

# *Software Design, Modelling and Analysis in UML*

## *Lecture 17: Live Sequence Charts II*

2012-01-31

Prof. Dr. Andreas Podelski, **Dr. Bernd Westphal**

Albert-Ludwigs-Universität Freiburg, Germany

- 17 - 2012-01-31 - main -

## Contents & Goals

### **Last Lecture:**

- Reflective vs. constructive description of behaviour
- Live Sequence Charts: syntax, intuition

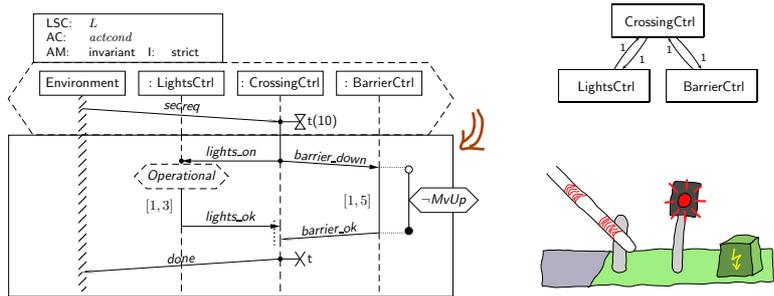
### **This Lecture:**

- **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.
  - LSC formal semantics.

- 17 - 2012-01-31 - Prelim -

## Recall: Live Sequence Charts Syntax

### Recall: Example



- **Whenever** the CrossingCtrl has consumed a 'secreq' event
- **then** it shall finally send 'lights\_on' and 'barrier\_down' to LightsCtrl and BarrierCtrl,
- if LightsCtrl **is not** 'operational' when receiving that event, the rest of this scenario doesn't apply; maybe there's another LSC for that case.
- if LightsCtrl **is** 'operational' when receiving that event, it shall reply with 'lights\_ok' within 1-3 time units,
- the BarrierCtrl shall reply with 'barrier\_ok' within 1-5 time units, during this time (dispatch time not included) it shall not be in state 'MvUp',
- 'lights\_ok' and 'barrier\_ok' may occur in any order.
- After having consumed both, CrossingCtrl may reply with 'done' to the environment.

## Recall: LSC Body – Abstract Syntax

Let  $\Theta = \{\text{hot}, \text{cold}\}$ . An **LSC body** is a tuple

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

where

- $I$  is a finite set of **instance lines**, each associated with a class  $C \in \mathcal{C}$
- $(\mathcal{L}, \preceq)$  is a finite, non-empty, partially ordered set of **locations**, each  $l \in \mathcal{L}$  is associated with a temperature  $\theta(l) \in \Theta$  and an instance line  $i_l \in I$ ,
- $\sim \subseteq \mathcal{L} \times \mathcal{L}$  is an **equivalence relation** on locations, the **simultaneity** relation,
- $\mathcal{S} = (\mathcal{I}, \mathcal{C}, V, \text{atr}, \mathcal{W})$  is a signature,
- $\text{Msg} \subseteq \mathcal{L} \times \mathcal{E} \times \mathcal{L}$  is a set of **asynchronous messages** with  $(l, b, l')$  in  $\text{Msg}$  only if  $l \sim l'$ ,
- **Not: instantaneous messages** — could be linked to method/operation calls.
- $\text{Cond} \subseteq (2^{\mathcal{L}} \setminus \emptyset) \times \text{Expr}_{\mathcal{S}} \times \Theta$  is a set of **conditions** with  $(L, \text{expr}, \theta) \in \text{Cond}$  only if  $l \sim l'$  for all  $l, l' \in L$ ,
- $\text{LocInv} \subseteq \mathcal{L} \times \{0, \bullet\} \times \text{Expr}_{\mathcal{S}} \times \Theta \times \mathcal{L} \times \{0, \bullet\}$  is a set of **local invariants**,

