

Software Design, Modelling and Analysis in UML

Lecture 18: Live Sequence Charts II

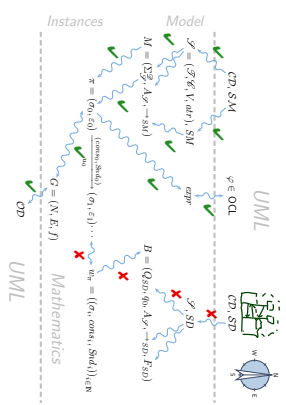
2013-01-22

Prof. Dr. Andreas Podolski, Dr. Bernd Westphal
 Albert-Ludwigs-Universität Freiburg, Germany

Contents & Goals

- Last Lecture:**
 - LSC concrete syntax.
 - LSC intuitive semantics.
- This Lecture:**
 - Educational Objectives:** Capabilities for following tasks/questions:
 - What does this LSC mean?
 - Are this UML model's state machines consistent with the interactions?
 - Please provide a UML model which is consistent with this LSC.
 - What is: activation, hot/cold condition, pre-chart, etc.?
 - Content:**
 - Symbolic Buchi Automata (TBA) and its (accepted) language.
 - Words of a model.
 - LSC abstract syntax.
 - LSC formal semantics.

Course Map



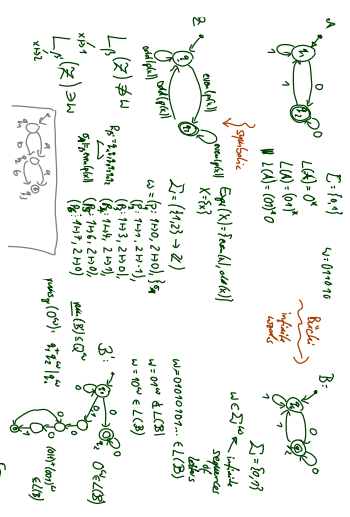
Excursus: Symbolic Buchi Automata (over Signature)

Definition. A Symbolic Buchi Automaton (TBA) is a tuple

$$B = (Expr_{st}(X), X, Q, q_{init}, \neg, Q_f)$$

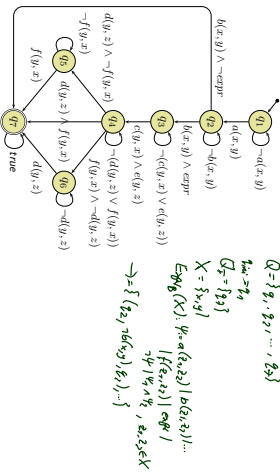
where

- X is a set of logical variables.
- $Expr_{st}(X)$ is a set of Boolean expressions over X .
- Q is a finite set of states.
- $q_{init} \in Q$ is the initial state.
- $\neg \subseteq Q \times Expr_{st}(X) \times Q$ is the transition relation.
- Transitions (q, ψ, q') from q to q' are labeled with an expression $\psi \in Expr_{st}(X)$.
- $Q_f \subseteq Q$ is the set of fair (or accepting) states.



TBA Example

$$(Expr_g(X), X, Q, q_{init}, \rightarrow, Q_f), (u, \psi, \delta) \in \dots$$



6/7

Word

Definition. Let X be a set of logical variables and let $Expr_g(X)$ be a set of Boolean expressions over X .
 A set $(\Sigma, \models \cdot)$ is called an **alphabet** for $Expr_g(X)$ if and only if

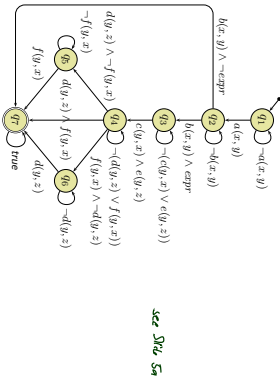
- For each $\sigma \in \Sigma$
- for each expression $expr \in Expr_g$ and
- for each valuation $\beta : X \rightarrow \mathcal{D}(X)$ of logical variables to domain $\mathcal{D}(X)$,

either $\sigma \models_{\beta} expr$ or $\sigma \not\models_{\beta} expr$.

$w = (\sigma_i)_{i \in \mathbb{N}_0} \in \Sigma^{\omega}$
 over $(\Sigma, \models \cdot)$ is called **word** for $Expr_g(X)$.

7/7

Word Example



8/7

Run of TBA over Word

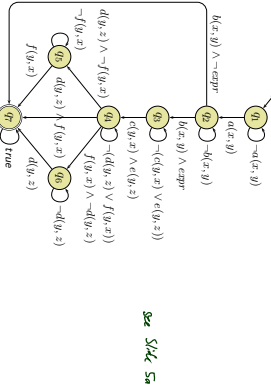
Definition. Let $B = (Expr_g(X), X, Q, q_{init}, \rightarrow, Q_f)$ be a TBA and $w = \sigma_1, \sigma_2, \sigma_3, \dots \in \Sigma^{\omega}$ a word for $Expr_g(X)$.
 An infinite sequence $\varrho = q_0, q_1, q_2, \dots \in Q^{\omega}$ is called **run** of B over w under valuation $\beta : X \rightarrow \mathcal{D}(X)$ if and only if

- $q_0 = q_{init}$,
- for each $i \in \mathbb{N}_0$ there is a transition $(q_i, \sigma_{i+1}, q_{i+1}) \in \rightarrow$ of B such that $\sigma_i \models_{\beta} \psi_i$.

9/7

Run Example

$$\varrho = (q_0, q_1, q_2, \dots \in Q^{\omega} \text{ s.t. } \sigma_i \models_{\beta} \psi_i, i \in \mathbb{N}_0)$$



10/7

The Language of a TBA

Definition. We say B **accepts** word w (under β) if and only if B has a run over w such that fair (or accepting) states are visited infinitely often by ϱ , i.e., such that $\forall i \in \mathbb{N}_0 \exists j > i : q_j \in Q_f$.

We call the set $L_{\beta}(B) \subseteq \Sigma^{\omega}$ of words for $Expr_g(X)$ that are accepted by B the **language** of B .

