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.
$I = (\mathcal{I}, \mathcal{E}, V, \text{atr}), SM$

$M = (\Sigma_\mathcal{I}, A_\mathcal{I}, \rightarrow_{SM})$

$\pi = (\sigma_0, \varepsilon_0) \xrightarrow{(\text{cons}_0, \text{Snd}_0)} (\sigma_1, \varepsilon_1) \cdot \cdot \cdot$

$\varphi \in \text{OCL}$

$B = (Q_{SD}, q_0, A_\mathcal{I}, \rightarrow_{SD}, F_{SD})$

$w_\pi = ((\sigma_i, \text{cons}_i, \text{Snd}_i))_{i \in \mathbb{N}}$

$G = (N, E, f)$

$\mathcal{O}D$

Mathematics
\[ \Sigma = \{0, 1\} \]

\[ L(A) = \{01\}^*0 \]

\[ w_1 = 010100 \in L(A) \]

\[ w_2 = 011 \]

\[ w_3 = 0101 \in L(A) \]

\[ \Sigma = \{0, 1\} \]

\[ w_4 = 010101... \]

\[ L(B) = \{01\}^\omega \leftarrow \text{infinite repetition} \]

\[ \text{acceptance criterion: visit accepting state infinitely often} \]

\[ L(B') = (01)^*10^\omega \]

\[ \Sigma = \{0, 1\} \]

\[ w_5 = 001000... \]

\[ w_6 = 01\omega \]

\[ X = \{x, y, z\} \]

\[ \Sigma = \{\{0, 1\} \rightarrow \mathbb{Z}\} \]

\[ \exp: = x \mid \rho(x) \mid \text{even} (\exp) \mid \text{odd} (\exp) \]

\[ \text{functions from } \mathbb{Z}, \mathbb{Z} \text{ to } \mathbb{Z} \]

\[ L_B(2) \ni w \quad \text{if } \beta = \{x \rightarrow 0\} \]

\[ L_B(2) \not\ni w \quad \text{if } \beta = \{x \rightarrow 1\} \]

\[ \rho : (p: 0 \rightarrow 0, 1 \rightarrow 0), \]

\[ (p: 0 \rightarrow 1, 1 \rightarrow ?), \]

\[ (p: 0 \rightarrow 4, 1 \rightarrow 3), \]

\[ (p: 0 \rightarrow 0, 1 \rightarrow 2) \]

\[ \text{Symbolic Büchi automaton} \]
Excursus: Symbolic Büchi Automata (over Signature)
Symbolic Büchi Automata

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

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

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,
- \( q_{ini} \in Q \) 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.
TBA Example

\[(\text{Expr}_B(X), X, Q, q_{\text{ini}}, \rightarrow, Q_F), (q, \psi, q') \in \rightarrow,\]

\[Q = \{q_1, \ldots, q_7\}\]

\[q_{\text{ini}} = q_1\]

\[Q_\forall = \{q_3, q_6\}\]

\[X = \{x, y, z\}\]

\[\text{Expr}(X) = a(x, y, z) | \text{expr}/\neg\text{expr}/\ldots\]

\[\rightarrow = \{ (q_1, \neg a(x, y), q_4), \ldots \}\]
Definition. Let $X$ be a set of logical variables and let $Expr_B(X)$ be a set of Boolean expressions over $X$.

A set $(\Sigma, \cdot \models \cdot)$ is called an alphabet for $Expr_B(X)$ if and only if

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

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

An infinite sequence

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

over $(\Sigma, \cdot \models \cdot)$ is called word for $Expr_B(X)$. 
\( w = (a: (1,2) \rightarrow 0, \ (2,1) \rightarrow 1, \ldots \) \\
\( b: \ldots \) \\
\( e: \ldots ) \)
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

$$\varrho = q_0, q_1, q_2, \ldots \in Q^\omega$$

is called run of $B$ over $w$ under valuation $\beta : X \rightarrow \mathcal{D}(X)$ if and only if

- $q_0 = q_{\text{ini}},$
- 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

\[ \rho = q_0, q_1, q_2, \ldots \in Q^\omega \text{ s.t. } \sigma_i \models_{\beta} \psi_i, \ i \in \mathbb{N}_0. \]
Definition.
We say $B$ accepts word $w$ (under $\beta$) if and only if $B$ has a run
$$\varrho = (q_i)_{i \in \mathbb{N}_0}$$
over $w$ such that fair (or accepting) states are visited infinitely often by $\varrho$, 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 $Expr_B(X)$ that are accepted by $B$ the language of $B$. 