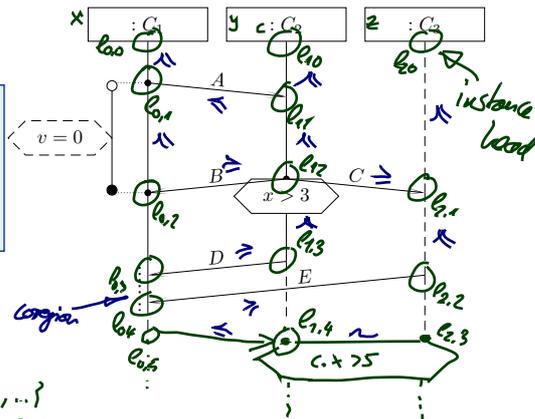
- 17 - 2012-01-31 - Skesyn -

5/47

### Example

$$\begin{aligned} &(I, (\mathcal{L}, \preceq), \sim, \mathcal{S}, \text{Msg}, \text{Cond}, \text{LocInv}) \\ &\text{Msg} \subseteq \mathcal{L} \times \mathcal{E} \times \mathcal{L} \\ &\text{Cond} \subseteq (2^{\mathcal{L}} \setminus \emptyset) \times \text{Expr}_{\mathcal{S}} \times \Theta \\ &\text{LocInv} \subseteq \\ &\mathcal{L} \times \{0, \bullet\} \times \text{Expr}_{\mathcal{S}} \times \Theta \times \mathcal{L} \times \{0, \bullet\} \end{aligned}$$

$$\begin{aligned} I &= \{x, y, z\}, \quad C(x) = C_1, \dots \\ \mathcal{L} &= \{(l_{0,0}, \text{hot}), (l_{1,0}, \text{cold}), \dots\} \\ \preceq \subseteq \mathcal{L} \times \mathcal{L} &: \{l_{0,0} \preceq l_{0,0}, \dots \\ &\quad l_{0,0} \preceq l_{0,1}, l_{0,2} \preceq l_{0,3}, l_{0,2} \preceq l_{0,4}, \dots\} \\ \text{Msg} &= \{(l_{1,1}, A, l_{2,1}), \dots\} \quad \sim = \{(l_{1,4}, l_{2,3})\} \\ \text{Cond} &= \{(\{l_{1,u}, l_{2,v}\}, (x > 5), \text{hot}), \dots\} \\ \text{LocInv} &= \{(l_{0,1}, 0, (v=0), \text{cold}, l_{0,2}, \bullet)\} \end{aligned}$$



- 17 - 2012-01-31 - Skesyn -

6/47

## Recall: Well-Formedness

**Bondedness/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.

$$\exists (L, expr, \theta) \in \text{Cond} : l \in L,$$

- a **local invariant**, i.e.

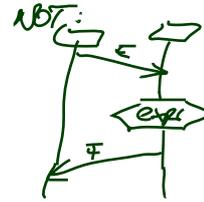
$$\exists (l_1, i_1, expr, \theta, l_2, i_2) \in \text{LocInv} : l \in \{l_1, l_2\}, \text{ or}$$

**then** there is a location  $l'$  **equivalent** to  $l$  which is the location of

- a **message**, i.e.

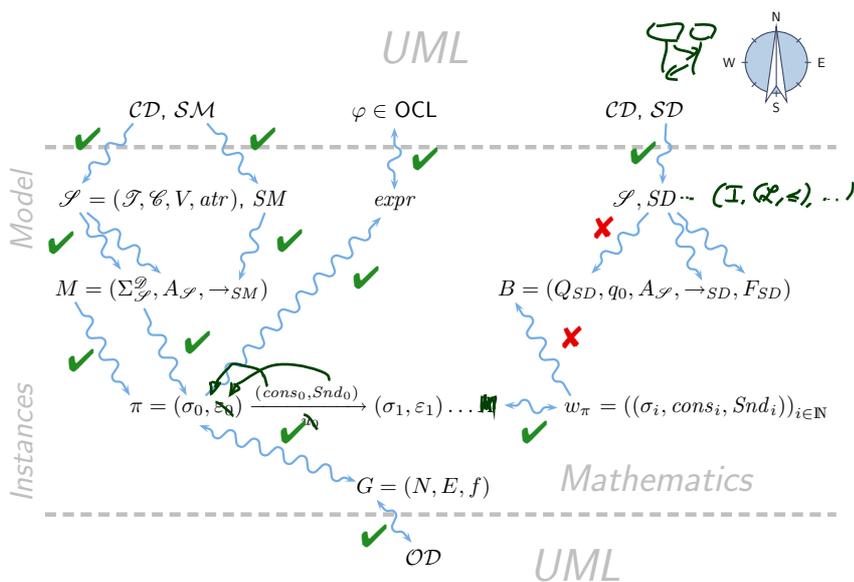
$$\exists (l_1, b, l_2) \in \text{Msg} : l \in \{l_1, l_2\}, \text{ or}$$

- an **instance head**, i.e.  $l'$  is minimal wrt.  $\preceq$ .