11/7

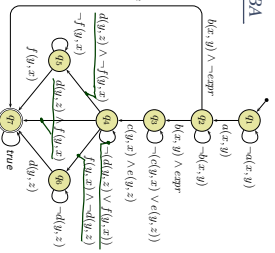
Language of the Example TBA

$L_1(\mathcal{B})$ consists of the words

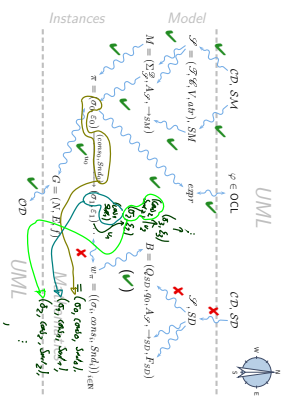
$$w = (a_i)_{i \in \mathbb{N}_0}$$

where for $0 \leq i < m < k < \ell$ we have

- For $0 \leq i < n$, $\sigma \notin \alpha(i)$
- $\sigma_n \notin \alpha(k)$
- for $n < i < m$, $\sigma_i \notin \alpha(k)$
- $\sigma_m \notin \alpha(k)$
- For $m < i < k$, $\sigma_i \notin \alpha(k)$
- $\sigma_k \in \alpha(\ell)$
- for $k < i < \ell$, $\sigma_i \notin \alpha(\ell)$
- ...



Course Map



Back to Main Track: Language of a Model

Words over Signature

Definition. Let $\mathcal{S} = (\mathcal{F}, \mathcal{G}, V, \text{dir}, \mathcal{D})$ be a signature and \mathcal{A} a structure of \mathcal{S} . A word over \mathcal{S} and \mathcal{A} is an infinite sequence

$$(a_1, \text{cons}_1, \text{SMod}_1)_{i \in \mathbb{N}_0} \in (\Sigma_{\mathcal{S}}^* \times \mathcal{C}^{\text{Dir}(\mathcal{G}) \times \text{Bnd}(\mathcal{G}) \times \mathcal{D}})^{\mathbb{N}}$$

The Language of a Model

Recall. A UML model $\mathcal{M} = (\mathcal{Q}, \mathcal{S}, \mathcal{M}, \mathcal{O}, \mathcal{D})$ and a structure \mathcal{A} denotes a set $[\mathcal{M}]$ of (initial and consecutive) computations of the form

$$(r_0, \varepsilon_0) \xrightarrow{\text{dir}_0} (r_1, \varepsilon_1) \xrightarrow{\text{dir}_1} (r_2, \varepsilon_2) \xrightarrow{\text{dir}_2} \dots \text{ where } a_i = (\text{cons}_i, \text{SMod}_i)_{i \in \mathbb{N}}$$

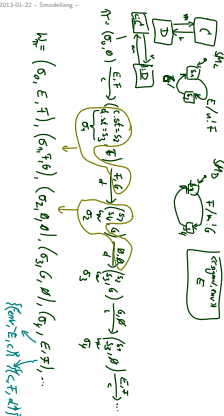
For the connection between models and interactions, we disregard the configuration of the ether and who made the step, and define as follows:

Definition. Let $\mathcal{M} = (\mathcal{Q}, \mathcal{S}, \mathcal{M}, \mathcal{O}, \mathcal{D})$ be a UML model and \mathcal{A} a structure. Then

$$L(\mathcal{M}) := \{ (a_i, \text{cons}_i, \text{SMod}_i)_{i \in \mathbb{N}_0} \in (\Sigma_{\mathcal{S}}^* \times \mathcal{A}^*) \mid \exists (r_i, \varepsilon_i)_{i \in \mathbb{N}_0} : (r_0, \varepsilon_0) \xrightarrow{\text{dir}_0} (r_1, \varepsilon_1) \dots \in [\mathcal{M}] \}$$

Example: The Language of a Model

$$L(\mathcal{M}) := \{ (a_i, \text{cons}_i, \text{SMod}_i)_{i \in \mathbb{N}_0} \in (\Sigma_{\mathcal{S}}^* \times \mathcal{A}^*) \mid \exists (r_i, \varepsilon_i)_{i \in \mathbb{N}_0} : (r_0, \varepsilon_0) \xrightarrow{\text{dir}_0} (r_1, \varepsilon_1) \dots \in [\mathcal{M}] \}$$



Signal and Attribute Expressions

- Let $\mathcal{S} = (\mathcal{S}, \mathcal{V}, \text{attr}, \delta)$ be a signature and X a set of logical variables.
- The signal and attribute expressions $\text{Expr}_{\mathcal{S}}(\delta, X)$ are defined by the grammar:

$$\psi ::= \text{true} \mid \text{expr} \mid E_{a,y}^2 \mid E_{a,x}^2 \mid \neg\psi \mid \psi_1 \vee \psi_2$$
 where $\text{expr} : \text{Bool} \in \text{Expr}_{\mathcal{S}}$, $E \in \delta$, $x, y \in X$.

Satisfaction of Signal and Attribute Expressions

- Let $(\alpha, \text{cons}, \text{Stnd}) \in \Sigma_{\mathcal{S}}^{\text{sig}} \times \mathbb{A}$ be a triple consisting of system state, consume set, and send set.
- Let $\beta : X \rightarrow \mathcal{D}(\mathcal{V})$ be a valuation of the logical variables.
- Then β is **admissible** if and only if β is a valuation of the logical variables.
- Then $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} \text{true}$
- $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} \neg\psi$ if and only if not $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} \psi$
- $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} \psi_1 \vee \psi_2$ if and only if $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} \psi_1$ or $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} \psi_2$
- $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} \text{expr}$ if and only if $\llbracket \text{expr} \rrbracket(\alpha, \beta) = 1$ for **single-bit** **event** **predicates** are **part of LSC**
- $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} E_{a,y}^2$ if and only if $\exists d \bullet (\beta(x), (E, \bar{d}), \beta(y)) \in \text{Stnd}$
- $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} E_{a,x}^2$ if and only if $\exists \bar{d} \bullet (\beta(x), (E, \bar{d}), \beta(y)) \in \text{cons}$

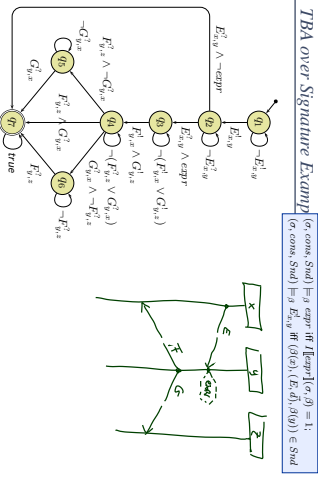
TBA over Signature

Definition. A TBA

$$B = (\text{Expr}_{\mathcal{S}}(\delta, X), X, Q, \text{Inits}, \neg, Q_P)$$
 where $\text{Expr}_{\mathcal{S}}(\delta, X)$ is the set of signal and attribute expressions $\text{Expr}_{\mathcal{S}}(\delta, X)$ over signature \mathcal{S} is called **TBA over \mathcal{S}** .

