Contents & Goals

Last Lecture:
- LSC intuition
- LSC abstract syntax

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 Büchi Automata (TBA) and its (accepted) language.
  - Words of a model.
  - LSC formal semantics.
Excursus: Symbolic Büchi Automata (over Signature)

Symbolic Büchi Automata

Definition. A **Symbolic Büchi Automaton** (TBA) is a tuple

\[ B = (\text{Expr}_B(X), X, Q, q_{\text{ini}}, \rightarrow, Q_F) \]

where

- \( X \) is a set of logical variables,
- \( \text{Expr}_B(X) \) is a set of Boolean expressions over \( X \),
- \( Q \) is a finite set of **states**, 
- \( q_{\text{ini}} \in Q \) is the initial state,
- \( \rightarrow \subseteq Q \times \text{Expr}_B(X) \times Q \) is the **transition relation**. Transitions \((q, \psi, q')\) from \( q \) to \( q' \) are labelled with an expression \( \psi \in \text{Expr}_B(X) \).
- \( Q_F \subseteq Q \) is the set of **fair** (or accepting) states.
**Definition.** Let $X$ be a set of logical variables and let $\text{Expr}_B(X)$ be a set of Boolean expressions over $X$.

A set $(\Sigma, \models)$ is called an alphabet for $\text{Expr}_B(X)$ if and only if

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

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

An infinite sequence

$$w = (\sigma_i)_{i \in \mathbb{N}_0} \in \Sigma^\omega$$

over $(\Sigma, \models)$ is called word for $\text{Expr}_B(X)$. 

---

$Q = \{ q_1, \ldots, q_6 \}$

$\forall \bar{x} = \bar{z}_1$

$Q_{\text{F}} = \{ q_5 \}$

$X = \{ x, y, z \}$

$\text{Expr}(X) = a(x, y) \lor \neg \text{expr} \lor \neg \text{expr}$

$\rightarrow = \{ (q_1, a(x, y), q_5), \ldots \}$
Word Example

\[ w = (q_0, (x,y) \rightarrow 0, (x,y) \rightarrow 4, \ldots) \]
\[ b_0' = \left( \begin{array}{c} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{array} \right), \]
\[ q_1' = \left( \begin{array}{c} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{array} \right) \]

Run of TBA over Word

**Definition.** Let \( B = (\text{Expr}_B(X), X, Q, q_{\text{ini}}, \rightarrow, Q_F) \) be a TBA and
\[ w = \sigma_1, \sigma_2, \sigma_3, \ldots \]
a word for \( \text{Expr}_B(X) \).

An infinite sequence
\[ q = q_0, q_1, q_2, \ldots \in Q^\omega \]
is called a **run** of \( B \) over \( w \) under valuation \( \beta : X \rightarrow \mathcal{P}(X) \) if and only if
- \( q_0 = q_{\text{ini}}, \)
- for each \( i \in \mathbb{N}_0 \) there is a transition \((q_i, \psi_i, q_{i+1}) \in \rightarrow \) of \( B \) such that \( \sigma_i \models \beta \psi_i \).
Run Example

\[ q = q_0, q_1, q_2, \ldots \in Q^\omega \text{ s.t. } \sigma_i \models \psi_i, i \in \mathbb{N}_0. \]

The Language of a TBA

**Definition.**

We say \( B \) **accepts** word \( w \) (under \( \beta \)) if and only if \( B \) **has a run**

\[ q = (q_i)_{i \in \mathbb{N}_0} \]

over \( w \) such that fair (or accepting) states are **visited infinitely often** by \( q \), i.e., such that

\[ \forall i \in \mathbb{N}_0 \exists j > i : q_j \in Q_F. \]

We call the set \( \mathcal{L}_\beta(B) \subseteq \Sigma^\omega \) of words for \( \text{Expr}_B(X) \) that are accepted by \( B \) the **language of** \( B \).
Language of the Example TBA

$L_\beta(B)$ consists of the words

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

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

- for $0 \leq i < n$, $\sigma_i \models \beta_{E_x, y}$
- $\sigma_n \models \beta_{E_x, y}$
- for $n < i < m$, $\sigma_i \models \beta_{E_x, y}$
- $\sigma_m \models \beta_{E_x, y}$
- for $m < i < k$, $\sigma_i \models \beta_{F_y, x}$
- $\sigma_k \models \beta_{F_y, x}$
- for $k < i < \ell$, $\sigma_i \not\models \beta_{F_y, x}$
- ...

