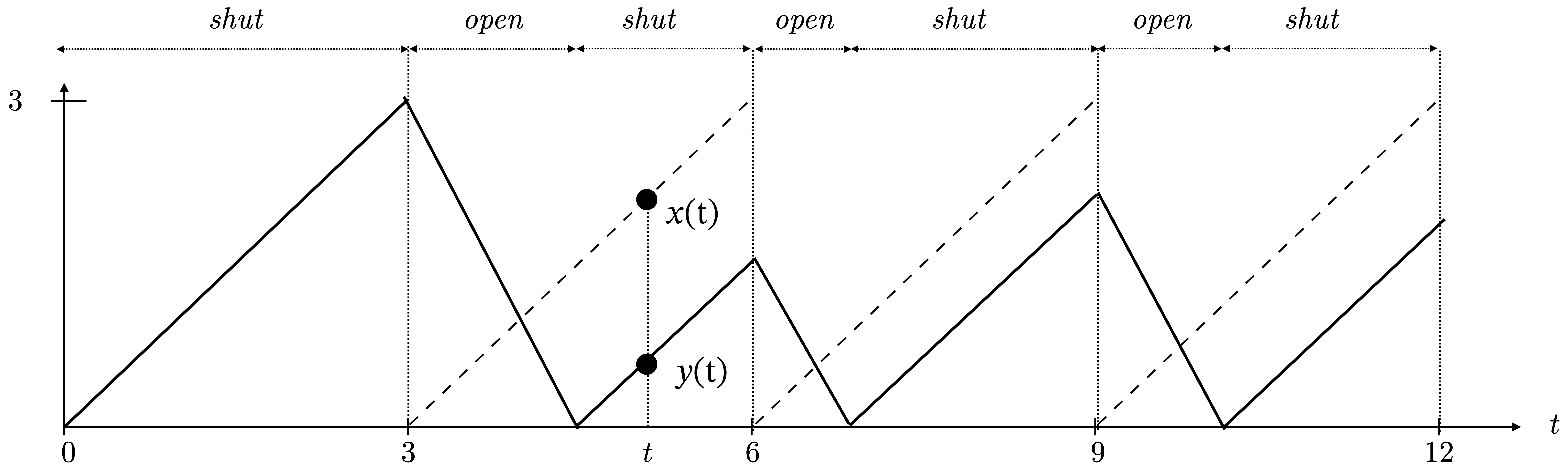
$$\tau^2 \triangleq (\mathsf{C}^{shut} \times \mathsf{C}^{open}) \cup (\mathsf{C}^{open} \times \mathsf{C}^{shut}) \text{ as restricted by } (22) \tag{25}$$

Hybrid semantics generated by a transition system

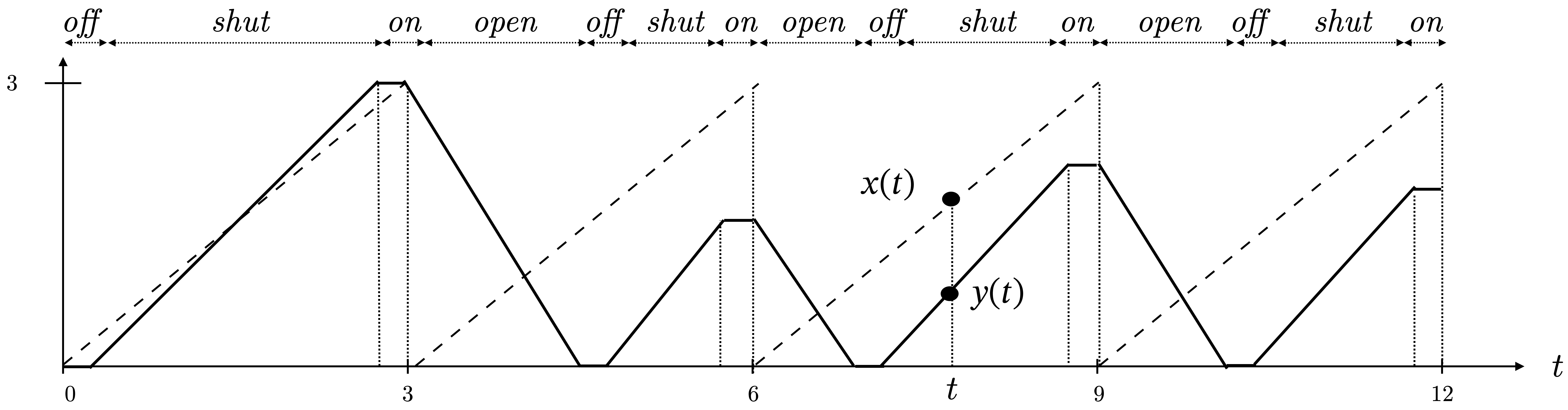
- $\llbracket\langle \mathsf{C},\ \mathsf{C}^0,\ \tau\rangle\rrbracket$ abbreviated $\llbracket\tau\rrbracket$

- $$\begin{aligned}
\llbracket\tau\rrbracket^n &\triangleq \{\sigma \in \mathsf{T}^n_{\mathsf{C}} \mid \sigma_0 \in \mathsf{C}^0 \wedge \forall i \in [0, n[\ .\ \langle\sigma_i,\ \sigma_{i+1}\rangle \in \tau \wedge \forall c\ .\ \langle\sigma_n,\ c\rangle \notin \tau\}\\
\llbracket\tau\rrbracket^+ &\triangleq \bigcup_{n\in\mathbb{N}} \llbracket\tau\rrbracket^n\\
\llbracket\tau\rrbracket^\infty &\triangleq \{\sigma \in \mathsf{T}^\infty_{\mathsf{C}} \mid \sigma_0 \in \mathsf{C}^0 \wedge \forall i \in \mathbb{N}\ .\ \langle\sigma_i,\ \sigma_{i+1}\rangle \in \tau\}\\
\llbracket\tau\rrbracket &\triangleq \llbracket\tau\rrbracket^+ \cup \llbracket\tau\rrbracket^\infty
\end{aligned} \tag{23}$$

Example: trajectory of the water tank automaton



Example: water tank implementation



State/configuration based correspondences between hybrid semantics

Relation between states and configurations

- Relation between states:

$$r \in \mathbb{R}_{\geqslant 0} \rightarrow \wp(\mathsf{S} \times \overline{\mathsf{S}})$$

- Relation between configurations:

$$\gamma(r) \triangleq \{\langle\langle f,\, i\rangle,\, \langle \overline{f},\, \overline{i}\rangle\rangle \mid i \cap \overline{i} \neq \emptyset \wedge \forall t \in i \cap \overline{i} \,.\, \langle f(t),\, \overline{f}(t)\rangle \in r(t)\}$$

- Equivalence:

$$\alpha(R) \triangleq \boldsymbol{\lambda} t \bullet \{\langle f(t),\, \overline{f}(t)\rangle \mid \exists i, \overline{i} \,.\, t \in i \cap \overline{i} \wedge \langle\langle f,\, i\rangle,\, \langle \overline{f},\, \overline{i}\rangle\rangle \in R\}$$