- Any word over \mathcal{S} and \mathcal{Q} is then a word for B . (By the satisfaction relation defined on the previous slide: $\mathcal{D}(X) = \mathcal{D}(\mathcal{V})$)
- Thus a TBA over \mathcal{S} accents words of models with signature \mathcal{S} . (By the previous definition of TBA)

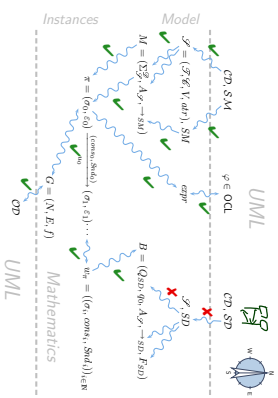
TBA over Signature Exmp



Satisfaction of Signal and Attribute Expressions

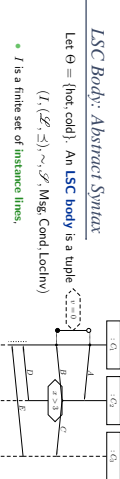
- Let $(\alpha, \text{cons}, \text{Stnd}) \in \Sigma_{\mathcal{S}}^{\text{sig}} \times \mathbb{A}$ be a triple consisting of system state, consume set, and send set.
 - Let $\beta : X \rightarrow \mathcal{D}(\mathcal{V})$ be a valuation of the logical variables.
 - Then $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} \text{true}$
 - $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} \neg\psi$ if and only if not $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} \psi$
 - $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} \psi_1 \vee \psi_2$ if and only if $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} \psi_1$ or $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} \psi_2$
 - $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} \text{expr}$ if and only if $\llbracket \text{expr} \rrbracket(\alpha, \beta) = 1$
 - $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} E_{a,y}^2$ if and only if $\exists d \bullet (\beta(x), (E, \bar{d}), \beta(y)) \in \text{Stnd}$
 - $(\alpha, \text{cons}, \text{Stnd}) \models_{\beta} E_{a,x}^2$ if and only if $\exists \bar{d} \bullet (\beta(x), (E, \bar{d}), \beta(y)) \in \text{cons}$
- Observation:** semantics of models keeps track of sender and receiver at sending and consumption time. We disregard the event identity.
Alternative: keep track of event identities.

Course Map



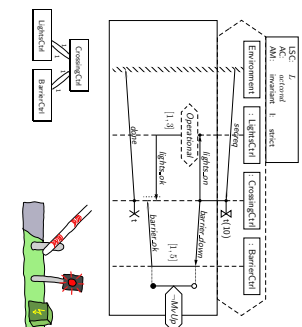
Live Sequence Charts Abstract Syntax

24/7

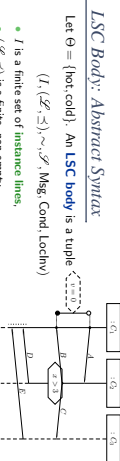


26/7

Example

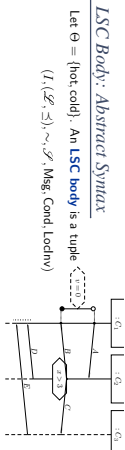


25/7

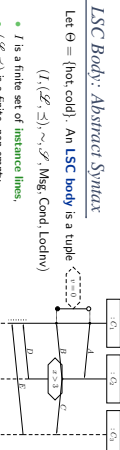


26/7

LSC Body: Abstract Syntax



26/7

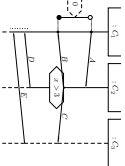


26/7

LSC Body: Abstract Syntax

Let $\Theta = \{\text{hot, cold}\}$. An LSC body is a tuple $(I, \mathcal{L}, \mathcal{S}, \sim, \mathcal{F}, \text{Msg}, \text{Cond}, \text{LocInv})$

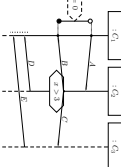
- I is a finite set of instance lines.
- $(\mathcal{L}, \mathcal{S})$ is a finite, non-empty, partially ordered set of locations, partially ordered by their temperature $\theta(l) \in \Theta$ and an instance line $l \in I$.
- $\sim \subseteq \mathcal{L} \times \mathcal{L}$ is an equivalence relation on locations, the simultaneity relation.
- $\mathcal{F} = (\mathcal{F}, \mathcal{V}, \text{dir}, \delta)$ is a signature.



LSC Body: Abstract Syntax

Let $\Theta = \{\text{hot, cold}\}$. An LSC body is a tuple $(I, \mathcal{L}, \mathcal{S}, \sim, \mathcal{F}, \text{Msg}, \text{Cond}, \text{LocInv})$

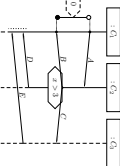
- I is a finite set of instance lines.
- $(\mathcal{L}, \mathcal{S})$ is a finite, non-empty, partially ordered set of locations, partially ordered by their temperature $\theta(l) \in \Theta$ and an instance line $l \in I$.
- $\sim \subseteq \mathcal{L} \times \mathcal{L}$ is an equivalence relation on locations, the simultaneity relation.
- $\mathcal{F} = (\mathcal{F}, \mathcal{V}, \text{dir}, \delta)$ is a signature.
- $\text{Msg} \subseteq \mathcal{L} \times \mathcal{L} \times \mathcal{L}$ is a set of asynchronous messages with $(l, h, t) \in \text{Msg}$ only if $l \preceq t$.
- Note:** instantaneous messages — could be linked to method/operation calls.



LSC Body: Abstract Syntax

Let $\Theta = \{\text{hot, cold}\}$. An LSC body is a tuple $(I, \mathcal{L}, \mathcal{S}, \sim, \mathcal{F}, \text{Msg}, \text{Cond}, \text{LocInv})$

- I is a finite set of instance lines.
- $(\mathcal{L}, \mathcal{S})$ is a finite, non-empty, partially ordered set of locations, partially ordered by their temperature $\theta(l) \in \Theta$ and an instance line $l \in I$.
- $\sim \subseteq \mathcal{L} \times \mathcal{L}$ is an equivalence relation on locations, the simultaneity relation.
- $\mathcal{F} = (\mathcal{F}, \mathcal{V}, \text{dir}, \delta)$ is a signature.
- $\text{Msg} \subseteq \mathcal{L} \times \mathcal{L} \times \mathcal{L}$ is a set of asynchronous messages with $(l, h, t) \in \text{Msg}$ only if $l \preceq t$.
- Note:** instantaneous messages — could be linked to method/operation calls.
- $\text{Cond} \subseteq (\mathcal{Z}^{\mathcal{L}} \setminus \emptyset) \times \text{Expr} \mathcal{F} \times \Theta$ is a set of conditions where $\text{Expr} \mathcal{F}$ are OCL expressions over $W = I \cup \{\text{obj}\}$ with $(l, \text{expr}, \theta) \in \text{Cond}$ only if $l \sim t$ for all $t, t' \in L$.
- $\text{LocInv} \subseteq \mathcal{L} \times \{\circ, \bullet\} \times \text{Expr} \mathcal{F} \times \Theta \times \mathcal{L} \times \mathcal{L} \times \{\circ, \bullet\}$ is a set of local invariants.