The Language of a TBA
\[ \mathcal{L}_\beta(\mathcal{B}) \] consists of the words

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

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

- for \( 0 \leq i < n \), \( \sigma_i \not\models_\beta E^i_{x,y} \)
- \( \sigma_n \models_\beta E^i_{x,y} \)
- for \( n < i < m \), \( \sigma_i \not\models_\beta E^i_{y} \)
- \( \sigma_m \models_\beta E^i_{y} \)
- for \( m < i < k \), \( \sigma_i \not\models_\beta E^i_{y,x} \)
- \( \sigma_k \models_\beta E^i_{y,x} \)
- for \( k < i < \ell \), \( \sigma_i \not\models_\beta E^i_{x,y} \)
- ...
Back to Main Track: Language of a Model
**Definition.** Let \( \mathcal{I} = (\mathcal{T}, \mathcal{C}, V, atr, \mathcal{E}) \) be a signature and \( \mathcal{D} \) a structure of \( \mathcal{I} \). A **word** over \( \mathcal{I} \) and \( \mathcal{D} \) is an infinite sequence

\[
(\sigma_i, cons_i, Snd_i)_{i \in \mathbb{N}_0} \\
\in \left( \sum_{\mathcal{D}} \times 2^{\mathcal{D}(C) \times Evs(\mathcal{E}, \mathcal{D}) \times \mathcal{D}(C)} \times 2^{\mathcal{D}(C) \times Evs(\mathcal{E}, \mathcal{D}) \times \mathcal{D}(C)} \right)^\omega.
\]
**The Language of a Model**

**Recall:** A UML model $\mathcal{M} = (\mathcal{C}, \mathcal{D}, \mathcal{S}, \mathcal{O})$ 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

$$ a_i = (\text{cons}_i, \text{Snd}_i, u_i) \in \mathcal{D}(\mathcal{C}) \times \text{Evs}(\mathcal{C}, \mathcal{O}) \times \mathcal{D}(\mathcal{C}) \times \mathcal{D}(\mathcal{C}) \times \mathcal{D}(\mathcal{C}) $$

$$ =: \tilde{A} $$

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

$$ \mathcal{L}(\mathcal{M}) := \{ (\sigma_i, \text{cons}_i, \text{Snd}_i) \in \mathcal{N} : (\Sigma_{\mathcal{C}} \times \tilde{A})^\omega | \}

\exists (\varepsilon_i, u_i) \in \mathcal{N} : (\sigma_0, \varepsilon_0) \xrightarrow{u_0} (\sigma_1, \varepsilon_1) \cdots \in [\mathcal{M}] \}

is the language of $\mathcal{M}$. 

Example: The Language of a Model

\[ \mathcal{L}(\mathcal{M}) := \left\{ (\sigma_i, cons_i, Snd_i)_{i \in \mathbb{N}_0} \in (\Sigma^\omega \times \tilde{A})^\omega \mid \right. \]

\[ \exists (\varepsilon_i, u_i)_{i \in \mathbb{N}_0} : (\sigma_0, \varepsilon_0) \xrightarrow{(cons_0, Snd_0)} (\sigma_1, \varepsilon_1) \cdots \in \llbracket \mathcal{M} \rrbracket \} \]
Signal and Attribute Expressions

• Let \( \mathcal{I} = (\mathcal{T}, \mathcal{C}, V, atr, \mathcal{E}) \) be a signature and \( X \) a set of logical variables,

• The signal and attribute expressions \( \text{Expr}_{\mathcal{G}}(\mathcal{E}, X) \) are defined by the grammar:

\[
\psi ::= \text{true} \mid \text{expr} \mid E_x^I_{\hspace{1pt}y} \mid E_x^?_{\hspace{1pt}y} \mid \neg \psi \mid \psi_1 \lor \psi_2,
\]

where \( \text{expr} : \text{Bool} \in \text{Expr}_{\mathcal{G}}, E \in \mathcal{E}, x, y \in X \).
• Let \((\sigma, \text{cons}, \text{Snd}) \in \Sigma_{\varphi} \times \tilde{A}\) be a triple consisting of system state, consume set, and send set.