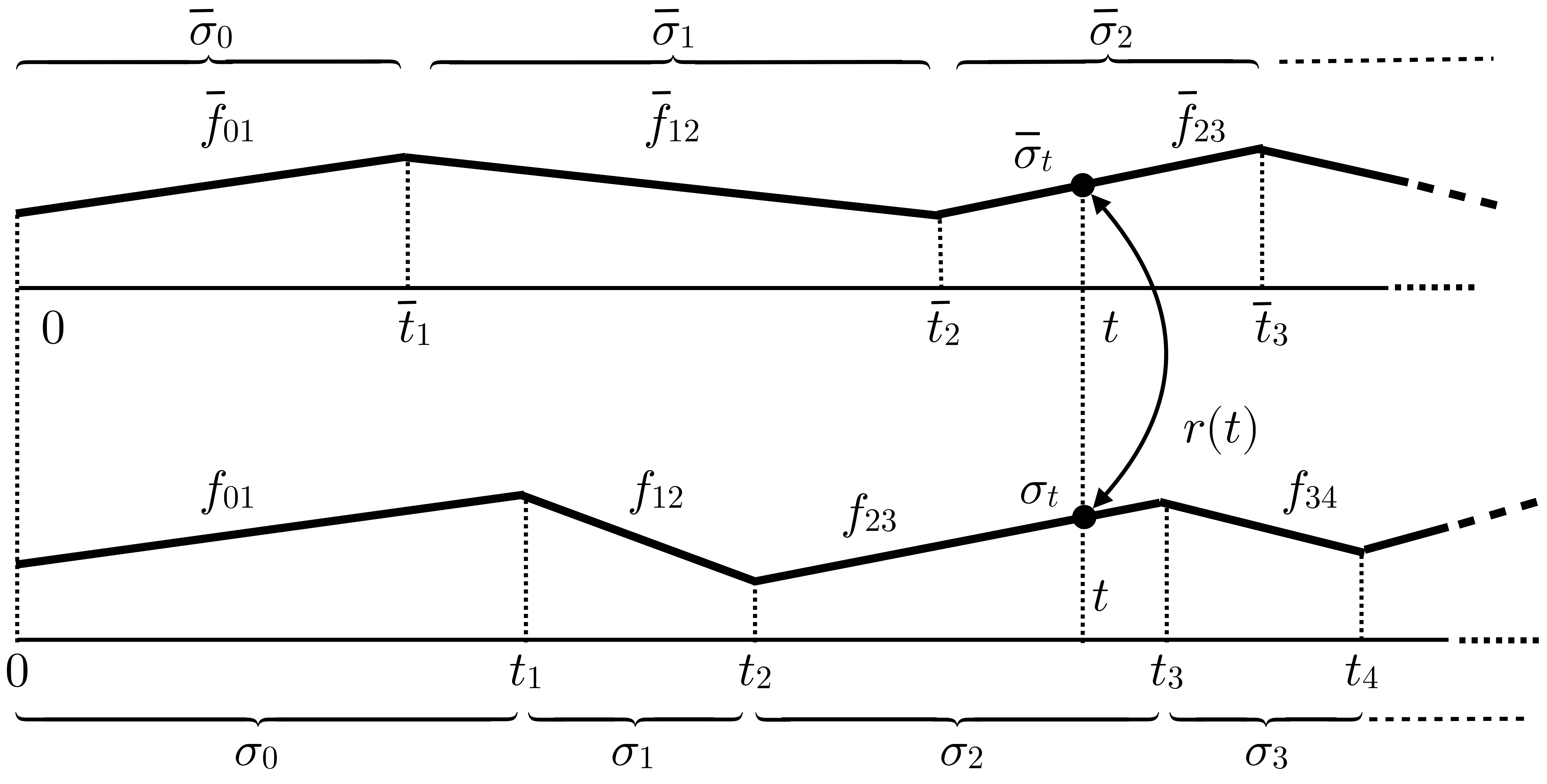
$$\mathsf{R}_{\mathsf{C}} \triangleq \{R \in \wp(\mathsf{C} \times (\mathsf{C} \cup \mathsf{cl}(\mathsf{C}))) \mid \forall \langle\langle f,\, i\rangle,\, \langle \overline{f},\, \overline{i}\rangle\rangle \in R \,.\, i \cap \overline{i} \neq \emptyset\}$$

$$\langle \mathsf{R}_{\mathsf{C}},\, \subseteq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle \mathbb{R}_{\geqslant 0} \rightarrow \wp(\mathsf{S} \times \mathsf{S}),\, \dot{\subseteq}\rangle$$

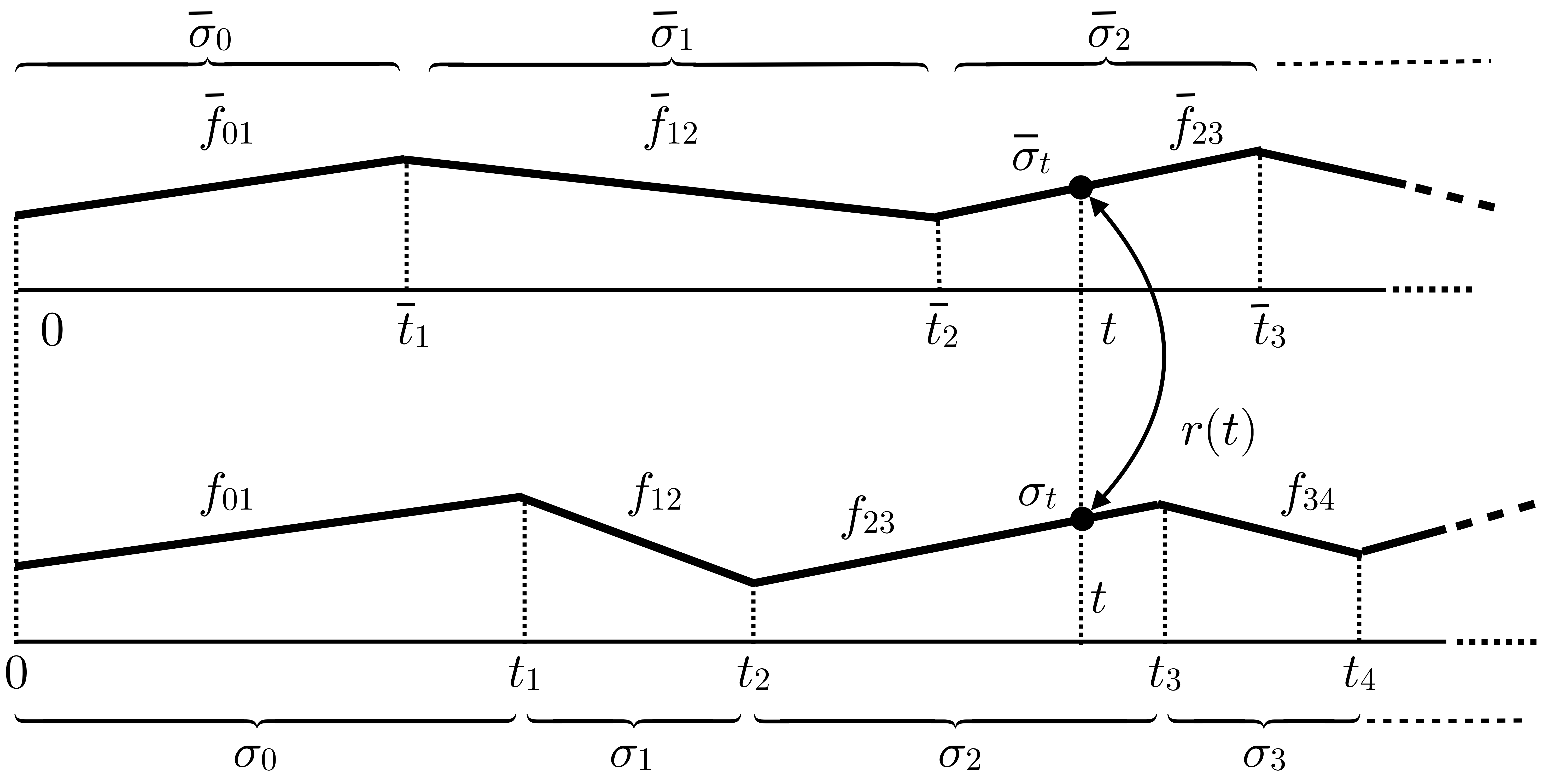
Relations between trajectories (using states)