Well-Formedness

Boundness/ no floating conditions: (could be relaxed a little if we wanted to)

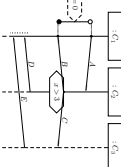
- For each location $l \in \mathcal{L}$, if l is the location of
 - a condition, i.e. $\exists (L, \text{expr}, \theta) \in \text{Cond} : l \in L$, or
 - a local invariant, i.e. $\exists (l, h, s_2) \in \text{LocInv} : l \in \{h, s_2\}$, or
 then there is a location l' equivalent to l , i.e. $l \sim l'$, which is the location of
 - an instance head, i.e. l' is minimal wrt. \preceq ; or
 - a message, i.e. $\exists (l, h, s_2) \in \text{Msg} : l \in \{h, s_2\}$.

Note: if messages in a chart are cyclic, then there doesn't exist a partial order (so such charts don't even have an abstract syntax)

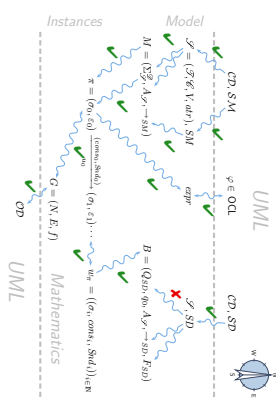
LSC Body: Abstract Syntax

Let $\Theta = \{\text{hot, cold}\}$. An LSC body is a tuple $(I, \mathcal{L}, \mathcal{S}, \sim, \mathcal{F}, \text{Msg}, \text{Cond}, \text{LocInv})$

- I is a finite set of instance lines.
- $(\mathcal{L}, \mathcal{S})$ is a finite, non-empty, partially ordered set of locations, partially ordered by their temperature $\theta(l) \in \Theta$ and an instance line $l \in I$.
- $\sim \subseteq \mathcal{L} \times \mathcal{L}$ is an equivalence relation on locations, the simultaneity relation.
- $\mathcal{F} = (\mathcal{F}, \mathcal{V}, \text{dir}, \delta)$ is a signature.
- $\text{Msg} \subseteq \mathcal{L} \times \mathcal{L} \times \mathcal{L}$ is a set of asynchronous messages with $(l, h, t) \in \text{Msg}$ only if $l \preceq t$.
- Note:** instantaneous messages — could be linked to method/operation calls.
- $\text{Cond} \subseteq (\mathcal{Z}^{\mathcal{L}} \setminus \emptyset) \times \text{Expr} \mathcal{F} \times \Theta$ is a set of conditions where $\text{Expr} \mathcal{F}$ are OCL expressions over $W = I \cup \{\text{obj}\}$ with $(l, \text{expr}, \theta) \in \text{Cond}$ only if $l \sim t$ for all $t, t' \in L$.



Course Map



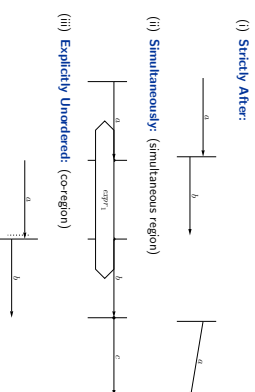
Live Sequence Charts Semantics

- Plan:**
- Given an LSC L with body $(\mathcal{L}, \mathcal{S}) \sim \mathcal{S}, \text{Msg}, \text{Cond}, \text{LocInv}$,
 - construct a TBA B_L , and
 - define $\mathcal{L}(L)$ in terms of $\mathcal{L}(B_L)$, in particular taking activation condition and activation mode into account.
 - Then $\mathcal{M} \models L$ (universal) if and only if $\mathcal{L}(\mathcal{M}) \subseteq \mathcal{L}(L)$.

TBA-based Semantics of LSCs

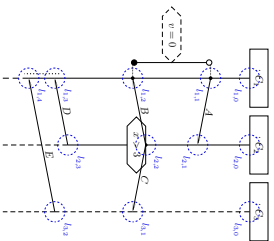
- Plan:**
- Given an LSC L with body $(\mathcal{L}, \mathcal{S}) \sim \mathcal{S}, \text{Msg}, \text{Cond}, \text{LocInv}$,
 - construct a TBA B_L , and
 - define $\mathcal{L}(L)$ in terms of $\mathcal{L}(B_L)$, in particular taking activation condition and activation mode into account.
 - Then $\mathcal{M} \models L$ (universal) if and only if $\mathcal{L}(\mathcal{M}) \subseteq \mathcal{L}(L)$.

Recall: Initiative Semantics



Intuition: A computation path **violates** an LSC if the occurrence of some events doesn't adhere to the partial order obtained as the **transitive closure** of (i) to (iii).

Examples: Semantics?



Formal LSC Semantics: It's in the Guts!

Definition.
Let $(\mathcal{L}, \mathcal{S}) \sim \mathcal{S}, \text{Msg}, \text{Cond}, \text{LocInv}$ be an LSC body.
A non-empty set $\emptyset \neq C \subseteq \mathcal{S}$ is called a **cut** of the LSC body iff

- it is **downward closed**, i.e. $\forall l, l' : l \in C \wedge l \leq l' \Rightarrow l' \in C$,
- it is **closed under simultaneity**, i.e. $\forall l, l' : l \in C \wedge l \sim l' \Rightarrow l' \in C$, and
- it comprises at least **one location per instance line**, i.e. $\forall l \in I \exists l' \in C : l' = l$.

Formal LSC Semantics: It's in the Guts!

Definition.
Let $(\mathcal{L}, \mathcal{S}) \sim \mathcal{S}, \text{Msg}, \text{Cond}, \text{LocInv}$ be an LSC body.
A non-empty set $\emptyset \neq C \subseteq \mathcal{S}$ is called a **cut** of the LSC body iff

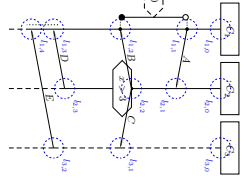
- it is **downward closed**, i.e. $\forall l, l' : l \in C \wedge l \leq l' \Rightarrow l' \in C$,
- it is **closed under simultaneity**, i.e. $\forall l, l' : l \in C \wedge l \sim l' \Rightarrow l' \in C$, and
- it comprises at least **one location per instance line**, i.e. $\forall l \in I \exists l' \in C : l' = l$.