Course Map

UML

Mathematics

Model

Instances

G = (N, E, f)

OD

$\varphi \in \text{OCL}$

$\mathcal{P} = (\mathcal{F}, \varnothing, V, \text{attr})$, SM

EXPR

$\mathcal{M} = (\Sigma_{\mathcal{F}}, A_{\mathcal{F}}, \neg_{\text{SM}})$

$B = (Q_{\text{SD}}, q_0, A_{\mathcal{F}}, \neg_{\text{SD}}, F_{\text{SD}})$

$\pi = (\sigma_0, \epsilon_0, \text{cons}_0, \text{Snd}_0, \sigma_1, \epsilon_1, \text{cons}_1, \text{Snd}_1, \ldots, \sigma_n, \epsilon_n, \text{cons}_n, \text{Snd}_n)$

$w_i = ((\sigma_i, \text{cons}_i, \text{Snd}_i))_{i \in \mathbb{N}}$
Words over Signature

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

$$(\sigma_i, cons_i, Snd_i)_{i \in \mathbb{N}_0} \in \left( \Sigma_{\mathcal{D}} \times 2^{\mathcal{G}(\mathcal{F})} \times \text{Ev}(\mathcal{F}, \mathcal{D}) \times \mathcal{D}(\mathcal{F}) \times 2^{\mathcal{G}(\mathcal{F})} \times \text{Ev}(\mathcal{F}, \mathcal{D}) \times \mathcal{D}(\mathcal{F}) \right) \omega.$$
**The Language of a Model**

**Recall:** A UML model \( \mathcal{M} = (\mathcal{C}, \mathcal{I}, \mathcal{O}, \mathcal{D}) \) and a structure \( \mathcal{D} \) denotes a set \([\mathcal{M}]\) of (initial and consecutive) **computations** of the form

\[
(\sigma_0, \varepsilon_0) \xrightarrow{a_0} (\sigma_1, \varepsilon_1) \xrightarrow{a_1} (\sigma_2, \varepsilon_2) \xrightarrow{a_2} \ldots
\]

where

\[
a_i = (cons_i, Snd_i, u_i) \in 2^{\mathcal{D}(\mathcal{E})} \times \mathcal{E}(\mathcal{D}) \times 2^{\mathcal{D}(\mathcal{E})} \times \mathcal{E}(\mathcal{D}) \times 2^{\mathcal{D}(\mathcal{E})}.
\]

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 \( \mathcal{M} = (\mathcal{C}, \mathcal{I}, \mathcal{O}, \mathcal{D}) \) be a UML model and \( \mathcal{D} \) a structure. Then

\[
\mathcal{L}(\mathcal{M}) := \{(\sigma_i, cons_i, Snd_i)_{i \in \mathbb{N}_0} \in (\Sigma^{\mathcal{D}} \times \hat{A})^\omega \mid \exists (\varepsilon_i, u_i)_{i \in \mathbb{N}_0} : (\sigma_0, \varepsilon_0) \xrightarrow{(cons_0, Snd_0)} u_0 (\sigma_1, \varepsilon_1) \ldots \in [\mathcal{M}]\}
\]

is the **language** of \( \mathcal{M} \).

---

**Example: The Language of a Model**

\[
\mathcal{L}(\mathcal{M}) := \{(\sigma_i, cons_i, Snd_i)_{i \in \mathbb{N}_0} \in (\Sigma^{\mathcal{D}} \times \hat{A})^\omega \mid \exists (\varepsilon_i, u_i)_{i \in \mathbb{N}_0} : (\sigma_0, \varepsilon_0) \xrightarrow{(cons_0, Snd_0)} u_0 (\sigma_1, \varepsilon_1) \ldots \in [\mathcal{M}]\}
\]
Signal and Attribute Expressions

- Let $\mathcal{S} = (\mathcal{S}, \mathcal{E}, V, atr, \mathcal{E})$ be a signature and $X$ a set of logical variables.