• Let \(\beta : X \to \mathcal{B}(\mathcal{C})\) be a valuation of the logical variables.

Then

• \((\sigma, \text{cons}, \text{Snd}) \vDash_{\beta} \text{true}\)
• \((\sigma, \text{cons}, \text{Snd}) \vDash_{\beta} \neg \psi\) if and only if not \((\sigma, \text{cons}, \text{Snd}) \vDash_{\beta} \psi\)
• \((\sigma, \text{cons}, \text{Snd}) \vDash_{\beta} \psi_1 \lor \psi_2\) if and only if \((\sigma, \text{cons}, \text{Snd}) \vDash_{\beta} \psi_1\) or \((\sigma, \text{cons}, \text{Snd}) \vDash_{\beta} \psi_2\)

• \((\sigma, \text{cons}, \text{Snd}) \vDash_{\beta} \text{expr}\) if and only if \(I[\lbrack \text{expr} \rbrack](\sigma, \beta) = 1\)

• \((\sigma, \text{cons}, \text{Snd}) \vDash_{\beta} E_x^l, y\) if and only if \(\exists \tilde{d} \bullet (\beta(x), (E, \tilde{d}), \beta(y)) \in \text{Snd}\)

• \((\sigma, \text{cons}, \text{Snd}) \vDash_{\beta} E_x^?, y\) if and only if \(\exists \tilde{d} \bullet (\beta(x), (E, \tilde{d}), \beta(y)) \in \text{cons}\)

**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.
**Definition.** A TBA

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

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

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

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

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

$$(\sigma, \text{cons}, \text{Snd}) \models_{\beta} E_{x,y}^! \iff (\beta(x), (E, \vec{d}), \beta(y)) \in \text{Snd}$$
Live Sequence Charts Semantics
TBA-based Semantics of LSCs

Plan:

- Given an LSC $L$ with body

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

- 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).
**Definition.**

Let \((I, (\mathcal{L}, \preceq), \sim, \mathcal{I}, \text{Msg}, \text{Cond}, \text{LocInv})\) 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.
  \[\forall l, l' : l' \in C \land l \preceq l' \implies l \in C,\]

- it is **closed under simultaneity**, i.e.
  \[\forall l, l' : l' \in C \land l \sim l' \implies l \in C,\]  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

\[\exists l \in C : \theta(l) = \text{hot} \land \nexists l' \in C : l \prec l'.\]

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.
\[ \forall l, l' : l' \in C \land l \preceq l' \implies l \in C \]
(iii) closed under simultaneity, i.e.
\[ \forall l, l' : l' \in C \land l \sim l' \implies l \in C \]
(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 "\(\sim\)" 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 \((\mathcal{L}, \preceq)\) and messages \(\text{Msg}\).

\(C'\) is called **direct successor** of \(C\) via **fired-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.

\[ \forall l, l' \in F : l \neq l' \land i_l = i_{l'} \implies l \nless l' \land l' \nless l \]
Properties of the Fired-set

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

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

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

\[
\forall l' \in F \exists l \in C : l \prec l' \land \not\exists l'' \in C : l' \prec l'' \prec l
\]
Successor Cut Examples

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

- Let \( w = (\sigma_0, cons_0, Snd_0), (\sigma_1, cons_1, Snd_1), (\sigma_2, cons_2, Snd_2), \ldots \) be a word of a UML model and \( \beta \) a valuation of \( I \cup \{self\} \).