A cut C is called **hot**, denoted by $\text{hot}(C) = \text{hot}$, if and only if at least one of its maximal elements is hot, i.e. if $\exists l \in C : \text{hot}(l) = \text{hot} \wedge \nexists l' \in C : l < l'$

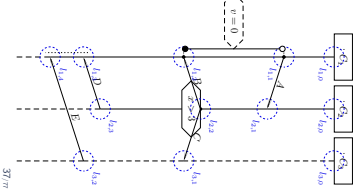
Otherwise, C is called **cold**, denoted by $\text{cold}(C) = \text{cold}$.

- (i) non-empty set $\emptyset \neq C \subseteq \mathcal{L}$.
- (ii) $\forall I, I' \in C: \forall I \subseteq I' \implies I \in C$
- (iii) closed under simultaneity, i.e. $\forall I, I' \in C: I \wedge I' \implies I \in C$
- (iv) at least one location per instance line, i.e. $\forall I \in I \exists l \in C: l \in I$.

- $C_0 = \emptyset$
- $C_1 = \{l_1, a, l_2, a, l_3, a\}$
- $C_2 = \{l_1, a, l_2, a, l_3, a\}$
- $C_3 = \{l_1, a, l_1, l_1\}$
- $C_4 = \{l_1, a, l_1, l_2, a, l_3, a\}$
- $C_5 = \{l_1, a, l_1, l_2, a, l_2, a, l_3, a\}$
- $C_6 = \mathcal{L} \setminus \{l_1, a, l_2, a\}$
- $C_7 = \mathcal{L}$



- Successor Cut Examples**
- (i) $F \neq \emptyset$, (ii) $C' \setminus C = F$.
 - (iii) $\forall I \in F, I' \in C: I \wedge I' \implies I \in C$ and
 - (iv) $\forall I, I' \in F: I \neq I' \wedge l_i = l_j \implies I \not\subseteq I' \wedge I' \not\subseteq I$

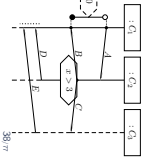


The partial order of (\mathcal{L}, \subseteq) and the simultaneously relation \sim induce a **direct successor relation** on cuts of \mathcal{L} as follows:

- Definition.** Let $C, C' \subseteq \mathcal{L}$ be cuts of an LSC body with locations (\mathcal{L}, \subseteq) and messages Msg . C' is called **direct successor** of C via **fixed-set** F , denoted by $C \rightsquigarrow_F C'$, if and only if
- $F \neq \emptyset$,
 - $C' \setminus C = F$,
 - for each message reception in F , the corresponding sending is already in C ,
 - $\forall (l, E, l') \in \text{Msg}: l' \in F \implies l \in C$, and
 - locations in F , that lie on the same instance line, are pairwise unordered, i.e. $\forall I, I' \in F: I \neq I' \wedge l_i = l_j \implies I \not\subseteq I' \wedge I' \not\subseteq I$

Idea: Accept Timed Words by Advancing the Cut

- Let $w = (a_1, \text{cons}_1, \text{Stid}_1), (a_2, \text{cons}_2, \text{Stid}_2), \dots$ be a word of a UML model and β a valuation of $I \cup \{\text{self}\}$.
- **Intuitively** (and for now **disregarding** cold conditions) an LSC body $(I, (\mathcal{L}, \subseteq), \sim, \text{Msg}, \text{Cond}, \text{LocIn})$ is **supposed to accept** w if and only if there exists a sequence $C_0 \rightsquigarrow_{F_1} C_1 \rightsquigarrow_{F_2} C_2 \rightsquigarrow_{F_3} \dots \rightsquigarrow_{F_n} C_n$ and indices $0 = i_0 < i_1 < \dots < i_n$ such that for all $0 \leq j < n$,
 - for all $i_j \leq k < i_{j+1}$, $(a_k, \text{cons}_k, \text{Stid}_k)$, β satisfies the **hold condition** of C_j ,
 - $(a_{i_j}, \text{cons}_{i_j}, \text{Stid}_{i_j})$, β satisfies the **transition condition** of F_j ,
 - C_j is **cold**,
 - for all $i_n < k$, $(a_k, \text{cons}_k, \text{Stid}_k)$, β satisfies the **hold condition** of C_n .



- $C \rightsquigarrow_F C'$ if and only if
- $F \neq \emptyset$,
 - $C' \setminus C = F$,
 - $\forall (l, E, l') \in \text{Msg}: l' \in F \implies l \in C$, and
 - $\forall I, I' \in F: I \neq I' \wedge l_i = l_j \implies I \not\subseteq I' \wedge I' \not\subseteq I$

- **Note:** F is closed under simultaneity.
- **Note:** locations in F are direct \exists -successors of locations in C , i.e. $\forall I \in F \exists I' \in C: I \prec I' \wedge \exists I'' \in C: I' \prec I'' \prec I$

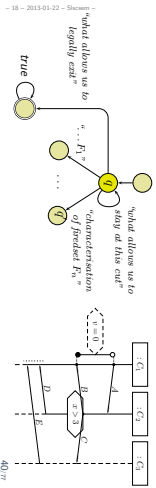
Language of LSC Body

- The **language of the body** $L(\mathcal{L}, \subseteq, \sim, \text{Msg}, \text{Cond}, \text{LocIn})$ of LSC I is the language of the TBA $B_I = (\text{Expr}_g(X), X, Q, q_{\text{init}}, \rightsquigarrow, Q_f)$ with
- $\text{Expr}_g(X) = \text{Expr}_g(\mathcal{L}, X)$
 - Q is the set of cuts of (\mathcal{L}, \subseteq) , q_{init} is the **instance heads cut**,
 - $F = \{C \in Q \mid \theta(C) = \text{cold}\}$ is the set of cold cuts of (\mathcal{L}, \subseteq) ,
 - \rightsquigarrow as defined in the following, consisting of
 - **loops** (q, ψ, q') ,
 - **progress transitions** (q, ψ, q') corresponding to $q \rightsquigarrow_F q'$ and
 - **legal exits** (q, ψ, \mathcal{L}) .