- The signal and attribute expressions $Expr_{\mathcal{S}}(\mathcal{E}, X)$ are defined by the grammar:

$$\psi ::= \text{true} \mid expr \mid E_x \mid E_y \mid \neg \psi \mid \psi_1 \lor \psi_2,$$

where $expr : \text{Bool} \in Expr_{\mathcal{S}}, E \in \mathcal{E}, x, y \in X$.

Satisfaction of Signal and Attribute Expressions

- Let $(\sigma, cons, Snd) \in \Sigma_{\mathcal{S}} \times \mathcal{A}$ be a triple consisting of system state, consume set, and send set.

- Let $\beta : X \rightarrow \mathcal{S}(\mathcal{E})$ be a valuation of the logical variables.

Then

- $(\sigma, cons, Snd) \models_{\beta} \text{true}$
- $(\sigma, cons, Snd) \models_{\beta} \neg \psi$ if and only if not $(\sigma, cons, Snd) \models_{\beta} \psi$
- $(\sigma, cons, Snd) \models_{\beta} \psi_1 \lor \psi_2$ if and only if $(\sigma, cons, Snd) \models_{\beta} \psi_1$ or $(\sigma, cons, Snd) \models_{\beta} \psi_2$
- $(\sigma, cons, Snd) \models_{\beta} expr$ if and only if $I(expr)(\sigma, \beta) = 1$
- $(\sigma, cons, Snd) \models_{\beta} E_x \if \text{and only if } \exists \vec{d} \bullet (\beta(x), (E, \vec{d}), \beta(y)) \in Snd$
- $(\sigma, cons, Snd) \models_{\beta} E_y \if \text{and only if } \exists \vec{d} \bullet (\beta(x), (E, \vec{d}), \beta(y)) \in cons$

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.
**TBA over Signature**

Definition. A TBA

\[ \mathcal{B} = (\text{Expr}_\mathcal{B}(X), X, Q, q_{\text{init}}, \rightarrow, Q_F) \]

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

- Any word over \( \mathcal{S} \) and \( \mathcal{D} \) is then a word for \( \mathcal{B} \).
  (By the satisfaction relation defined on the previous slide; \( \mathcal{D}(X) = \mathcal{D}(\mathcal{S}) \).)

- Thus a TBA over \( \mathcal{S} \) accepts words of models with signature \( \mathcal{S} \).
  (By the previous definition of TBA.)

---

**TBA over Signature Example**

\[ (\sigma, \text{cons}, \text{Snd}) \models_{\text{B}} \text{expr} \iff I[\text{expr}](\sigma, \beta) = 1; \]

\[ (\sigma, \text{cons}, \text{Snd}) \models_{\text{B}} E_{x,y} \iff (\beta(x), (E, d), \beta(y)) \in \text{Snd} \]
Course Map

Mathematics

Live Sequence Charts Semantics
**TBA-based Semantics of LSCs**

**Plan:**
- Given an LSC $L$ with body
  \[(I, (\mathcal{L}, \preceq), \sim, \mathcal{R}, \text{Msg, Cond, LocInv}),\]
- 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: Intuitive Semantics**

(i) **Strictly After:**

(ii) **Simultaneously:** (simultaneous region)

(iii) **Explicitly Unordered:** (co-region)

**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 Cuts!**

**Definition.**

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

- it is **downward closed**, i.e.
  \[
  \forall l, l' : l', l \in C \wedge l \preceq l' \implies l \in C,
  \]

- it is **closed** under simultaneity, i.e.
  \[
  \forall l, l' : l, l' \in C \wedge l \sim l' \implies l \in C, \text{ and}
  \]

- it comprises at least **one location per instance line**, i.e.
  \[
  \forall i \in I \exists l \in C : i_l = i.
  \]

A cut \(C\) is called **hot**, denoted by \(\theta(C) = \text{hot}\), if and only if at least one of its maximal elements is hot, i.e. if

\[
\exists l \in C : \theta(l) = \text{hot} \wedge \not\exists l' \in C : l \prec l'
\]

Otherwise, \(C\) is called **cold**, denoted by \(\theta(C) = \text{cold}\).
Examples: Cut or Not Cut? Hot/Cold?