**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).

## Course Map



## Live Sequence Charts Semantics

### TBA-based Semantics of LSCs

**Plan:**

- Given an LSC  $L$  with body

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

- Construct a TBA  $\mathcal{B}_L$  — taking the **cuts** of  $L$  as states.
- Define  $\mathcal{L}(L)$  **in terms of**  $\mathcal{L}(\mathcal{B}_L)$ ,  
in particular taking activation condition and activation mode into account.

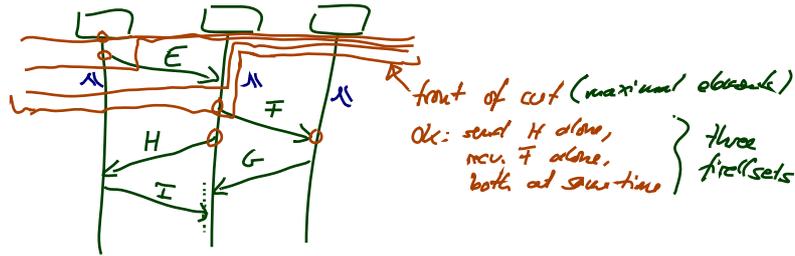
## Formal LSC Semantics: It's in the Cuts

- Let  $(I, (\mathcal{L}, \preceq), \sim, \mathcal{S}, \text{Msg}, \text{Cond}, \text{LocInv})$  be an LSC body.
- A non-empty set

$$\emptyset \neq C \subseteq \mathcal{L}$$

is called a **cut** of the LSC body if and only if

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



- 17 - 2012-01-31 - Scits -

11/47

## Formal LSC Semantics: It's in the Cuts

- Let  $(I, (\mathcal{L}, \preceq), \sim, \mathcal{S}, \text{Msg}, \text{Cond}, \text{LocInv})$  be an LSC body.
- A non-empty set

$$\emptyset \neq C \subseteq \mathcal{L}$$

is called a **cut** of the LSC body if and only if

- it is **downward closed**, i.e.  $\forall l, l' : l' \in C \wedge l \preceq l' \implies l \in C$ ,
  - it is **closed** under **simultaneity**, i.e.  $\forall l, l' : l' \in C \wedge l \sim l' \implies l \in C$ , 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

$$\exists l \in C : \theta(l) = \text{hot} \wedge \nexists l' \in C : l \prec l'$$

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

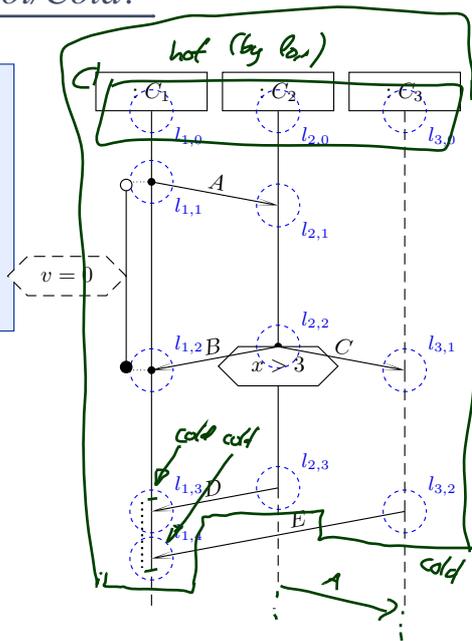
- 17 - 2012-01-31 - Scits -

11/47

## Examples: Cut or Not Cut? Hot/Cold?

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

- $C_0 = \emptyset$
- $C_1 = \{l_{1,0}, l_{2,0}, l_{3,0}\}$
- $C_2 = \{l_{1,1}, l_{2,1}, l_{3,0}\}$
- $C_3 = \{l_{1,0}, l_{1,1}\}$
- $C_4 = \{l_{1,0}, l_{1,1}, l_{2,0}, l_{3,0}\}$
- $C_5 = \{l_{1,0}, l_{1,1}, l_{2,0}, l_{2,1}, l_{3,0}\}$
- $C_6 = \mathcal{L} \setminus \{l_{1,3}, l_{2,3}\}$
- $C_7 = \mathcal{L}$