Language of LSC Body: Intuition

$b_i = (\text{Expr}_i(X), X, Q, \text{inv}_i, \neg Q_i)$ with

- $\text{Expr}_i(X) = \text{Expr}_{\neq}(\mathcal{L}, X)$
- Q is the set of cuts of (\mathcal{L}, Σ) , inv_i is the instance heads cut.
- $F = \{C \in Q \mid \theta(C) = \text{cold}\}$ is the set of cold cuts.
- \neg consists of
 - loops (q, ψ, q) ,
 - progress transitions (q, ψ, q') corresponding to $q \rightsquigarrow_{\text{pr}} q'$, and
 - legal exits (q, ψ, \mathcal{L}) .



440

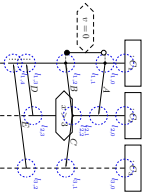
Step 1: Only Messages

– 18 – 2013-01-22 – Shalom –

417

Loops

- How long may we legally stay at a cut q^i ?

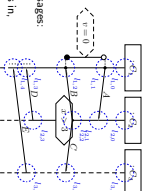


– 18 – 2013-01-22 – Shalom –

437

Loops

- How long may we legally stay at a cut q^i ?
- **Intuition:** those $(\text{Pr}_i, \text{cons}_i, \text{Stnd}_i)$ are allowed to fire the self-loop (q, ψ, q) where
 - $\text{cons}_i \cup \text{Stnd}_i$ comprises only irrelevant messages;
 - weak nodes from a direct successor cut is in;
 - strict nodes;
 - no message occurring in the LSC is in;
- And nothing else.



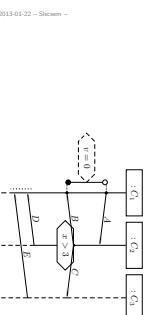
– 18 – 2013-01-22 – Shalom –

437

Some Helper Functions

- **Message-expressions of a location:**

$$\begin{aligned} \mathcal{E}(l) &:= \{E_{l, \text{inv}}^i \mid (l, E, l') \in \text{Msg}\} \cup \{E_{l, \text{inv}}^i \mid (l', E, l) \in \text{Msg}\}, \\ \mathcal{E}(l_1, \dots, l_n) &:= \mathcal{E}(l_1) \cup \dots \cup \mathcal{E}(l_n), \\ \bigvee \emptyset &:= \text{true}, \bigvee \{E_{l_1, \text{inv}}^1, \dots, E_{l_n, \text{inv}}^n\} := \bigvee_{1 \leq i \leq n} E_{l_i, \text{inv}}^i \bigvee \bigvee_{K \in \mathcal{S}} F_{l_i, \text{inv}}^K \end{aligned}$$

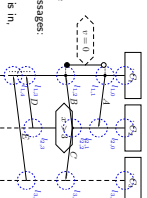


– 18 – 2013-01-22 – Shalom –

427

Loops

- How long may we legally stay at a cut q^i ?
- **Intuition:** those $(\text{Pr}_i, \text{cons}_i, \text{Stnd}_i)$ are allowed to fire the self-loop (q, ψ, q) where
 - $\text{cons}_i \cup \text{Stnd}_i$ comprises only irrelevant messages;
 - weak nodes from a direct successor cut is in;
 - strict nodes;
 - no message occurring in the LSC is in;
- And nothing else.
- **Formally:** Let $F^i := F^i \cup \dots \cup F^n$ be the union of the firesets of q^i .
- $\psi := \bigwedge_{\text{weak } F^i} \mathcal{E}(F^i) \bigvee_{\text{strict } F^i} \text{true}$

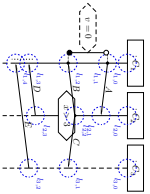


– 18 – 2013-01-22 – Shalom –

437

Progress

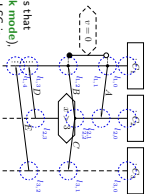
- When do we move from q to q' ?



44/77

Progress

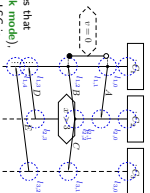
- When do we move from q to q' ?
- **Intuition:** those $(\sigma_i, \text{omns}_i, \text{Std}_i)$ fire the progress transition (q, ψ, q') for which there exists a freelist F such that $q \rightsquigarrow_F q'$ and $\text{omns}_i \cup \text{Std}_i$ comprises exactly the messages that distinguish F from other freelists of q (weak order) and in addition messages occurring in the LSC is in $\text{omns}_i \cup \text{Std}_i$ (strict mode).
- **Formally:** the linearizability condition relevant at q'



44/77

Progress

- When do we move from q to q' ?
- **Intuition:** those $(\sigma_i, \text{omns}_i, \text{Std}_i)$ fire the progress transition (q, ψ, q') for which there exists a freelist F such that $q \rightsquigarrow_F q'$ and $\text{omns}_i \cup \text{Std}_i$ comprises exactly the messages that distinguish F from other freelists of q (weak order) and in addition messages occurring in the LSC is in $\text{omns}_i \cup \text{Std}_i$ (strict mode).
- **Formally:** Let F, F_1, \dots, F_n be the freelists of q and let $q \rightsquigarrow_F q'$ (unique)
- $\psi := \bigwedge \ell(F) \wedge \neg (\ell(F_1) \vee \dots \vee \ell(F_n)) \wedge \ell(F)$
- $\psi := \bigwedge_{\text{weak } F} \ell(F)$

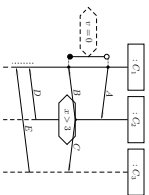


44/77

Step II: Conditions and Local Invariants

Some More Helper Functions

- **Constraints relevant at cut q :**
- $\psi_0(q) = \{\psi \mid \exists l \in q, l' \notin q \mid (l, \psi, \theta, l') \in \text{Local} \vee (l', \psi, \theta, l) \in \text{Local}\}$
- $\psi_l(q) = \psi_{\text{local}(q)} \cup \psi_{\text{local}(l)}$
- $\bigwedge \psi := \text{false}; \bigwedge_{1 \leq l \leq |S|} \psi_{l_1} := \bigwedge_{1 \leq l \leq |S|} \psi_l$



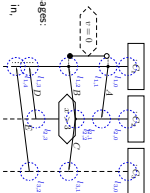
45/77

45/77

46/77

Loops with Conditions

- How long may we **legally** stay at a cut q^i ?
- **Intuition:** those $(\sigma_i, \text{omns}_i, \text{Std}_i)$ are allowed to fire the self-loop (q, ψ, q) where $\text{omns}_i \cup \text{Std}_i$ comprises only relevant messages:
- weak nodes: from a direct successor cut b in
- strict mode: no message occurring in the LSC is in
- **And nothing else.**
- **Formally:** Let $F := F_1 \cup \dots \cup F_n$ be the union of the freelists of q
- $\psi := \neg \bigwedge_{\text{weak } F} \ell(F) \vee \bigwedge_{\text{strict } F} \ell(F)$