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

$C_0 = \emptyset$
$C_1 = \{l_1,0,l_2,0,l_3,0\}$
$C_2 = \{l_1,1,l_2,1,l_3,0\}$
$C_3 = \{l_1,0,l_1,1\}$
$C_4 = \{l_1,0,l_1,1,l_2,0,l_3,0\}$
$C_5 = \{l_1,0,l_1,1,l_2,0,l_2,1,l_3,0\}$
$C_6 = \mathcal{L} \setminus \{l_1,3,l_2,3\}$
$C_7 = \mathcal{L}$

A Successor Relation on Cuts

The partial order of $(\mathcal{L}, \preceq)$ and the simultaneity relation "~" 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 $(\mathcal{L}, \preceq)$ and messages $\text{Msg}$.

$C'$ is called **direct successor** of $C$ via **fired-set** $F$, denoted by $C \xrightarrow{F} C'$, 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.
  
  $\forall l, l' \in F : l \neq l' \land i_l = i_{l'} \implies l \not\preceq l' \land l' \not\preceq l$.
Properties of the Fired-set

\( C \sim_F C' \) 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
- \( \forall l, l' \in F : l \neq l' \land i_l = i_{l'} \implies l \not{\leq} l' \land l' \not{\leq} l \)

**Note:** \( F \) is closed under simultaneity.

**Note:** locations in \( F \) are direct \( \preceq \)-successors of locations in \( C \), i.e.

\[ \forall l' \in F \exists l \in C : l \prec l' \land \exists l'' \in C : l' \prec l'' \prec l \]

Successor Cut Examples

(i) \( F \neq \emptyset \), (ii) \( C' \setminus C = F \),
(iii) \( \forall (l, E, l') \in \text{Msg} : l' \in F \implies l \in C \), and
(iv) \( \forall l, l' \in F : l \neq l' \land i_l = i_{l'} \implies l \not{\leq} l' \land l' \not{\leq} l \)
Idea: Accept Timed Words by Advancing the Cut

- Let $w = (\sigma_0, \text{cons}_0, \text{Snd}_0), (\sigma_1, \text{cons}_1, \text{Snd}_1), (\sigma_2, \text{cons}_2, \text{Snd}_2), \ldots$ be a word of a UML model and $\beta$ a valuation of $I \cup \{\text{self}\}$.

- Intuitively (and for now disregarding cold conditions), an LSC body $(I,(\mathcal{L},\preceq),\sim,\mathcal{P},\text{Msg},\text{Cond},\text{LocInv})$ is supposed to accept $w$ if and only if there exists a sequence
  
  $$C_0 \xrightarrow{F_1} C_1 \xrightarrow{F_2} C_2 \cdots \xrightarrow{F_n} C_n$$

  and indices $0 = i_0 < i_1 < \cdots < i_n$ such that for all $0 \leq j < n$,

  - for all $i_j \leq k < i_{j+1}$, $(\sigma_k, \text{cons}_k, \text{Snd}_k), \beta$ satisfies the hold condition of $C_j$,
  - $(\sigma_{i_j}, \text{cons}_{i_j}, \text{Snd}_{i_j}), \beta$ satisfies the transition condition of $F_j$,
  - $C_n$ is cold,
  - for all $i_n < k$, $(\sigma_k, \text{cons}_{i_j}, \text{Snd}_{i_j}), \beta$ satisfies the hold condition of $C_n$.

Language of LSC Body

The language of the body

$$(I,(\mathcal{L},\preceq),\sim,\mathcal{P},\text{Msg},\text{Cond},\text{LocInv})$$

of LSC $L$ is the language of the TBA

$$B_L = (\text{Expr}_B(X),X,Q,q_{\text{ini}},\rightarrow,Q_F)$$

with

- $\text{Expr}_B(X) = \text{Expr}_B(\mathcal{P},X)$
- $Q$ is the set of cuts of $(\mathcal{L},\preceq)$, $q_{\text{ini}}$ is the instance heads cut,
- $F = \{C \in Q \mid \theta(C) = \text{cold}\}$ is the set of cold cuts of $(\mathcal{L},\preceq)$,
- $\rightarrow$ as defined in the following, consisting of
  - loops $(q,\psi,q)$,
  - progress transitions $(q,\psi,q')$ corresponding to $q \xrightarrow{F} q'$, and
  - legal exits $(q,\psi,\mathcal{L})$. 