- 17 - 2012-01-31 - Scits -

12/47

## 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:

- Let  $C, C' \subseteq \mathcal{L}$  be cuts.  $C'$  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  $C$ ,
- locations in  $F$ , that lie on the same instance line, are pairwise unordered, i.e.

$$\forall l, l' \in F : l \neq l' \wedge i_l = i_{l'} \implies l \not\preceq l' \wedge l' \not\preceq l$$

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

- In other words: locations in  $F$  are direct  $\preceq$ -successors of locations in  $C$ , i.e.

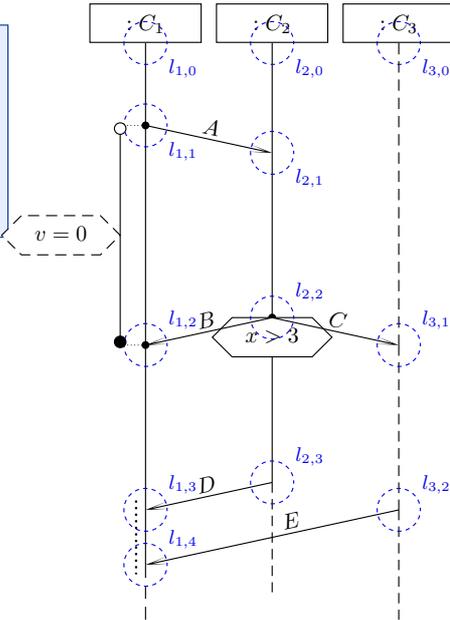
$$\forall l' \in F \exists l \in C : l \prec l' \wedge \nexists l'' \in C : l' \prec l'' \prec l$$

- 17 - 2012-01-31 - Scits -

13/47

## Successor Cut Examples

- (i)  $F \neq \emptyset$ ,
- (ii)  $C' \setminus C = F$ ,
- (iii) message send before receive,
- (iv) locations on same instance line unordered, i.e.  
 $\forall l, l' \in F : l \neq l' \wedge i_l = i_{l'} \implies l \not\leq l' \wedge l' \not\leq l$



- 17 - 2012-01-31 - Scits -

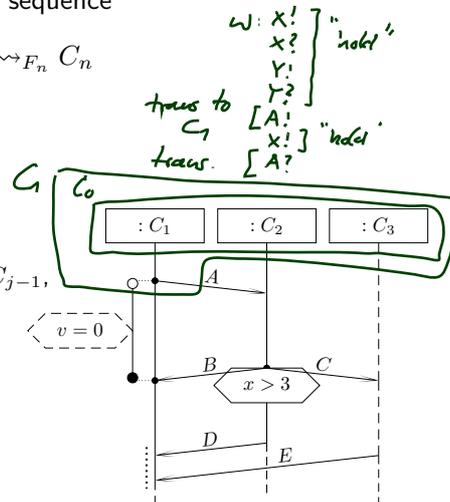
## Idea: Accepting Words by Advancing the Cut

Let  $w = (\sigma_i, cons_i, Snd_i)_{i \in \mathbb{N}_0}$  be a word over  $\mathcal{S}$  and  $\mathcal{D}$ .

**Intuitively** (and for now **disregarding** cold conditions), an LSC body  $(I, (\mathcal{L}, \preceq), \sim, \mathcal{S}, \text{Msg}, \text{Cond}, \text{LocInv})$  is **supposed** to **accept**  $w$  (under valuation  $\beta$ ) if and only if there exists a sequence

which maps instance lines to objects  
 $C_0 \rightsquigarrow_{F_1} C_1 \rightsquigarrow_{F_2} C_2 \dots \rightsquigarrow_{F_n} C_n$   
 and indices  $i_1 < \dots < i_n$  such that

- $C_0$  consists of the instance heads,
- for all  $1 \leq j < n$ ,
  - for all  $i_j \leq k < i_{j+1}$ ,  $(\sigma_k, cons_k, Snd_k)$  satisfies (under  $\beta$ ) the **hold condition** of  $C_{j-1}$ ,
  - $(\sigma_{i_j}, cons_{i_j}, Snd_{i_j})$  satisfies (under  $\beta$ ) the **transition condition** of  $F_j$ ,
- $C_n$  is cold,  $C_n = \mathcal{L}$
- for all  $i_n < k$ ,  $(\beta_k, \mu_{i_j}, t_{i_j})$  satisfies (under  $\beta$ ) the **hold condition** of  $C_n$ .