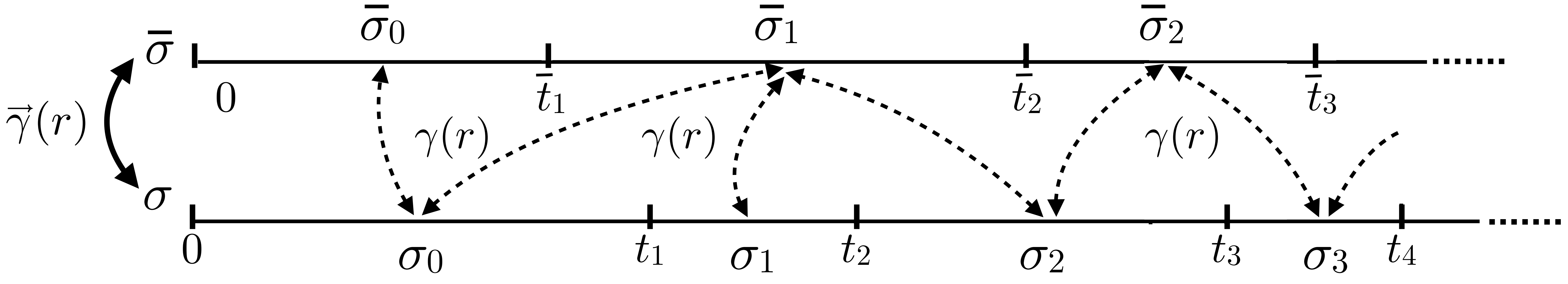
- $\vec{\gamma}(r) \triangleq \{\langle\sigma,\ \overline{\sigma}\rangle \mid \forall t \in [0, \min([\![\sigma]\!], [\![\overline{\sigma}]\!])[\ .\ \langle\sigma_t,\ \overline{\sigma}_t\rangle \in r(t)\}$

- Example:



Relations between trajectories (using configurations)

- 



Relations between trajectories (using configurations)

- same correspondance between trajectories using configurations:

$$\vec{\gamma}(r) \triangleq \vec{\gamma}_c(r) \cap \vec{\gamma}_a(r)$$

$$\vec{\gamma}_c(r) \triangleq \{\langle\sigma,\,\overline{\sigma}\rangle \mid \forall j < |\sigma| \,.\, (\mathsf{e}(\sigma_j) \leqslant [\![\overline{\sigma}]\!]) \Longrightarrow (\exists k < |\overline{\sigma}| \,.\, \langle\sigma_j,\,\overline{\sigma}_k\rangle \in \gamma(r))\}$$

$$\vec{\gamma}_a(r) \triangleq \{\langle\sigma,\,\overline{\sigma}\rangle \mid \forall k < |\overline{\sigma}| \,.\, (\mathsf{e}(\overline{\sigma}_k) \leqslant [\![\sigma]\!]) \Longrightarrow (\exists j < |\sigma| \,.\, \langle\sigma_j,\,\overline{\sigma}_k\rangle \in \gamma(r))\}$$

- abstraction:

$$\langle\wp(\mathsf{T}_{\mathsf{C}}^{+\infty} \times \mathsf{T}_{\overline{\mathsf{C}}}^{+\infty}),\ \subseteq\rangle \xleftrightarrow[\vec{\alpha}]{\vec{\gamma}} \langle\mathbb{R}_{\geqslant 0} \to \wp(\mathsf{S} \times \overline{\mathsf{S}}),\ \dot{\subseteq}\rangle$$

Relation between hybrid semantics

- $\vec{\vec{\gamma}}(R) \triangleq \{\langle T,\ \overline{T}\rangle \mid T \subseteq \mathsf{pre}[R]\overline{T}\}$
  $= \{\langle T,\ \overline{T}\rangle \mid \forall \sigma \in T\ .\ \exists \overline{\sigma} \in \overline{T}\ .\ \langle \sigma,\ \overline{\sigma}\rangle \in R\}$

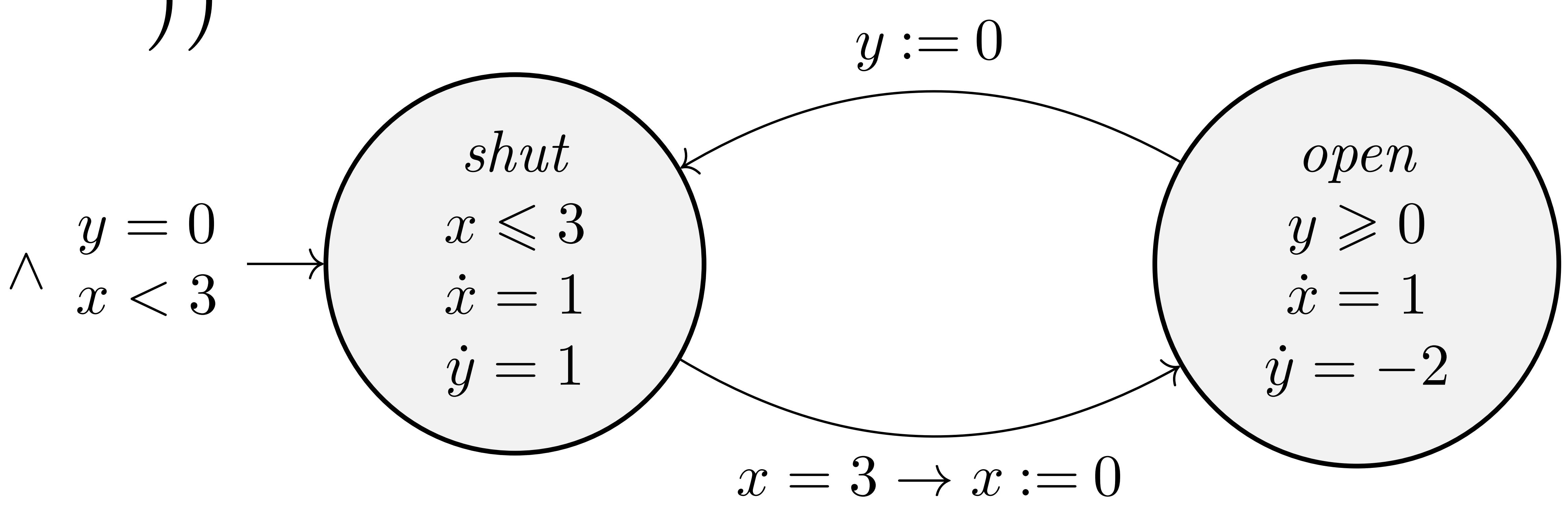
- abstraction:

$$\langle\{\langle T,\ \overline{T}\rangle \in \wp(\mathsf{T}_{\mathsf{c}}^{+\infty}) \otimes \wp(\mathsf{T}_{\overline{\mathsf{c}}}^{+\infty}) \mid \overline{T} = \emptyset \Longrightarrow T = \emptyset\},\ \supseteq\rangle \xleftarrow[\vec{\vec{\alpha}}]{\vec{\vec{\gamma}}} \langle\wp(\mathsf{T}_{\mathsf{c}}^{+\infty} \times \mathsf{T}_{\overline{\mathsf{c}}}^{+\infty}),\ \supseteq\rangle$$

Example: The water tank automaton is a state-based refinement of the specification

- $r^{(39)}(t) \triangleq \{\langle\langle v,\ x,\ y\rangle,\ \langle v,\ y\rangle\rangle \mid v \in \{shut, open\} \wedge x, y \in \mathbb{R}\}$

- $\langle [\![\tau^2]\!],\ \mathcal{S}^1\rangle \in \vec{\gamma}(\vec{\gamma}(r^{(39)}))$



  - y is always between 0 and 3
  - if the valve is shut the level y goes up
  - if the valve is open the level y goes down
  - cannot stay zero more than ς

Correspondance between hybrid semantics defined by a correspondance between transition systems

Examples for discrete trace semantics

- Homomorphisms
- Simulations
- Bisimulations
- Preservation and progress (for type soundness)

and for hybrid semantics

- Discretization/sampling

Simulation

Notations

- empty configuration:

$$\varepsilon \triangleq \langle\emptyset, \emptyset\rangle \qquad \mathsf{b}(\varepsilon) \triangleq +\infty \text{ and } \mathsf{e}(\varepsilon) = -\infty$$

- consecutive configurations concatenation:

$$\langle f,\ i\rangle \mathbin{;} \langle f',\ i'\rangle \triangleq \langle f'',\ i \cup i'\rangle \text{ where } \begin{cases} f''(t) = f(t) \text{ when } t \in i \\ f''(t) = f'(t) \text{ when } t \in i' \end{cases}$$

$$\langle f,\ i\rangle \mathbin{;} \varepsilon = \varepsilon \mathbin{;} \langle f,\ i\rangle = \langle f,\ i\rangle$$