Language of LSC Body: Intuition

$B_L = (\text{Expr}_B(X), X, Q, q_{\text{ini}}, \rightarrow, Q_F)$ with

- $\text{Expr}_B(X) = \text{Expr}_{\mathcal{B}}(\mathcal{A}, X)$
- $Q$ is the set of cuts of $(\mathcal{L}, \preceq)$, $q_{\text{ini}}$ is the instance heads cut,
- $F = \{C \in Q \mid \theta(C) = \text{cold}\}$ is the set of cold cuts,
- $\rightarrow$ consists of
  - loops $(q, \psi, q)$,
  - progress transitions $(q, \psi, q')$ corresponding to $q \rightarrow^F q'$, and
  - legal exits $(q, \psi, \mathcal{L})$.

Step I: Only Messages
Some Helper Functions

- **Message-expressions of a location**:
  \[
  \delta(l) := \{E_{i_j}^j, i_j | (l, E, l') \in \text{Msg} \} \cup \{E_{i_j}^j, i_j' | (l', E, l) \in \text{Msg} \},
  \]
  \[
  \delta([l_1, \ldots, l_n]) := \delta(l_1) \cup \ldots \cup \delta(l_n).
  \]

\[
\bigvee \emptyset := \text{true}; \bigvee \{E_{i_1}^{k_1}, \ldots F_{i_k}^{k_k} \} := \bigvee_{1 \leq j < k} E_{i_j} \bigvee_{k \leq j} F_{i_j}
\]

Loops

- How long may we legally stay at a cut \( q \)?
- **Intuition**: those \((\sigma_i, \text{cons}_i, \text{Snd}_i)\) are allowed to fire the self-loop \((q, \psi, q)\) where
  - \(\text{cons}_i \cup \text{Snd}_i\) comprises only irrelevant messages:
    - **weak mode**: no message from a direct successor cut is in,
    - **strict mode**: no message occurring in the LSC is in,
  - \(\sigma_i\) satisfies the local invariants active at \( q \)

And nothing else.

- **Formally**: Let \( F := F_1 \cup \ldots \cup F_n \) be the union of the firedsets of \( q \).\]
  \[
  \psi := \neg \left( \bigvee \delta(F) \right) \land \psi(q).
  \]
  \[
  = \text{true if } F = \emptyset
  \]
Progress

- When do we move from $q$ to $q'$?

**Intuition:** those $(\sigma_i, \text{cons}_i, \text{Snd}_i)$ fire the progress transition $(q, \psi, q')$ for which there exists a firedset $F$ such that $q \xrightarrow{F} q'$ and

- $\text{cons}_i \cup \text{Snd}_i$ comprises exactly the messages that distinguish $F$ from other firedsets of $q$ (weak mode), and in addition no message occurring in the LSC is in $\text{cons}_i \cup \text{Snd}_i$ (strict mode),

- $\sigma_i$ satisfies the local invariants and conditions relevant at $q$

**Formally:** Let $F, F_1, \ldots, F_n$ be the firedsets of $q$ and let $q \xrightarrow{F} q'$ (unique).

\[ \psi := \bigwedge F \land \neg \bigvee F_1 \lor \cdots \lor F_n \land \bigwedge F \lor \psi(q, q'). \]

---

**Step II: Conditions and Local Invariants**
Some More Helper Functions

- **Constraints** relevant at cut $q$:

  $\psi(q) = \{ \psi \mid \exists l \in q, l' \notin q \mid (l, \psi, \theta, l') \in \text{LocInv} \lor (l', \psi, \theta, l) \in \text{LocInv} \}$,

  $\psi(q) = \psi_{\text{hot}}(q) \cup \psi_{\text{cold}}(q)$

  $\bigwedge \emptyset := \text{false}; \quad \bigwedge \{ \psi_1, \ldots, \psi_n \} := \bigwedge_{1 \leq i \leq n} \psi_i$

Loops with Conditions

- How long may we **legally** stay at a cut $q$?

