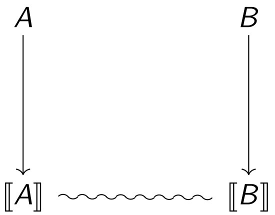
“Inverse semantics” for timed automata

Uli Fahrenberg

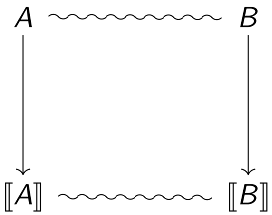
November 27, 2007

$$A \longrightarrow [\![A]\!]$$

- timed automata $\rightsquigarrow$ operational semantics: transition systems

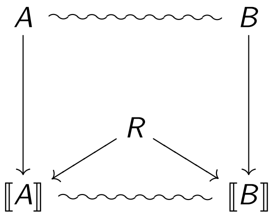


- timed automata $\rightsquigarrow$ operational semantics: transition systems
- transition systems $\rightsquigarrow$ notion of bisimulation



- timed automata $\rightsquigarrow$ operational semantics: transition systems
- transition systems $\rightsquigarrow$ notion of bisimulation

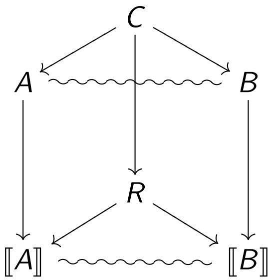
$\rightsquigarrow$ bisimulation for timed automata



- timed automata $\rightsquigarrow$ operational semantics: transition systems
- transition systems $\rightsquigarrow$ notion of bisimulation

$\rightsquigarrow$ bisimulation for timed automata

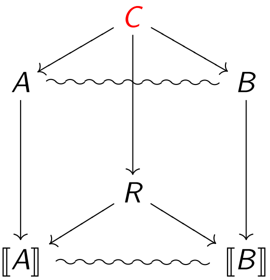
- transition systems $\rightsquigarrow$ notion of open maps
- Two transition systems are bisimilar if and only if they are connected by a "span" of open maps.



- timed automata $\rightsquigarrow$ operational semantics: transition systems
- transition systems $\rightsquigarrow$ notion of bisimulation

$\rightsquigarrow$ bisimulation for timed automata

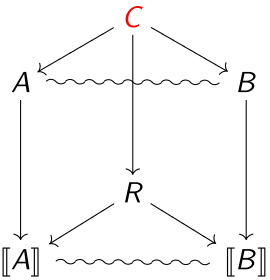
- transition systems $\rightsquigarrow$ notion of open maps
- want to "pull back" these open maps "along the semantics functor"



- timed automata $\rightsquigarrow$ operational semantics: transition systems
- transition systems $\rightsquigarrow$ notion of bisimulation

$\rightsquigarrow$ bisimulation for timed automata

- transition systems $\rightsquigarrow$ notion of open maps
- want to "pull back" these open maps "along the semantics functor"
- central piece: how to construct C from R ("inverse semantics")



- timed automata $\rightsquigarrow$ operational semantics: transition systems
- transition systems $\rightsquigarrow$ notion of bisimulation

$\rightsquigarrow$ bisimulation for timed automata

- transition systems $\rightsquigarrow$ notion of open maps
- want to "pull back" these open maps "along the semantics functor"
- central piece: how to construct C from R ("inverse semantics")
- Generalization!

Open maps:

- [Joyal, Nielsen, Winskel: *Bisimulation from open maps*. Information and Computation 127(2), 1996]
- standard models ("presheaves")
- standard logics
- relations between different formalisms ("adjoint functors")
- connection to algebraic topology ("model categories")

- transition system:
  - S states
  - $s^0 \in S$ initial state
  - Σ labels
  - $E \subseteq S \times \Sigma \times S$ transitions