- Intuitively (and for now disregarding cold conditions), an LSC body \((I, (\mathcal{L}, \subseteq), \sim, \mathcal{I}, \text{Msg}, \text{Cond}, \text{LocInv})\) is supposed to accept \( w \) if and only if there exists a sequence

\[
C_0 \rightsquigarrow F_1 C_1 \rightsquigarrow F_2 C_2 \cdots \rightsquigarrow F_n C_n
\]

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

- for all \( i_j \leq k < i_{j+1} \), \((\sigma_k, cons_k, Snd_k), \beta\) satisfies the hold condition of \( C_j \),

- \((\sigma_{i_j}, cons_{i_j}, Snd_{i_j}), \beta\) satisfies the transition condition of \( F_j \),

- \( C_n \) is cold,

- for all \( i_n < k \), \((\sigma_k, cons_{i_j}, Snd_{i_j}), \beta\) satisfies the hold condition of \( C_n \).
Language of LSC Body

The **language** of the body

\[(I, (\mathcal{L}, \preceq), \sim, \mathcal{I}, \text{Msg, Cond, LocInv})\]

of LSC \(L\) is the language of the TBA

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

with

- \(\text{Expr}_B(X) = \text{Expr}_\mathcal{I}(\mathcal{I}, X)\)
- \(Q\) is the set of cuts of \((\mathcal{L}, \preceq)\), \(q_{ini}\) 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 \(q \sim_F q'\), and
  - **legal exits** \((q, \psi, \mathcal{L})\).
Language of LSC Body: Intuition

\[ \mathcal{B}_L = (Expr_B(X), X, Q, q_{ini}, \to, Q_F) \]

with

- \( Expr_B(X) = Expr_\mathcal{L}(\mathcal{L}, X) \)

- \( Q \) is the set of cuts of \( (\mathcal{L}, \preceq) \), \( q_{ini} \) is the instance heads cut,

- \( F = \{ C \in Q \mid \theta(C) = \text{cold} \} \) is the set of cold cuts,

- \( \to \) consists of
  - loops \((q, \psi, q)\),
  - progress transitions \((q, \psi, q')\) corresponding to \( q \leadsto_F q' \), and
  - legal exits \((q, \psi, \mathcal{L})\).

“what allows us to stay at this cut”

“what allows us to legally exit”

“characterisation of firedset \( F_n \)”

true

\[ v = 0 \]

\[ x > 3 \]
Step I: Only Messages
Some Helper Functions

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

\[ \mathcal{E}(l) := \{ E_{i_1, i}^! \mid (l, E, l') \in \text{Msg} \} \cup \{ E_{i_1, i}^? \mid (l', E, l) \in \text{Msg} \}, \]

\[ \mathcal{E}(\{l_1, \ldots, l_n\}) := \mathcal{E}(l_1) \cup \cdots \cup \mathcal{E}(l_n). \]

\[ \bigvee \emptyset := \text{true}; \quad \bigvee \{ E_{1_{i_1, i_2}}, \ldots, F_{k_{i, k_1, k_2}}, \ldots \} := \bigvee_{1 \leq j < k} E_{j_{i_1, i_2}} \lor \bigvee_{k \leq j} F_{j_{i_1, i_2}} \]

\[ A \quad B \quad C \]

\[ v = 0 \]

\[ x > 3 \]

\[ D \quad E \]
Loops

- How long may we **legally** stay at a cut \( q \)?

- **Intuition**: those \( (\sigma_i, cons_i, Snd_i) \) are allowed to fire the self-loop \( (q, \psi, q) \) where
  - \( cons_i \cup Snd_i \) 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,

- \( \text{sigma}_i \) 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 \( q \).

  - \( \psi := \neg (\bigvee F^c) \land \psi(q) \).  
  \[ = \text{true if } F = \emptyset \]
When do we move from $q$ to $q'$?

**Intuition:** those $({\sigma_i, cons_i, Snd_i})$ fire the progress transition $(q, \psi, q')$ for which there exists a firedset $F$ such that $q \rightsquigarrow F q'$ and

- $cons_i \cup Snd_i$ 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 $cons_i \cup Snd_i$ (**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 $q \rightsquigarrow F q'$ (unique).

$$\psi := \bigwedge \mathcal{E}(F) \land - \left( \bigvee \left( \mathcal{E}(F_1) \cup \cdots \cup \mathcal{E}(F_n) \right) \setminus \mathcal{E}(F) \right) \land \psi(q, q').$$
Step II: Conditions and Local Invariants
Some More Helper Functions