- **Intuition**: those $(\sigma_i, \text{cons}_i, \text{Snd}_i)$ are allowed to fire the self-loop $(q, \psi, q)$ where

  - $\text{cons}_i \cup \text{Snd}_i$ comprises only irrelevant messages:
    - **weak mode**: no message from a direct successor cut is in,
    - **strict mode**: no message occurring in the LSC is in,
  - $\sigma_i$ satisfies the local invariants active at $q$

  And nothing else.

- **Formally**: Let $F := F_1 \cup \cdots \cup F_n$

  be the union of the firedsets of $q$.

  $\psi := \neg(\bigvee \delta(F)) \land \bigwedge \psi(q)$.

  = **true if $F = \emptyset$**
**Even More Helper Functions**

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

  $$
  \psi_0(q, q') = \{ \psi \mid \exists L \subseteq \mathcal{L} \mid (L, \psi, \theta) \in \text{Cond} \land L \cap (q' \setminus q) \neq \emptyset \} \\
  \cup \psi_0(q') \\
  \setminus \{ \psi \mid \exists l \in q' \setminus q, t' \in \mathcal{L} \mid (l, o, \text{expr}, \theta, t') \in \text{LocInv} \lor (l', \text{expr}, \theta, o, t) \in \text{LocInv} \} \\
  \cup \{ \psi \mid \exists l \in q' \setminus q, t' \in \mathcal{L} \mid (l, \bullet, \text{expr}, \theta, l') \in \text{LocInv} \lor (l', \text{expr}, \theta, \bullet, l) \in \text{LocInv} \}
  $$

  $$
  \psi(q, q') = \psi_{\text{hot}}(q, q') \cup \psi_{\text{cold}}(q, q')
  $$

**Progress with Conditions**

- When do we move from $q$ to $q'$?

  - **Intuition**: those $(\sigma_i, \text{cons}_i, \text{Snd}_i)$ fire the progress transition $(q, \psi, q')$ for which there exists a firedset $F$ such that $q \leadsto_F q'$ and

    - $\text{cons}_i \cup \text{Snd}_i$ comprises exactly the messages that distinguish $F$ from other firedsets of $q$ (weak mode), and in addition no message occurring in the LSC is in $\text{cons}_i \cup \text{Snd}_i$ (strict mode),
    - $\sigma_i$ satisfies the local invariants and conditions relevant at $q'$.

  - **Formally**: Let $F, F_1, \ldots, F_n$ be the firedsets of $q$ and let $q \leadsto_F q'$ (unique).

    - $\psi := \bigwedge \mathcal{E}(F) \land \neg(\bigvee \{ \mathcal{E}(F_1) \cup \cdots \cup \mathcal{E}(F_n) \} \setminus \mathcal{E}(F)) \land \psi(q, q')$. 

Step III: Cold Conditions and Cold Local Invariants

Legal Exits

- When do we take a legal exit from \( q \)?
- **Intuition**: those \( (\sigma_i, \text{cons}_i, \text{Snd}_i) \) fire the legal exit transition \( (q, \psi, \mathcal{L}) \)
  - for which there exists a firedset \( F \) and some \( q' \) such that \( q \rightsquigarrow_F q' \) and
  - \( \text{cons}_i \cup \text{Snd}_i \) comprises exactly the messages that distinguish \( F \) from other firedsets of \( q \) (weak mode), and in addition no message occurring in the LSC is in \( \text{cons}_i \cup \text{Snd}_i \) (strict mode) and
    - at least one cold condition or local invariant relevant when moving to \( q' \) is violated, or
    - for which there is no matching firedset and
      - at least one cold local invariant relevant at \( q \) is violated.
- **Formally**: Let \( F_1, \ldots, F_n \) be the firedsets of \( q \) with \( q \rightsquigarrow_F q' \).
  - \( \psi := \bigwedge_{i=1}^n \delta(F_i) \land \neg(\bigvee(\delta(F_1) \cup \cdots \cup \delta(F_n)) \setminus \delta(F_i)) \land \bigvee_{i=1}^n \psi_{\text{cold}}(q, q'_i) \land \neg(\bigvee\delta(F_i)) \land \bigvee\psi_{\text{cold}}(q) \)
**Example**

Finally: The LSC Semantics

A full LSC $L$ consist of

- a **body** $(I, (L, \preceq), \sim, S, \text{Msg}, \text{Cond}, \text{LocInv})$,
- an **activation condition** (here: event) $ac = E_{i_1,i_2}^{r}, E \in S, i_1, i_2 \in I$,
- an **activation mode**, either **initial** or **invariant**,
- a **chart mode**, either **existential** (cold) or **universal** (hot).