- 17 - 2012-01-31 - Scits -

## Excursus: Symbolic Büchi Automata (over Signature)

### Symbolic Büchi Automata

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

$$\mathcal{B} = (\text{Expr}_{\mathcal{B}}, X, Q, q_{\text{ini}}, \rightarrow, Q_F)$$

where

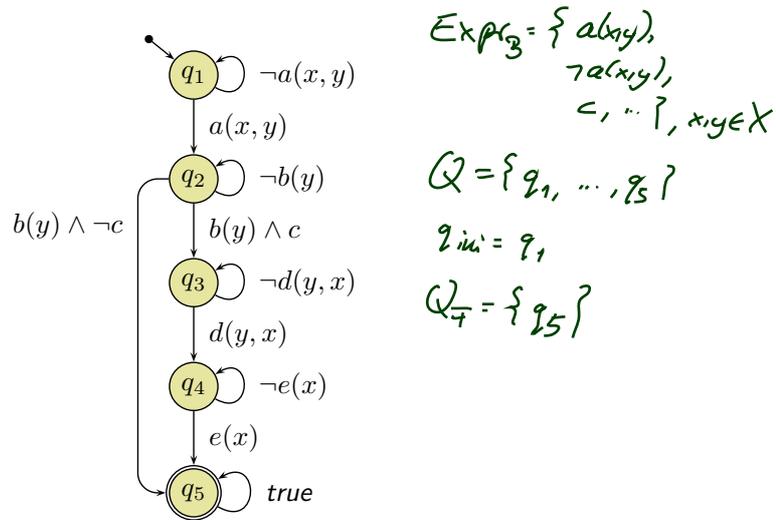
- $\text{Expr}_{\mathcal{B}}$  is a set of expressions over logical variables from  $X$ ,
- $Q$  is a finite set of **states**,  $q_{\text{ini}}$  <sup>←  $Q$</sup>  the initial state,
- $\rightarrow \subseteq Q \times \text{Expr}_{\mathcal{B}} \times Q$  is the **transition relation**.

Transitions  $(q, \text{expr}, q')$  from  $q$  to  $q'$  are labelled with a constraint  $\text{expr} \in \text{Expr}_{\mathcal{B}}$  over the ~~signals and state~~ variables.

- $Q_F \subseteq Q$  is the set of **fair** (or accepting) states.

## TBA Example

$(Expr_{\mathcal{B}}, X, Q, q_{ini}, \rightarrow, Q_F)$



- 17 - 2012.01.31 - Stha -

19/47

## Word

**Definition.** Let  $Expr_{\mathcal{B}}$  be a set of expressions over logical variables  $X$ . and let  $\Sigma$  be the set of interpretation functions of  $Expr_{\mathcal{B}}$ , i.e.

$$\Sigma = Expr_{\mathcal{B}} \times (X \rightarrow \mathcal{D}(X)) \rightarrow \{0, 1\}.$$

For  $\sigma \in \Sigma$ , we write  $\sigma \models_{\beta} expr$  if and only if  $\sigma(expr, \beta) = 1$ .

A **word** over  $Expr_{\mathcal{B}}$  is an infinite sequence of interpretations of  $Expr_{\mathcal{B}}$

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

$\omega: \sigma_0 \models_{\beta} a(x,y) \quad , \quad \beta = \{ x \mapsto 1, y \mapsto 2 \}$   
 $\sigma_1 \models_{\beta} c, \sigma_1 \not\models e(x) \quad (\text{nothing else})$   
 $\vdots$

- 17 - 2012.01.31 - Stha -

20/47

## Run of TBA over Word

**Definition.** Let  $\mathcal{B} = (Expr_{\mathcal{B}}, X, Q, q_{ini}, \rightarrow, Q_F)$  be a TBA and

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

a word over  $Expr_{\mathcal{B}}$ .