- configuration slice:

$$\langle f,\ i\rangle(\!|t_1, t_2|\!) \triangleq \langle f,\ i \cap [t_1, t_2]\rangle \quad \text{where} \quad \mathsf{b}(i \cap [t_1, t_2]) + \zeta \leqslant \mathsf{e}(i \cap [t_1, t_2])$$

$$\langle f,\ i\rangle(\!|t_1, t_2(\!| \triangleq \langle f,\ i \cap [t_1, t_2[\rangle \quad \mathsf{b}(i \cap [t_1, t_2[) + \zeta \leqslant \mathsf{e}(i \cap [t_1, t_2[)$$

$$\varepsilon(\!|t_1, t_2|\!) \triangleq \varepsilon(\!|t_1, t_2(\!| \triangleq \varepsilon.$$

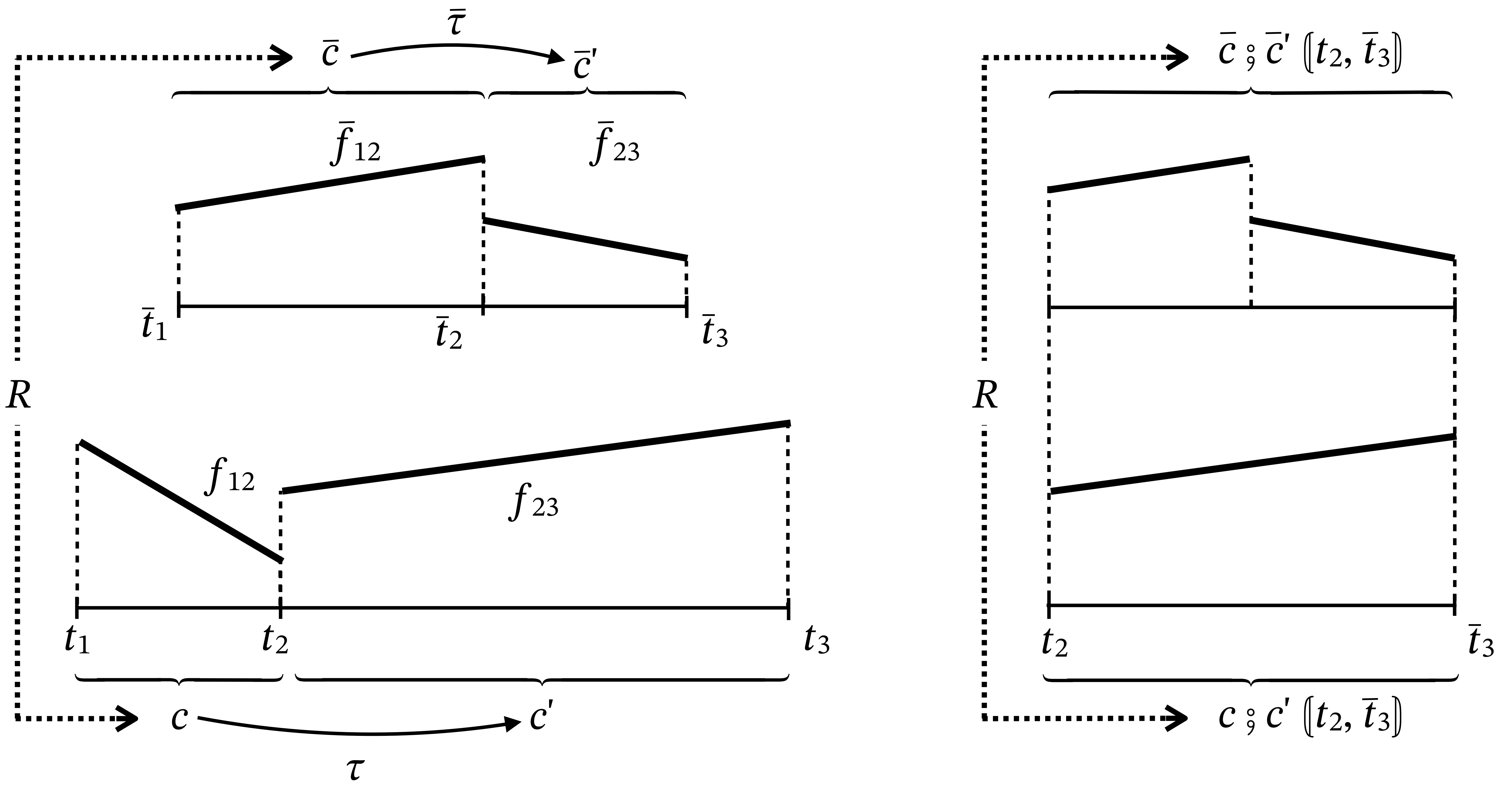
Discrete simulation

$$\forall c, \overline{c}, c' \,.\, \exists \overline{c}' \,.\, (\langle c,\ \overline{c}\rangle \in R \wedge (\langle c,\ c'\rangle \in \tau\,) \Longrightarrow$$
$$(\langle \overline{c},\ \overline{c}'\rangle \in \overline{\tau}\ \wedge\ \langle c',\ \overline{c}'\rangle \in\ R)$$

Robin Milner. An algebraic definition of simulation between programs. In *Proceedings IJCAI 1971*, pages 481–489, 1971.