A set $W$ of words over $S$ and $D$ **satisfies** $L$, denoted $W \models L$, iff $L$

- **universal** (\(=\) hot), **initial**, and
  \[ \forall w \in W \forall \beta : I \to \text{dom}(\sigma(w^0)) \bullet w \text{ activates } L \implies w \in L_\beta(B_L). \]
- **existential** (\(=\) cold), **initial**, and
  \[ \exists w \in W \exists \beta : I \to \text{dom}(\sigma(w^0)) \bullet w \text{ activates } L \wedge w \in L_\beta(B_L). \]
- **universal** (\(=\) hot), **invariant**, and
  \[ \forall w \in W \forall k \in \mathbb{N}_0 \forall \beta : I \to \text{dom}(\sigma(w^k)) \bullet w/k \text{ activates } L \implies w/k \in L_\beta(B_L). \]
- **existential** (\(=\) cold), **invariant**, and
  \[ \exists w \in W \exists k \in \mathbb{N}_0 \exists \beta : I \to \text{dom}(\sigma(w^k)) \bullet w/k \text{ activates } L \wedge w/k \in L_\beta(B_L). \]
Model Consistency wrt. Interaction

- We assume that the set of interactions \( \mathcal{I} \) is partitioned into two (possibly empty) sets of \textit{universal} and \textit{existential} interactions, i.e.

\[
\mathcal{I} = \mathcal{I}_\forall \cup \mathcal{I}_\exists.
\]

Definition. A model

\[
\mathcal{M} = (\mathcal{C}, \mathcal{M}, \mathcal{D}, \mathcal{I})
\]

is called \textit{consistent} (more precise: the constructive description of behaviour is consistent with the reflective one) if and only if

\[
\forall \mathcal{I} \in \mathcal{I}_\forall : \mathcal{L}(\mathcal{M}) \subseteq \mathcal{L}(\mathcal{I})
\]

and

\[
\forall \mathcal{I} \in \mathcal{I}_\exists : \mathcal{L}(\mathcal{M}) \cap \mathcal{L}(\mathcal{I}) \neq \emptyset.
\]
In UML, reflective (temporal) descriptions are subsumed by interactions. A UML model $M = (CD, LM, OD, I)$ has a set of interactions $I$. An interaction $I \in I$ can be (OMG claim: equivalently) diagrammed as

- sequence diagram,
- timing diagram, or
- communication diagram (formerly known as collaboration diagram).
Interactions as Reflective Description

- In UML, reflective (temporal) descriptions are subsumed by interactions.
- A UML model $M = (O, M, OD, J)$ has a set of interactions $J$.
- An interaction $I \in J$ can be (OMG claim: equivalently) diagrammed as
  - sequence diagram,
  - timing diagram, or
  - communication diagram (formerly known as collaboration diagram).

Why Sequence Diagrams?

Most Prominent: Sequence Diagrams — with long history:
- Message Sequence Charts, standardized by the ITU in different versions, often accused to lack a formal semantics.
- Sequence Diagrams of UML 1.x

Most severe drawbacks of these formalisms:
- unclear interpretation: example scenario or invariant?
- unclear activation: what triggers the requirement?
- unclear progress requirement: must all messages be observed?
- conditions merely comments
- no means to express forbidden scenarios
Thus: Live Sequence Charts

- SDs of UML 2.x address some issues, yet the standard exhibits unclarities and even contradictions [Harel and Maoz, 2007, Störrle, 2003]
- For the lecture, we consider Live Sequence Charts (LSCs) [Damm and Harel, 2001, Klose, 2003, Harel and Marelly, 2003], who have a common fragment with UML 2.x SDs [Harel and Maoz, 2007]
- Modelling guideline: stick to that fragment.

Side Note: Protocol Statemachines

Same direction: call orders on operations
- “for each C instance, method f() shall only be called after g() but before h()”

Can be formalised with protocol state machines.
References