- transition system: $(S, s^0, \Sigma, E \subseteq S \times \Sigma \times S)$
- morphism of transition systems $(S_1, s_1^0, \Sigma, E_1)$, $(S_2, s_2^0, \Sigma, E_2)$: $f : S_1 \to S_2$ such that

$$f(s_1^0) = s_2^0$$
$$(s, a, s') \in E_1 \implies (f(s), a, f(s')) \in E_2$$

- morphisms are *functional simulations*
- (in actual fact, morphisms can also change the labeling. We don't need this here)

- transition system: $(S, s^0, \Sigma, E \subseteq S \times \Sigma \times S)$
- morphism of transition systems $(S_1, s_1^0, \Sigma, E_1)$, $(S_2, s_2^0, \Sigma, E_2)$: $f : S_1 \to S_2$ such that

$$f(s_1^0) = s_2^0$$
$$(s, a, s') \in E_1 \implies (f(s), a, f(s')) \in E_2$$

$\rightsquigarrow$ category of transition systems

- well-behaved category; natural constructions are well-known; relates to other formalisms by (reflective) functors
- [Winskel, Nielsen: *Models for concurrency*. In Handbook of Logic in Computer Science, Oxford Univ. Press 1995]

- transition system: $(S, s^0, \Sigma, E \subseteq S \times \Sigma \times S)$
- morphism of transition systems $(S_1, s_1^0, \Sigma, E_1)$, $(S_2, s_2^0, \Sigma, E_2)$: $f : S_1 \to S_2$ such that

$$f(s_1^0) = s_2^0$$
$$(s, a, s') \in E_1 \implies (f(s), a, f(s')) \in E_2$$

$\rightsquigarrow$ category of transition systems

- a morphism $f : (S_1, s_1^0, \Sigma, E_1) \to (S_2, s_2^0, \Sigma, E_2)$ is open if

- transition system: $(S, s^0, \Sigma, E \subseteq S \times \Sigma \times S)$
- morphism of transition systems $(S_1, s_1^0, \Sigma, E_1)$, $(S_2, s_2^0, \Sigma, E_2)$: $f : S_1 \to S_2$ such that

$$f(s_1^0) = s_2^0$$
$$(s, a, s') \in E_1 \implies (f(s), a, f(s')) \in E_2$$

⇝ category of transition systems

- a morphism $f : (S_1, s_1^0, \Sigma, E_1) \to (S_2, s_2^0, \Sigma, E_2)$ is open if

$$\forall \text{ reachable } s_1 \in S_1 \qquad \begin{array}{ccc} S_1 & & s_1 \\ {\scriptstyle f}\big\downarrow & & \\ S_2 & & \end{array}$$

- transition system: $(S, s^0, \Sigma, E \subseteq S \times \Sigma \times S)$
- morphism of transition systems $(S_1, s_1^0, \Sigma, E_1)$, $(S_2, s_2^0, \Sigma, E_2)$: $f : S_1 \to S_2$ such that

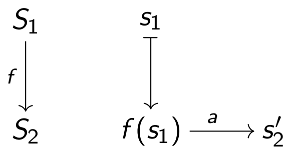
$$\begin{aligned} & f(s_1^0) = s_2^0 \\ & (s, a, s') \in E_1 \implies (f(s), a, f(s')) \in E_2 \end{aligned}$$

$\rightsquigarrow$ category of transition systems

- a morphism $f : (S_1, s_1^0, \Sigma, E_1) \to (S_2, s_2^0, \Sigma, E_2)$ is open if

$\forall$ reachable $s_1 \in S_1$

$\forall$ edges $(f(s_1), a, s_2') \in E_2$



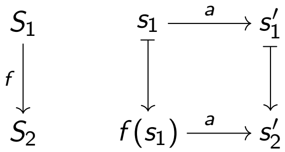
- transition system: $(S, s^0, \Sigma, E \subseteq S \times \Sigma \times S)$
- morphism of transition systems $(S_1, s_1^0, \Sigma, E_1)$, $(S_2, s_2^0, \Sigma, E_2)$: $f : S_1 \to S_2$ such that

$$f(s_1^0) = s_2^0$$
$$(s, a, s') \in E_1 \implies (f(s), a, f(s')) \in E_2$$

$\rightsquigarrow$ category of transition systems

- a morphism $f : (S_1, s_1^0, \Sigma, E_1) \to (S_2, s_2^0, \Sigma, E_2)$ is open if