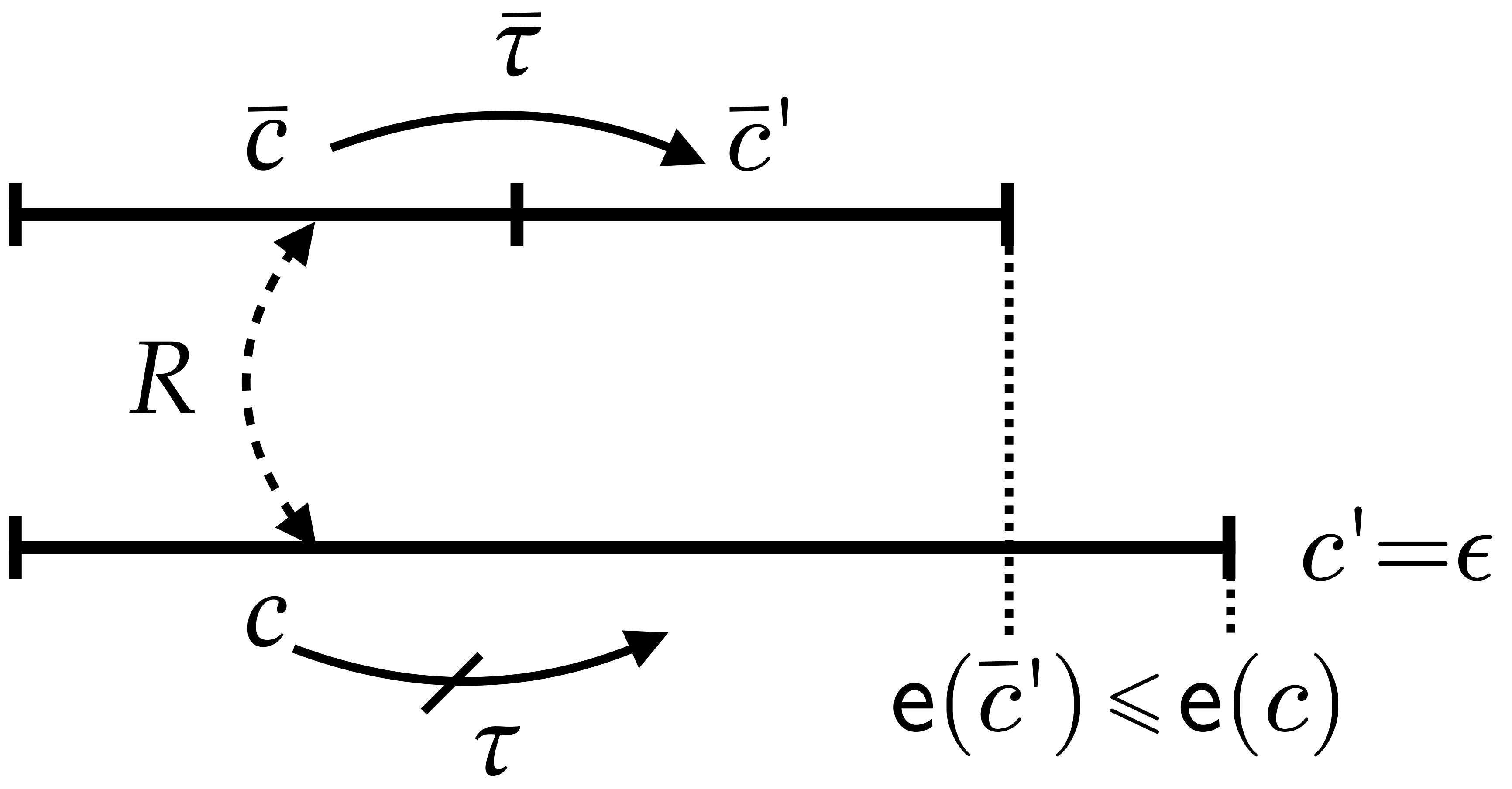
Asynchronous hybrid simulation

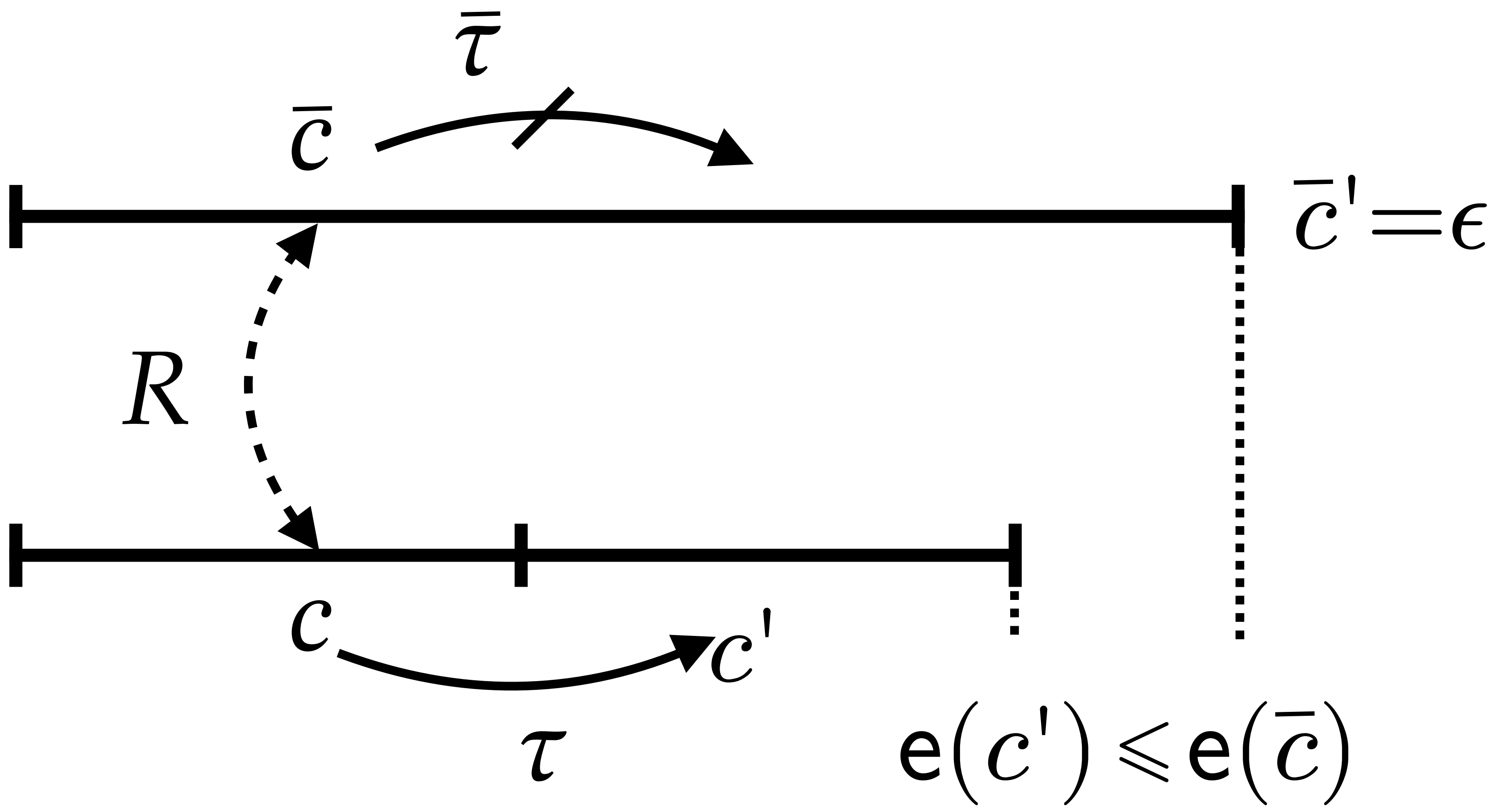
$$\forall c, \overline{c}, c' \,.\, \exists \overline{c}' \,.\, (\langle c,\ \overline{c}\rangle \in R \wedge (\langle c,\ c'\rangle \in \tau \vee c' = \varepsilon)) \Longrightarrow$$
$$(((\langle \overline{c},\ \overline{c}'\rangle \in \overline{\tau} \vee \overline{c}' = \varepsilon) \wedge \langle c \,\mathbin{;}\, c' (\!| \min(\mathsf{b}(c'), \mathsf{b}(\overline{c}')), \min(\mathsf{e}(c'), \mathsf{e}(\overline{c}')) |\!),$$
$$\overline{c} \,\mathbin{;}\, \overline{c}' (\!| \min(\mathsf{b}(c'), \mathsf{b}(\overline{c}')), \min(\mathsf{e}(c'), \mathsf{e}(\overline{c}')) |\!) \rangle \in R)$$



Asynchronous hybrid simulation

$$\forall c, \overline{c}, c' \,.\, \exists \overline{c}' \,.\, (\langle c,\ \overline{c}\rangle \in R \wedge (\langle c,\ c'\rangle \in \tau \vee c' = \varepsilon)) \Longrightarrow$$
$$((\langle \overline{c},\ \overline{c}'\rangle \in \overline{\tau} \vee \overline{c}' = \varepsilon) \wedge \langle c \,⨾\, c'(\!|\min(\mathsf{b}(c'), \mathsf{b}(\overline{c}')), \min(\mathsf{e}(c'), \mathsf{e}(\overline{c}'))|\!),$$
$$\overline{c} \,⨾\, \overline{c}'(\!|\min(\mathsf{b}(c'), \mathsf{b}(\overline{c}')), \min(\mathsf{e}(c'), \mathsf{e}(\overline{c}'))|\!)\rangle \in R)$$