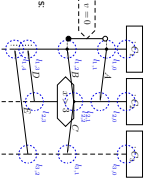
47/77

47/77

Loops with Conditions

- How long may we legally stay at a cut q ?
- **Intuition:** those $(\sigma_i, \text{cons}_i, \text{Stid}_i)$ are allowed to fire the self-loop (q, ψ, q) where
 - $\text{cons}_i \cup \text{Stid}_i$ comprises only irrelevant messages
 - weak nodes from a direct successor cut is in,
 - strict nodes
 - no message occurring in the LSC is in,
- σ_i satisfies the local invariants active at q
- And nothing else.
- **Formally:** Let $F := F_1 \cup \dots \cup F_n$ be the union of the freetimes of q .

$$\psi := \bigwedge_{\sigma \in \text{Free}(F)} \bigwedge_{\text{node } q' \in \text{node}}$$

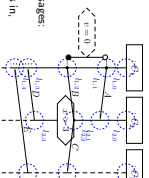


487/7

Loops with Conditions

- How long may we legally stay at a cut q ?
- **Intuition:** those $(\sigma_i, \text{cons}_i, \text{Stid}_i)$ are allowed to fire the self-loop (q, ψ, q) where
 - $\text{cons}_i \cup \text{Stid}_i$ comprises only irrelevant messages
 - weak nodes from a direct successor cut is in,
 - strict nodes
 - no message occurring in the LSC is in,
- σ_i satisfies the local invariants active at q
- And nothing else.
- **Formally:** Let $F := F_1 \cup \dots \cup F_n$ be the union of the freetimes of q .

$$\psi := \bigwedge_{\sigma \in \text{Free}(F)} \bigwedge_{\text{node } q' \in \text{node}}$$

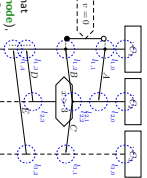


487/7

Progress with Conditions

- When do we move from q to q' ?
- **Intuition:** those $(\sigma_i, \text{cons}_i, \text{Stid}_i)$ fire the progress transition (q, ψ, q') for which there exists a freetime F such that $q \xrightarrow{\sigma_i} q'$ and
 - $\text{cons}_i \cup \text{Stid}_i$ comprises exactly the messages that distinguish F from other freetimes of q (weak nodes), and no other messages occurring in the LSC is in $\text{cons}_i \cup \text{Stid}_i$ (strict nodes).
 - σ_i satisfies the local invariants and conditions relevant at q' .
- **Formally:** Let F_1, F_2, \dots, F_n be the freetimes of q and let $q \xrightarrow{\sigma_i} q'$ (unique)

$$\psi := \bigwedge_{\sigma \in \text{Free}(F)} \bigwedge_{\text{node } q' \in \text{node}} \bigwedge_{\text{node } q'' \in \text{node}} \bigwedge_{\text{node } q''' \in \text{node}}$$

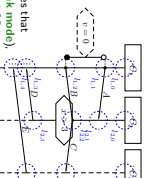


489/7

Progress with Conditions

- When do we move from q to q' ?
- **Intuition:** those $(\sigma_i, \text{cons}_i, \text{Stid}_i)$ fire the progress transition (q, ψ, q') for which there exists a freetime F such that $q \xrightarrow{\sigma_i} q'$ and
 - $\text{cons}_i \cup \text{Stid}_i$ comprises exactly the messages that distinguish F from other freetimes of q (weak nodes), and no other messages occurring in the LSC is in $\text{cons}_i \cup \text{Stid}_i$ (strict nodes).
 - σ_i satisfies the local invariants and conditions relevant at q' .
- **Formally:** Let F_1, F_2, \dots, F_n be the freetimes of q and let $q \xrightarrow{\sigma_i} q'$ (unique)

$$\psi := \bigwedge_{\sigma \in \text{Free}(F)} \bigwedge_{\text{node } q' \in \text{node}} \bigwedge_{\text{node } q'' \in \text{node}} \bigwedge_{\text{node } q''' \in \text{node}}$$



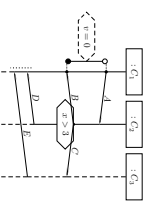
489/7

Even More Helper Functions

- **Constraints relevant when moving from q to cut q' :**

$$\psi_{\text{cut}}(q, q') = \{ \psi \mid \exists I \subseteq \mathcal{S}^1 \mid (I, \psi, I) \in \text{Cond} \wedge I \cap (q' \setminus \psi) \neq \emptyset \} \cup \psi_{\text{cut}}(q)$$

$$\{ \psi \mid \exists I \in \mathcal{S}^1 \setminus q, I \in \mathcal{S}^1 \mid (I, \psi, I) \in \text{Loctiv} \vee (I \bullet \text{cap}_i, \theta, \bullet, i) \in \text{Loctiv} \} \cup \{ \psi \mid \exists I \in \mathcal{S}^1 \setminus q, I \in \mathcal{S}^1 \mid (I \bullet \text{cap}_i, \theta, i, j) \in \text{Loctiv} \vee (I \bullet \text{cap}_j, \theta, j, i) \in \text{Loctiv} \}$$
- $\psi_{\text{local}}(q, q') = \psi_{\text{weak}}(q, q') \cup \psi_{\text{local}}(q, q')$

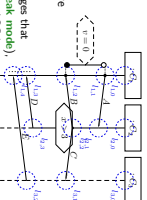


488/7

Progress with Conditions

- When do we move from q to q' ?
- **Intuition:** those $(\sigma_i, \text{cons}_i, \text{Stid}_i)$ fire the progress transition (q, ψ, q') for which there exists a freetime F such that $q \xrightarrow{\sigma_i} q'$ and
 - $\text{cons}_i \cup \text{Stid}_i$ comprises exactly the messages that distinguish F from other freetimes of q (weak nodes), and no other messages occurring in the LSC is in $\text{cons}_i \cup \text{Stid}_i$ (strict nodes).
 - σ_i satisfies the local invariants and conditions relevant at q' .
- **Formally:** Let F_1, F_2, \dots, F_n be the freetimes of q and let $q \xrightarrow{\sigma_i} q'$ (unique)

$$\psi := \bigwedge_{\sigma \in \text{Free}(F)} \bigwedge_{\text{node } q' \in \text{node}} \bigwedge_{\text{node } q'' \in \text{node}} \bigwedge_{\text{node } q''' \in \text{node}}$$