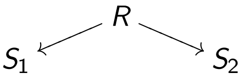
$\forall$ reachable $s_1 \in S_1$
$\forall$ edges $(f(s_1), a, s_2') \in E_2$
$\exists$ edge $(s_1, a, s_1') \in E_1$
for which $s_2' = f(s_1')$



- (again:) a morphism $f : (S_1, s_1^0, \Sigma E_1) \to (S_2, s_2^0, \Sigma, E_2)$ is open if
  - $\forall$ reachable $s_1 \in S_1$
  - $\forall$ edges $\big(f(s_1), a, s_2'\big) \in E_2$
  - $\exists$ edge $(s_1, a, s_1') \in E_1$ for which $s_2' = f(s_1')$
- open map $f : (S_1, s_1^0, \Sigma, E_1) \to (S_2, s_2^0, \Sigma, E_2) \rightsquigarrow$ bisimulation

$$R = \big\{ \big(s, f(s)\big) \;\big|\; s \in S_1 \text{ reachable} \big\}$$

- conversely: bisimulation $R \subseteq S_1 \times S_2 \rightsquigarrow$ span of open maps



- a path transition system:

$$s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} s_2 \longrightarrow \dots \xrightarrow{a_n} s_n$$

- **P** : the category of paths and inclusion morphisms
- (a *full* subcategory of transition systems)

- a path transition system:

$$s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} s_2 \longrightarrow \dots \xrightarrow{a_n} s_n$$

- $\mathbf{P}$: the category of paths and inclusion morphisms
- a path in a transition system $T \triangleq$ a morphism $P \to T$, for $P \in \mathbf{P}$

- a path transition system:

$$s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} s_2 \longrightarrow \dots \xrightarrow{a_n} s_n$$

- $\mathbf{P}$: the category of paths and inclusion morphisms
- a path in a transition system $T \mathrel{\hat{=}}$ a morphism $P \to T$, for $P \in \mathbf{P}$
- a morphism $f : T_1 \to T_2$ is open if and only if:

- a path transition system:

$$s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} s_2 \longrightarrow \dots \xrightarrow{a_n} s_n$$

- $\mathbf{P}$: the category of paths and inclusion morphisms
- a path in a transition system $T \mathrel{\hat{=}}$ a morphism $P \to T$, for $P \in \mathbf{P}$
- a morphism $f : T_1 \to T_2$ is open if and only if:

$$\forall\ m : P_1 \to P_2 \in \mathbf{P}$$

$$\begin{array}{ccc} P_1 & & T_1 \\ {\scriptstyle m}\big\downarrow & & \big\downarrow{\scriptstyle f} \\ P_2 & & T_2 \end{array}$$

- a path transition system:

$$s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} s_2 \longrightarrow \dots \xrightarrow{a_n} s_n$$

- $\mathbf{P}$: the category of paths and inclusion morphisms
- a path in a transition system $T \mathrel{\hat{=}}$ a morphism $P \to T$, for $P \in \mathbf{P}$
- a morphism $f : T_1 \to T_2$ is open if and only if:

$\forall\ m : P_1 \to P_2 \in \mathbf{P}$

$\forall\ p_1 : P_1 \to T_1,\ p_2 : P_2 \to T_2$
with $p_2 \circ m = f \circ p_1$

$$\begin{array}{ccc} P_1 & \xrightarrow{p_1} & T_1 \\ {\scriptstyle m}\downarrow & & \downarrow{\scriptstyle f} \\ P_2 & \xrightarrow[p_2]{} & T_2 \end{array}$$

- a path transition system:

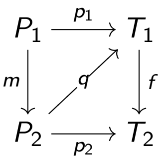
$$s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} s_2 \longrightarrow \dots \xrightarrow{a_n} s_n$$

- $\mathbf{P}$: the category of paths and inclusion morphisms
- a path in a transition system $T \mathrel{\hat{=}}$ a morphism $P \to T$, for $P \in \mathbf{P}$
- a morphism $f : T_1 \to T_2$ is open if and only if:

$\forall\ m : P_1 \to P_2 \in \mathbf{P}$

$\forall\ p_1 : P_1 \to T_1,\ p_2 : P_2 \to T_2$
with $p_2 \circ m = f \circ p_1$

$\exists\ q : P_2 \to T_1$ such that
$q \circ m = p_1$ and $f \circ q = p_2$



- a path transition system:

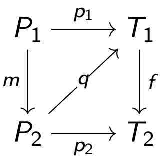
$$s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} s_2 \longrightarrow \dots \xrightarrow{a_n} s_n$$

- $\mathbf{P}$: the category of paths and inclusion morphisms
- a path in a transition system $T \hat{=}$ a morphism $P \to T$, for $P \in \mathbf{P}$
- a morphism $f : T_1 \to T_2$ is open if and only if:

$$\forall\ m : P_1 \to P_2 \in \mathbf{P}$$

$$\forall\ p_1 : P_1 \to T_1,\ p_2 : P_2 \to T_2 \quad \text{with } p_2 \circ m = f \circ p_1$$

$$\exists\ q : P_2 \to T_1 \text{ such that } q \circ m = p_1 \text{ and } f \circ q = p_2$$



- a.k.a. open maps $= RLP(\mathbf{P})$
- see also [Kurz, Rosický: *Weak Factorizations, Fractions and Homotopies*. Applied Categorical Structures 13, 2005]

- a path transition system:

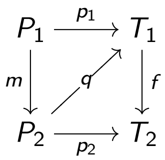
$$s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} s_2 \longrightarrow \dots \xrightarrow{a_n} s_n$$

- $\mathbf{P}$: the category of paths and inclusion morphisms
- a path in a transition system $T \hat{=}$ a morphism $P \to T$, for $P \in \mathbf{P}$
- a morphism $f : T_1 \to T_2$ is open if and only if:

$\forall\ m : P_1 \to P_2 \in \mathbf{P}$

$\forall\ p_1 : P_1 \to T_1,\ p_2 : P_2 \to T_2$
with $p_2 \circ m = f \circ p_1$

$\exists\ q : P_2 \to T_1$ such that
$q \circ m = p_1$ and $f \circ q = p_2$

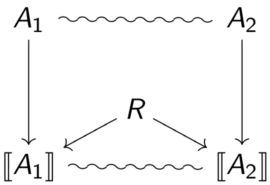


- a.k.a. open maps $= RLP(\mathbf{P})$
- generalization to higher-dimensional transition systems: [Fahrenberg: *A category of higher-dimensional automata.* FOSSACS 2005]

Back to timed automata:

- $A_i = (Q_i, q_i^0, \Sigma, C_i, \iota_i, E_i)$ timed automata

$\rightsquigarrow$ $[\![A_i]\!] = (S_i, s_i^0, \Sigma \cup \mathbb{R}_{\geq 0}, E_i')$ location-valuation timed transition systems:



$$S_i = \big\{(q, \nu) \in Q_i \times \mathbb{R}_{\geq 0}^{C_i} \;\big|\; \nu \vdash \iota_i(q)\big\}$$

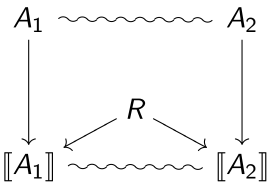
$$E_i' = \big\{(q, \nu) \xrightarrow{a} (q', \nu') \;\big|\; \exists q \xrightarrow[\varphi, S]{a} q' \in E_i : \nu \vdash \varphi, \nu' = \nu[S \leftarrow 0]\big\}$$

$$\cup \big\{(q, \nu) \xrightarrow{t} (q, \nu + t) \;\big|\; \forall t' \in [0, t] : \nu + t' \vdash \iota_i(q)\big\}$$