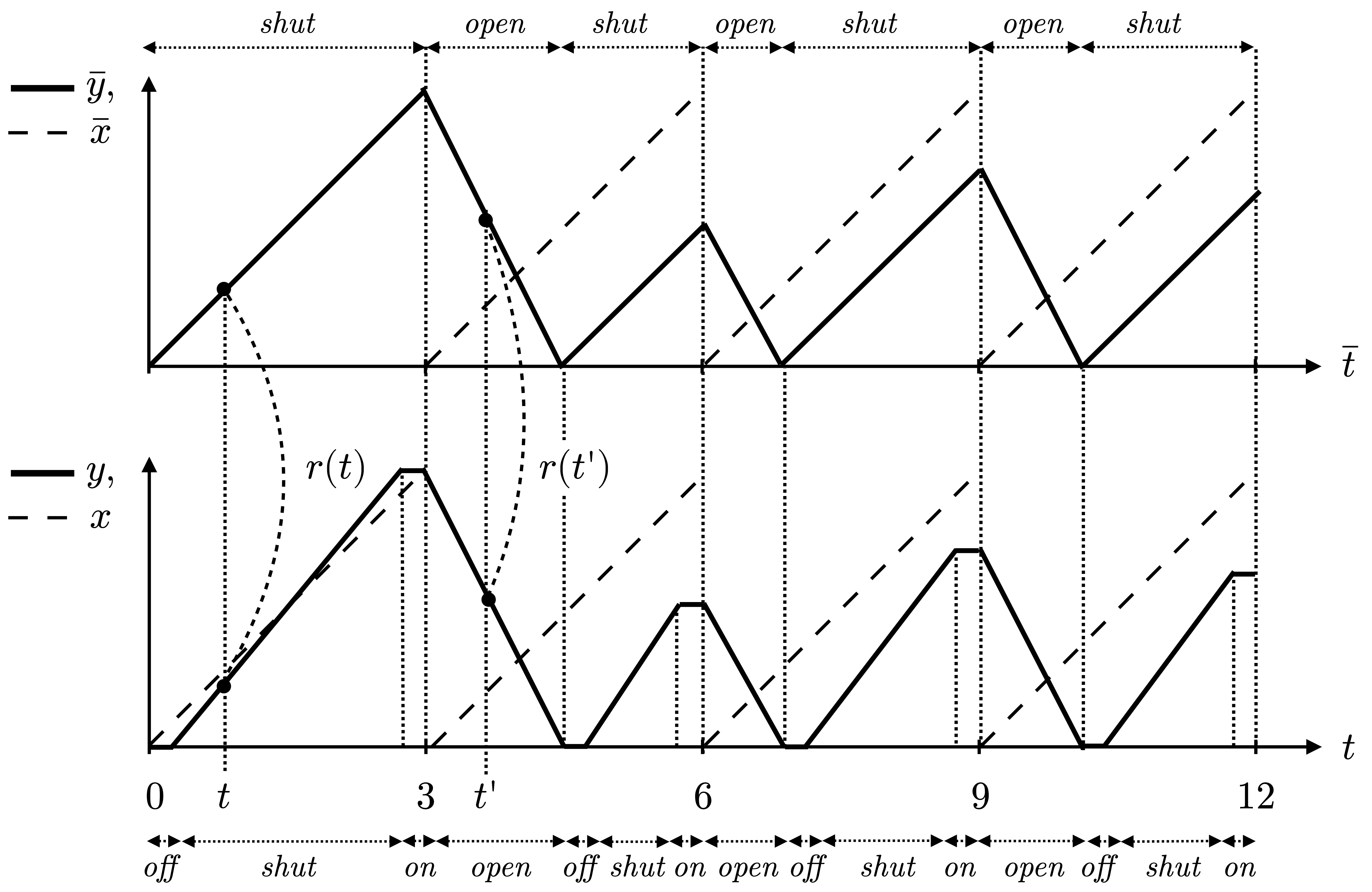


Synchronous hybrid simulation

- well-nesting: the abstract time line is included in the concrete time line

$$\forall c, \overline{c}, c' \;.\; \exists \overline{c}' \;.\; (\langle c,\ \overline{c}\rangle \in R \wedge (\langle c,\ c'\rangle \in \tau)) \Longrightarrow$$
$$((\langle \overline{c},\ \overline{c}'\rangle \in \overline{\tau} \vee \overline{c}' = \varepsilon) \wedge \langle c',\ \overline{c}'(\!| \mathsf{b}(c'), \mathsf{e}(c') |\!)\rangle \in R)$$

- example:



Simulation between transitions extends to hybrid semantics

Theorem 4. *If the timed relation r between states in (29) is such that its extension $\gamma(r)$ to configurations in (30) is a simulation (51) between* $\langle \mathsf{C},\ \mathsf{C}^0,\ \tau\rangle$ *and* $\langle \overline{\mathsf{C}},\ \overline{\mathsf{C}}^0,\ \overline{\tau}\rangle$ *satisfying the* initialization hypothesis

$$\forall c \in \mathsf{C}^0\ .\ \exists \overline{c} \in \overline{\mathsf{C}}^0\ .\ \langle c,\ \overline{c}\rangle \in \gamma(r)$$

and *the* blocking hypothesis

$$\forall c, \overline{c}\ .\ (\langle c,\ \overline{c}\rangle \in \gamma(r) \wedge \forall c'\ .\ \langle c,\ c'\rangle \notin \tau) \Longrightarrow (\forall \overline{c}'\ .\ \langle \overline{c},\ \overline{c}'\rangle \notin \overline{\tau})$$

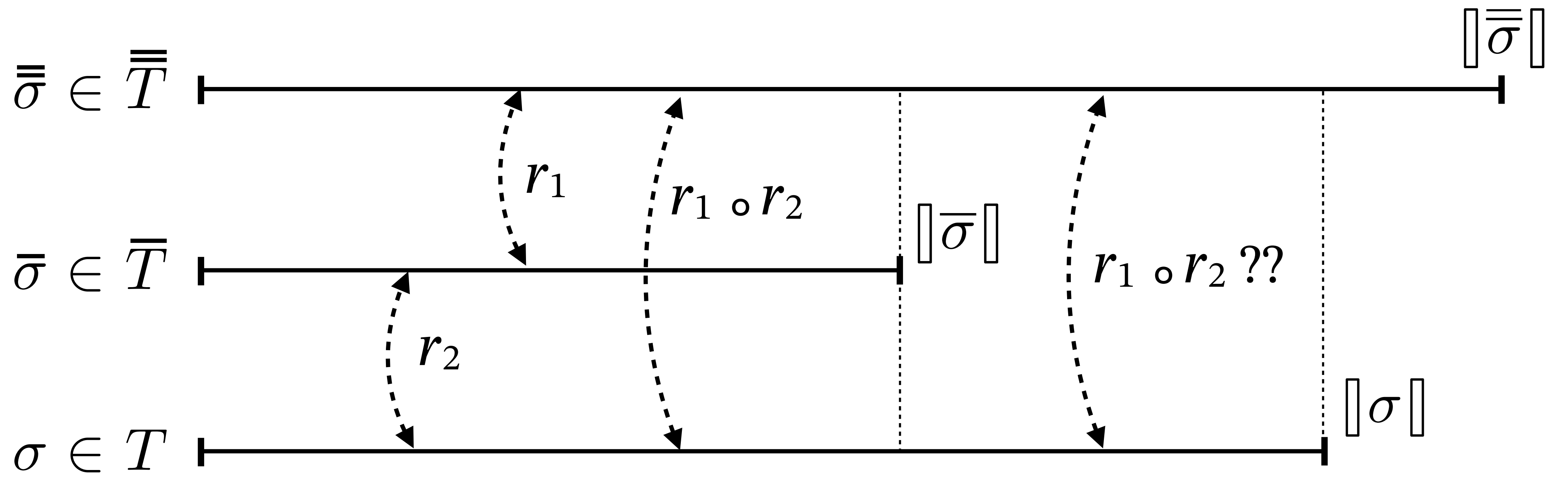
then

$$\langle [\![\tau]\!],\ [\![\overline{\tau}]\!]\rangle \in \vec{\gamma}(\vec{\gamma}(r))$$