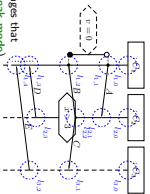
489/7

Step III: Cold Conditions and Cold Local Invariants

50/77

Legal Exits

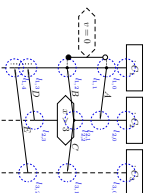
- When do we take a legal exit from q^i ?
- **Intuition:** those $(q^i, \text{cons}_i, \text{Stid}_i)$ fire the legal exit transition $(q^i, \psi_i, \mathcal{L}^i)$
 - for which there exists a freenet F and some q^j such that $q \rightsquigarrow q^j$ and
 - $\text{cons}_i \cup \text{Stid}_i$ comprises exactly the messages that distinguish F from other freenets of q^i (weak mode) and in addition no message occurring in the LSC is in $\text{cons}_i \cup \text{Stid}_i$ (strict mode) and
 - at least one cold condition or local invariant relevant when moving to q^j is violated, or
 - for which there is no matching freenet and at least one cold local invariant relevant at q^i is violated.
- **Formally:** Let F_1, \dots, F_n be the freenets of q with $q \rightsquigarrow q^i, q^j$.
 - $\psi_i := \bigvee_{n=1}^n \bigwedge \delta(F_n) \wedge \neg \bigvee \delta(F) \cup \dots \cup \delta(F_n) \setminus \delta(F_i) \wedge \bigvee \text{Weak}(q, q^i)$
 - $\psi_j := \bigvee_{n=1}^n \bigwedge \delta(F_n) \wedge \bigvee \text{Weak}(q)$



51/77

Legal Exits

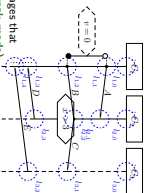
- When do we take a legal exit from q^i ?



51/77

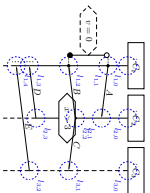
Legal Exits

- When do we take a legal exit from q^i ?
- **Intuition:** those $(q^i, \text{cons}_i, \text{Stid}_i)$ fire the legal exit transition $(q^i, \psi_i, \mathcal{L}^i)$
 - for which there exists a freenet F and some q^j such that $q \rightsquigarrow q^j$ and
 - $\text{cons}_i \cup \text{Stid}_i$ comprises exactly the messages that distinguish F from other freenets of q^i (weak mode) and in addition no message occurring in the LSC is in $\text{cons}_i \cup \text{Stid}_i$ (strict mode) and
 - at least one cold condition or local invariant relevant when moving to q^j is violated, or
 - for which there is no matching freenet and at least one cold local invariant relevant at q^i is violated.



51/77

Example



52/77

Finally: The LSC Semantics

- A full LSC L consist of
 - a body L $(\mathcal{L}^i, \rightarrow, \sim, \mathcal{L}^i, \text{Msg}, \text{Cond}, \text{Lock})$,
 - an activation condition (here: event) $ac = E_{i_1, i_2}^i, E \in \mathcal{E}, i_1, i_2 \in I$,
 - an activation mode, either initial or invariant,
 - a chart mode, either existential (cold) or universal (hot).

53/77

A full LSC L consist of

- a body $(L, \mathcal{L}^{\rightarrow}, \sim, \mathcal{L}^{\leftarrow}, \text{Msg}, \text{Cond}, \text{Lochv})$,
- an activation condition (here, event) $\text{ac} = E_{i_1, i_2}^+, E \in \mathcal{E}, i_1, i_2 \in I$,
- an activation mode, either *initial* or *invariant*,
- a chart mode, either *existential* (cold) or *universal* (hot)

A set W of words over $\mathcal{L}^{\rightarrow}$ and \mathcal{L}^{\leftarrow} satisfies L , denoted $W \models L$, iff L

- **universal** (= hot), **initial**, and
 $\forall w \in W \forall \beta : I \rightarrow \text{dom}(cr(w^{\beta})) \bullet w$ activates $L \implies w \in C_{\beta}(B_L)$.
- **existential** (= cold), **initial**, and
 $\exists w \in W \exists \beta : I \rightarrow \text{dom}(cr(w^{\beta})) \bullet w$ activates $L \wedge w \in C_{\beta}(B_L)$.
- **universal** (= hot), **invariant**, and
 $\forall w \in W \forall k \in \mathbb{N}_0 \forall \beta : I \rightarrow \text{dom}(cr(w^{\beta})) \bullet w/k$ activates $L \implies w/k \in C_{\beta}(B_L)$.
- **existential** (= cold), **invariant**, and
 $\exists w \in W \exists k \in \mathbb{N}_0 \exists \beta : I \rightarrow \text{dom}(cr(w^{\beta})) \bullet w/k$ activates $L \wedge w/k \in C_{\beta}(B_L)$.

53/77

References

76/77

References

[Damm and Harel, 2001] Damm, W. and Harel, D. (2001). LSCs: Breathing life into Message Sequence Charts. *Formal Methods in System Design*, 19(1):45–80.

[Fecher and Schönborn, 2007] Fecher, H. and Schönborn, J. (2007). UML 2.0 state machines: A formal semantics. In *Proceedings of the 11th International Conference on Software Engineering and Formal Methods (SEFM’07)*, volume 4386 of LNCS, pages 244–260. Springer, MA, and on de Pol, J. editor. *FMICS’07/ICFMT’07*, volume 4386 of LNCS, number TUM-10323. IEEE Computer, 2007:31–42.

[Harel and Gery, 1997] Harel, D. and Gery, E. (1997). Executable object modeling with statecharts. *IEEE Computer*, 30(7):31–42.

[Harel and Miozzo, 2007] Harel, D. and Miozzo, S. (2007). Assert and negate related: Model semantics for UML sequence diagrams. *Software and System Modeling (SSoM’07)*. (Early version in SCSM’06, 2006, pp. 13–20).

[Harel and Mardalyi, 2003] Harel, D. and Mardalyi, R. (2003). *Come, Let’s Play: Scenario-Based Programming Using LSCs and the Play-Engine*. Springer-Verlag.

[Klose, 2003] Klose, J. (2003). *LSCs: A Graphical Formalism for the Specification of Communication Behavior*. PhD thesis, Carl von Ossietzky Universität Oldenburg.

[OMG, 2007a] OMG (2007a). Unified modeling language: Infrastructure, version 2.1.2. Technical Report formal/07-11-02.

[OMG, 2007b] OMG (2007b). Unified modeling language: Superstructure, version 2.1.2. Technical Report formal/07-11-02.

[Stern, 2003] Stern, H. (2003). Assert, negate and refinement in UML 2 interactions. In Jippen, J., Frensch, B., France, R. and Fernandez, E. B., editors. *CSO/UML 2003*, number TUM-10323. Technische Universität München.

77/77