Back to timed automata:

- $A_i = (Q_i, q_i^0, \Sigma, C_i, \iota_i, E_i)$ timed automata

$\rightsquigarrow$ $[\![A_i]\!] = (S_i, s_i^0, \Sigma \cup \mathbb{R}_{\geq 0}, E_i')$ location-valuation timed transition systems:



$$S_i = \big\{ (q, \nu) \in Q_i \times \mathbb{R}_{\geq 0}^{C_i} \bigm| \nu \vdash \iota_i(q) \big\}$$

$$E_i' = \big\{ (q, \nu) \xrightarrow{a} (q', \nu') \bigm| \exists q \xrightarrow[\varphi, S]{a} q' \in E_i : \nu \vdash \varphi, \nu' = \nu[S \leftarrow 0] \big\}$$

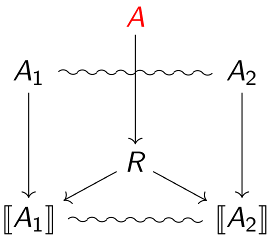
$$\cup \big\{ (q, \nu) \xrightarrow{t} (q, \nu + t) \bigm| \forall t' \in [0, t] : \nu + t' \vdash \iota_i(q) \big\}$$

$\rightsquigarrow$ $R = (S, \Sigma \cup \mathbb{R}_{\geq 0}, E')$ is also a LVTTS:

$$S \subseteq S_1 \times S_2 \overset{\sim}{\subseteq} Q_1 \times Q_2 \times \mathbb{R}_{\geq 0}^{C_1 \sqcup C_2}$$

$$E' = \big\{ (q_1, q_2, \nu_1, \nu_2) \xrightarrow{\alpha} (q_1', q_2', \nu_1', \nu_2') \bigm| (q_i, \nu_i) \xrightarrow{\alpha} (q_i', \nu_i') \in E_i' \big\}$$

Back to timed automata:



- $A_i = (Q_i, q_i^0, \Sigma, C_i, \iota_i, E_i)$ timed automata

$\rightsquigarrow$ $[\![A_i]\!] = (S_i, s_i^0, \Sigma \cup \mathbb{R}_{\geq 0}, E_i')$ location-valuation timed transition systems:

$$S_i = \big\{(q, \nu) \in Q_i \times \mathbb{R}_{\geq 0}^{C_i} \;\big|\; \nu \vdash \iota_i(q)\big\}$$

$$E_i' = \big\{(q, \nu) \xrightarrow{a} (q', \nu') \;\big|\; \exists q \xrightarrow[\varphi, S]{a} q' \in E_i : \nu \vdash \varphi, \nu' = \nu[S \leftarrow 0]\big\}$$

$$\cup \big\{(q, \nu) \xrightarrow{t} (q, \nu + t) \;\big|\; \forall t' \in [0, t] : \nu + t' \vdash \iota_i(q)\big\}$$

$\rightsquigarrow$ $R = (S, \Sigma \cup \mathbb{R}_{\geq 0}, E')$ is also a LVTTS:

$$S \subseteq S_1 \times S_2 \overset{\sim}{\subseteq} Q_1 \times Q_2 \times \mathbb{R}_{\geq 0}^{C_1 \sqcup C_2}$$

$$E' = \big\{(q_1, q_2, \nu_1, \nu_2) \xrightarrow{\alpha} (q_1', q_2', \nu_1', \nu_2') \;\big|\; (q_i, \nu_i) \xrightarrow{\alpha} (q_i', \nu_i') \in E_i'\big\}$$

- Theorem: A LVTTS is the semantics of a timed automaton if and only if it has a stable region quotient.

Break $\rightsquigarrow$ Coffee $\rightsquigarrow$ Proof