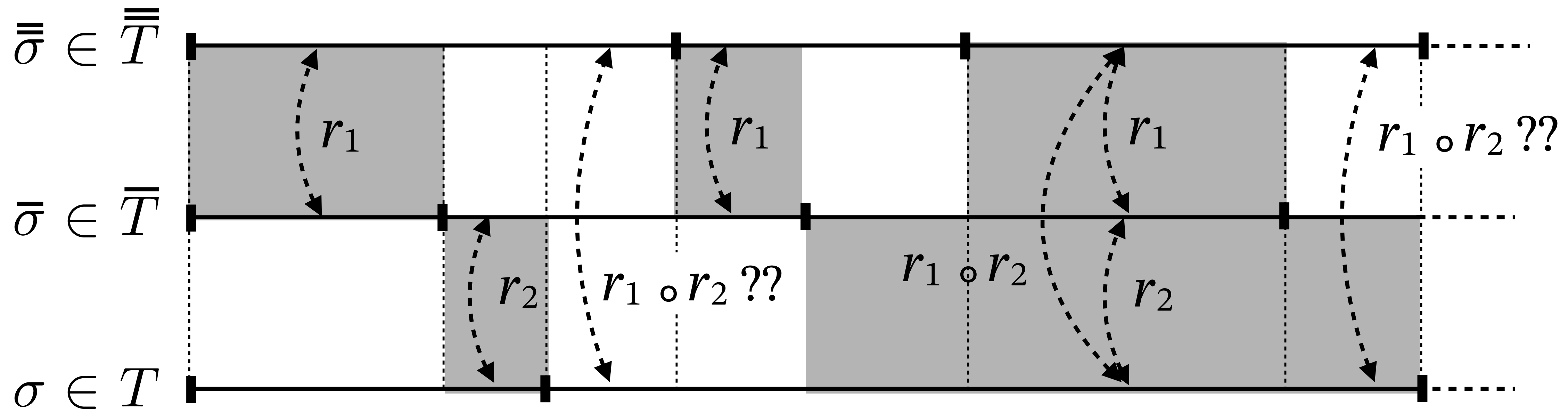
(*that is, by* (37), $\forall \sigma \in [\![\tau]\!]\ .\ \exists \overline{\sigma} \in [\![\overline{\tau}]\!]\ .\ \langle \sigma,\ \overline{\sigma}\rangle \in \vec{\gamma}(r)$ *and so, by* (34), $\forall t \in [0, \min([\![\sigma]\!], [\![\overline{\sigma}]\!])[\cap \mathsf{dom}(r)\ .\ \langle \sigma_t,\ \overline{\sigma}_t\rangle \in r(t)$).

Asynchronous simulations may not compose

- We may have $\langle T,\ \overline{T}\rangle \in \vec{\vec{\gamma}}(\vec{\gamma}_c(r_1))$ and $\langle \overline{T},\ \overline{\overline{T}}\rangle \in \vec{\vec{\gamma}}(\vec{\gamma}_c(r_2))$ but not $\langle T,\ \overline{\overline{T}}\rangle \in \vec{\vec{\gamma}}(\vec{\gamma}_c(r_1 \circ r_2))$



Non-composition due to short intermediate trajectory duration



Non-nested intervals

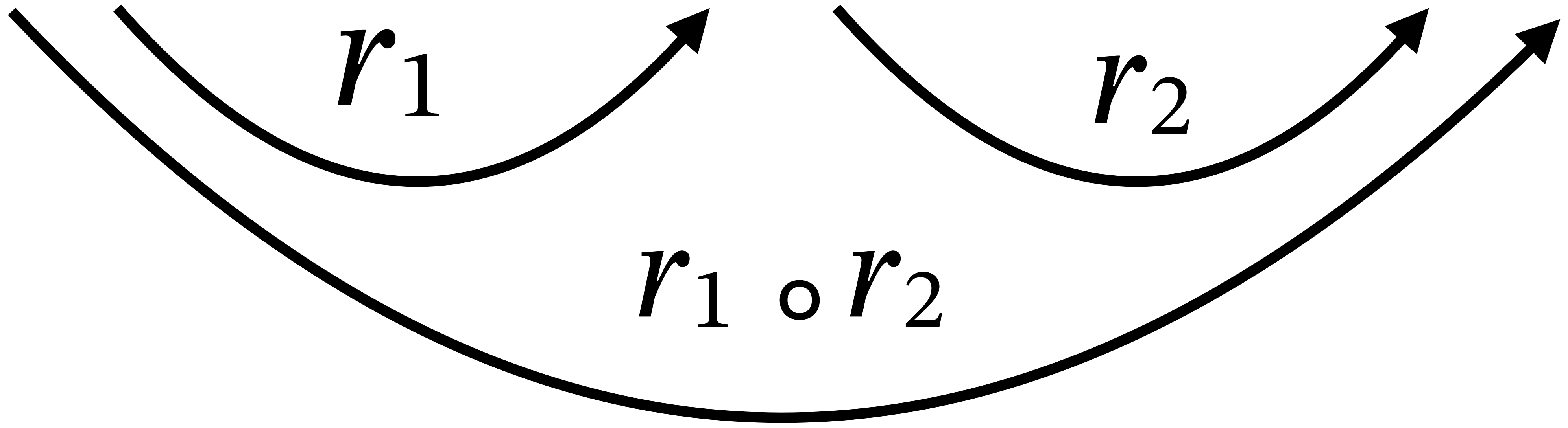
Synchronous simulations do compose

- This holds for synchronous hybrid simulations:

Theorem 5. *If* $T \in \mathsf{T}^{\infty}_{\mathsf{C}}$, $\overline{T} \in \mathsf{T}^{\infty}_{\overline{\mathsf{C}}}$, $\overline{\overline{T}} \in \mathsf{T}^{\infty}_{\overline{\overline{\mathsf{C}}}}$ *are well-nested,* $\langle T,\, \overline{T}\rangle \in \vec{\vec{\gamma}}(\vec{\gamma}_c(r_1))$ *and* $\langle \overline{T},\, \overline{\overline{T}}\rangle \in \vec{\vec{\gamma}}(\vec{\gamma}_c(r_2))$ *then* $\langle T,\, \overline{\overline{T}}\rangle \in \vec{\vec{\gamma}}(\vec{\gamma}_c(r_1 \circ r_2))$.

- Example: this holds for the water tank

implementation ∘ automaton ∘ specification



What ?

- The implementation has $y = 0$ for time ε
- The specification says y cannot stay 0 for more than ζ
- What if $\varepsilon > \zeta$???

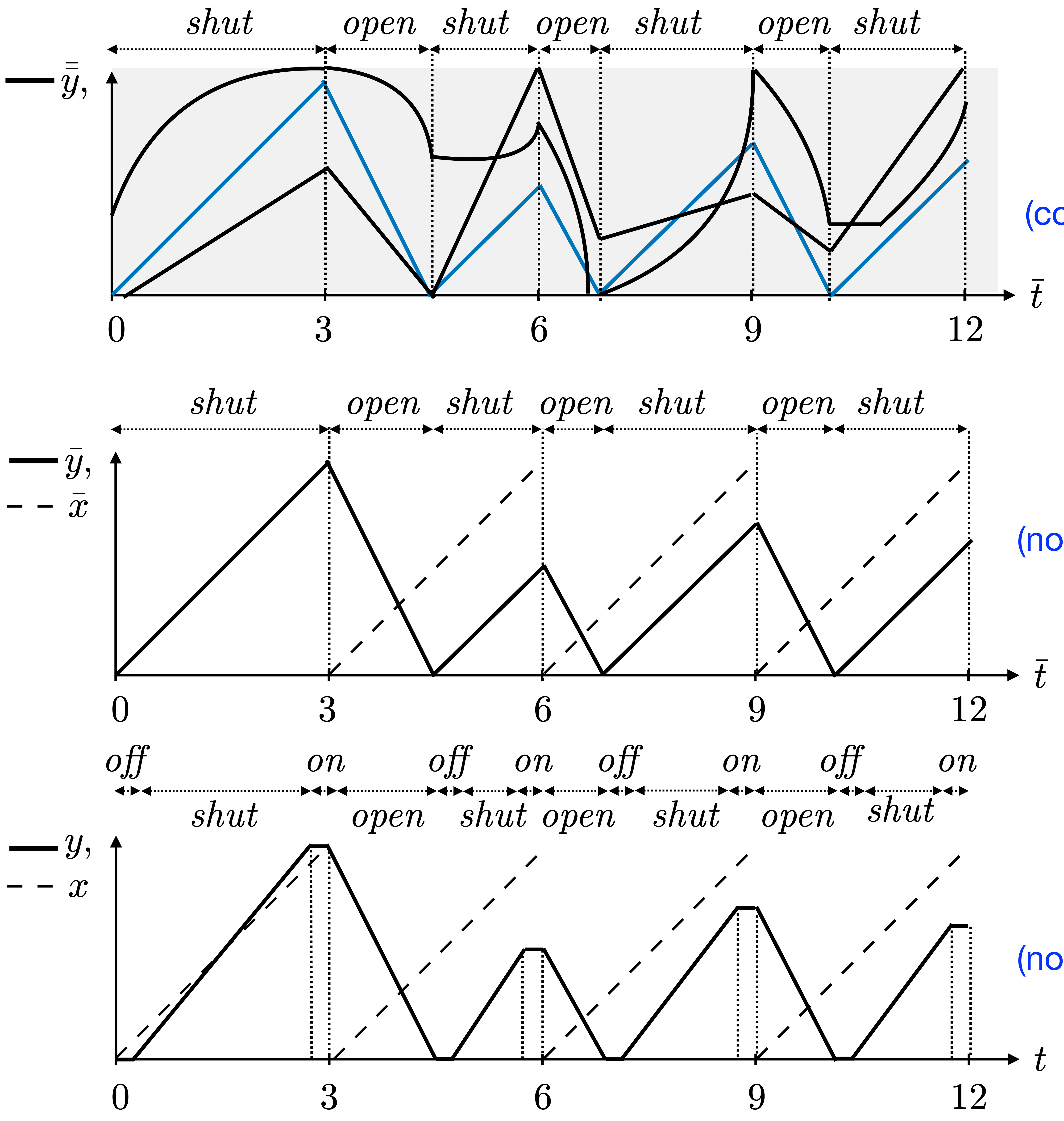
What ?