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

$$
\psi_{\theta}(q) = \{ \psi \mid \exists l \in q, l' \notin q \mid (l, \psi, \theta, l') \in \text{LocInv} \lor (l', \psi, \theta, l) \in \text{LocInv} \}, \\
\psi(q) = \psi_{\text{hot}}(q) \cup \psi_{\text{cold}}(q) \\
\bigwedge \emptyset := \text{false}; \quad \bigwedge \{ \psi_1, \ldots, \psi_n \} := \bigwedge_{1 \leq i \leq n} \psi_i
$$
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 \( q \).
  - \( \psi := \neg (\bigvee E^c(F)) \land \psi(q) \).
    - \(= \text{true if } F = \emptyset \)
Even More Helper Functions

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

\[
\psi_\theta(q, q') = \{ \psi \mid \exists L \subseteq \mathcal{L} \mid (L, \psi, \theta) \in \text{Cond} \land L \cap (q' \setminus q) \neq \emptyset \} \\
\cup \psi_\theta(q') \\
\setminus \{ \psi \mid \exists l \in q' \setminus q, l' \in \mathcal{L} \mid (l, \circ, expr, \theta, l') \in \text{LocInv} \lor (l', expr, \theta, \circ, l) \in \text{LocInv} \} \\
\cup \{ \psi \mid \exists l \in q' \setminus q, l' \in \mathcal{L} \mid (l, \bullet, expr, \theta, l') \in \text{LocInv} \lor (l', expr, \theta, \bullet, l) \in \text{LocInv} \}
\]

\[
\psi(q, q') = \psi_{\text{hot}}(q, q') \cup \psi_{\text{cold}}(q, q')
\]
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 $q \rightarrow F q'$ 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 $q \rightarrow F q'$ (unique).
  - $\psi := \bigwedge \mathcal{E}(F) \land \neg\left(\bigvee \left(\mathcal{E}(F_1) \cup \cdots \cup \mathcal{E}(F_n)\right) \setminus \mathcal{E}(F')\right) \land \bigwedge \psi(q, q')$. 
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 \( q \leadsto_F q' \) 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**) 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 \( q \leadsto q' \).
  - \( \psi := \bigvee_{i=1}^n \mathcal{E}(F_i) \land \neg \left( \Big( \mathcal{E}(F_1) \cup \cdots \cup \mathcal{E}(F_n) \right) \setminus \mathcal{E}(F_i) \right) \land \bigvee \psi_{\text{cold}}(q, q'_i) \)
    \( \lor \neg \left( \bigvee \mathcal{E}(F_i) \right) \land \bigvee \psi_{\text{cold}}(q) \).
Example
Finally: The LSC Semantics

A full LSC $L$ consist of

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

A set $W$ of words over $\mathcal{I}$ and $\emptyset$ **satisfies** $L$, denoted $W \models L$, iff $L$

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

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

$$\mathcal{I} = \mathcal{I}_\forall \cup \mathcal{I}_\exists.$$ 

**Definition.** A model

$$\mathcal{M} = (\mathcal{C}D, \mathcal{I}M, \mathcal{O}D, \mathcal{I})$$

is called **consistent** (more precise: the constructive description of behaviour is consistent with the reflective one) if and only if

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

and

$$\forall I \in \mathcal{I}_\exists : \mathcal{L}(\mathcal{M}) \cap \mathcal{L}(I) \neq \emptyset.$$
Interactions as Reflective Description

- In UML, reflective (temporal) descriptions are subsumed by interactions.
- A UML model \( \mathcal{M} = (C \mathcal{D}, \mathcal{I} \mathcal{M}, O \mathcal{D}, \mathcal{I}) \) has a set of interactions \( \mathcal{I} \).
- An interaction \( \mathcal{I} \in \mathcal{I} \) 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 \( \mathcal{M} = (\mathcal{D}, \mathcal{M}, \mathcal{O}, \mathcal{I}) \) has a set of interactions \( \mathcal{I} \).
- An interaction \( \mathcal{I} \in \mathcal{I} \) 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 $\mathcal{M} = (\mathcal{CD}, \mathcal{IM}, \mathcal{OD}, \mathcal{I})$ has a set of interactions $\mathcal{I}$.
- An interaction $\mathcal{I} \in \mathcal{I}$ 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.
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
References