- The implementation has $y = 0$ for time ε
- The specification says y cannot stay 0 for more than ζ
- What if $\varepsilon > \zeta$???
- NOT A CONTRADICTION since

$$r^{(53)} \circ r^{(39)} \triangleq \{\langle\langle m_t,\ x_t,\ y_t\rangle,\ \langle \overline{m}_t,\ \overline{y}_t\rangle\rangle \mid \exists [t_1, t_2[\subseteq [\bar{t}_1, \bar{t}_2[\ .\ t \in [t_1, t_2[\wedge P^{(53)}(m_t, x_t, y_t, t_1, t_2, \overline{m}_t, x_t, \overline{y}_t, \bar{t}_1, \bar{t}_2)\}$$

By definition (53), this expresses that the height $\overline{y}_t$ of the water in the specification when the valve is *off* for ϵ units of time is equal to the time $x_t > 0$, not to the level of water $y_t = 0$ in the implementation.

The composition of specifications is incomplete

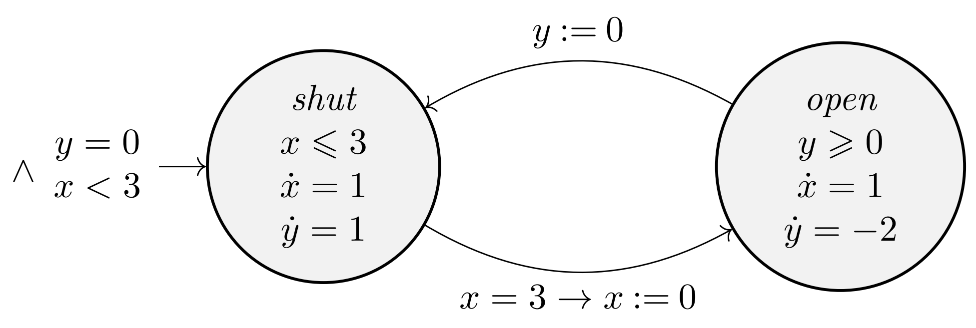


Specification

(constraining tank emptyness)

Automaton

(not constraining tank emptyness)



Implementation

(not constraining tank emptyness)

$$\lambda t \bullet \langle shut, \bar{\bar{y}}_t, t_1 \rangle$$

$r^{(39)}$ =

$$\exists\ \lambda t \bullet \langle shut, \bar{x}_t, \bar{y}_t = t - t_1, t_1 \rangle$$

$R^{(53)}$ = $r^{(39)} \circ R^{(53)}$

$$\lambda t \bullet \langle off, x_t, 0, t_1 \rangle$$

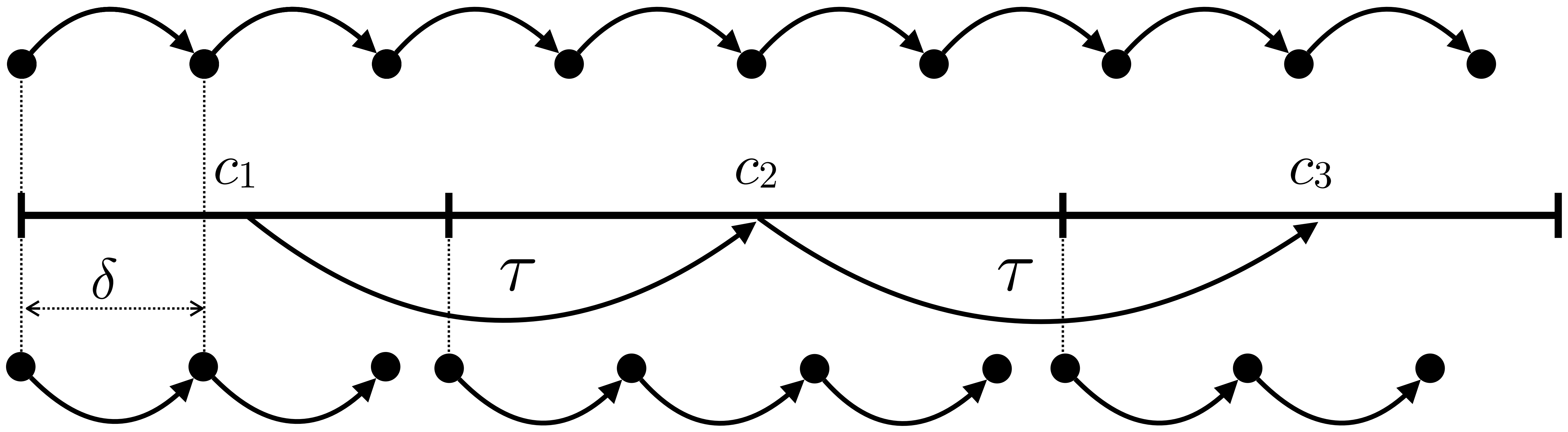
$\bar{\bar{y}}_t = t - t_1$ not 0 for any time t larger than t_1

Discretization

Example: discretization

- $\delta > 0$ be a sampling interval
- $h_\delta(\sigma) \triangleq \langle \sigma_{n\delta},\ n \in \mathbb{N} \wedge n\delta \leqslant [\![\sigma]\!] \rangle$ (using the time evolution abstraction)

  $\alpha_\delta(T) \triangleq \{h_\delta(\sigma) \mid \sigma \in T\}$
- $\langle \wp(\mathsf{T}_{\mathsf{C}}^{+\infty}),\ \subseteq \rangle \xleftarrow[\alpha_\delta]{\gamma_\delta} \langle \wp(\mathsf{T}_{\mathsf{S}}^{+\infty}),\ \subseteq \rangle$
- Not definable using a discretization of the transition relation:



trajectory discretization

transition-generated trajectory

transition configuration discretization

Discretization

- The discretization of an hybrid simulation may not be a discrete simulation
- We have studied sufficient conditions to satisfy this goal.

Conclusion

Conclusion

- All hybrid simulations, bisimulations, preservation with progress, and discretization are Galois connections

$$\langle\{\langle T,\ \overline{T}\rangle \in \wp(\mathsf{T}_{\mathsf{C}}^{+\infty}) \otimes \wp(\mathsf{T}_{\overline{\mathsf{C}}}^{+\infty}) \mid \overline{T} = \emptyset \Longrightarrow T = \emptyset\},\ \supseteq\rangle \xleftarrow[\vec{\vec{\alpha}}]{\vec{\vec{\gamma}}} \langle\wp(\mathsf{T}_{\mathsf{C}}^{+\infty} \times \mathsf{T}_{\overline{\mathsf{C}}}^{+\infty}),\ \supseteq\rangle$$

- Can be composed with further abstractions of the relation between trajectories for the static analysis of hybrid systems

- However, except for the synchronous case, this composition may not correspond to the composition of the relations between states (or configurations)

- Not a problem in Milner's definition which makes no difference between states and configurations and trajectories are traces i.e. synchronous

The End, Thank You