An infinite sequence

$$\rho = q_0, q_1, q_2, \dots \in Q^\omega$$

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

- $q_0 = q_{ini}$ ,
- for each  $i \in \mathbb{N}_0$  there is a transition  $(q_i, \psi_i, q_{i+1}) \in \rightarrow$  such that

$$\sigma_i \models_{\beta} \psi_i.$$

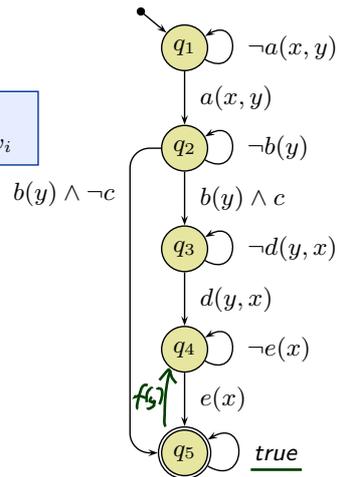
## Run or Not Run Examples

$$\rho = (q_i)_{i \in \mathbb{N}_0}, \quad q_0 = q_{ini},$$

$$\forall i \in \mathbb{N}_0 \exists (q_i, \psi_i, q_{i+1}) \in \rightarrow : (\sigma_i, cons_i, Snd_i) \models_{\beta} \psi_i$$

$w$ :  $\sigma_0 \not\models_{\beta} a(x,y) \quad (\Rightarrow \sigma_0 \not\models_{\beta} \neg a(x,y))$   
 $\sigma_1 \not\models_{\beta} a(x,y)$   
 $\sigma_2 \models_{\beta} a(x,y), \sigma_2 \not\models_{\beta} c(x)$   
 $\sigma_3 \models_{\beta} b(y) \wedge \neg c$   
 $\sigma_4 \models_{\beta} e(x) \wedge d(y,x)$   
 $\vdots$

$R = q_0, q_1, q_1, q_2, q_3, q_3, q_3, \dots$   
 $\underbrace{\quad} \underbrace{\quad} \underbrace{\quad} \underbrace{\quad} \underbrace{\quad}$   
 $b_0 \quad b_1 \quad b_2 \quad b_3 \quad b_4 \quad \vdots$   
 $\sigma_0 \quad \sigma_1 \quad \sigma_2 \quad \sigma_3 \quad \sigma_4$



## The Language of a TBA

### Definition.

We say  $\mathcal{B} = (\text{Expr}_{\mathcal{B}}, X, Q, q_{ini}, \rightarrow, Q_F)$  **accepts**  $w$  (under valuation  $\beta : X \rightarrow \mathcal{D}(X)$ ) if and only if  $\mathcal{B}$  **has a run**

$$(q_i)_{i \in \mathbb{N}_0}$$

over  $w$  such that fair (or accepting) states are **visited infinitely often**, that is,

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

We call the set  $\mathcal{L}_{\beta}(\mathcal{B})$  of words over  $\mathcal{S}$  that are accepted by  $\mathcal{B}$  under  $\beta$  the **language of  $\mathcal{B}$** .

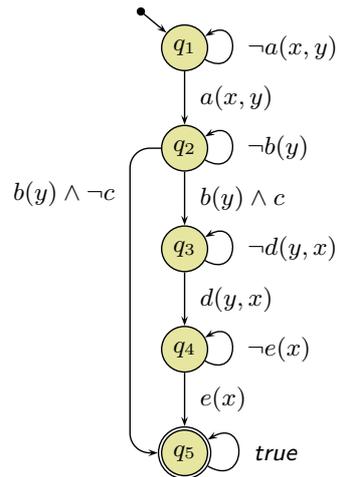
## Language of the Example TBA

$\mathcal{L}_{\beta}(\mathcal{B})$  consists of the words

$$(\sigma_i, \text{Snd}_i, \text{cons}_i)_{i \in \mathbb{N}_0}$$

where there exist  $0 \leq n < m < k < \ell$  such that

- for  $0 \leq i < n$ ,  $\sigma_i \not\models_{\beta} a(x, y)$
- $\sigma_n \models_{\beta} a(x, y)$
- for  $n < i < m$ ,  $\sigma_i \not\models_{\beta} b(y)$
- $\sigma_m \models_{\beta} b(y) \wedge \neg c$  and
  - for  $m < i < k$ ,  $\sigma_i \not\models_{\beta} d(y, x)$
  - $\sigma_k \models_{\beta} d(y, x)$
  - for  $k < i < \ell$ ,  $\sigma_i \not\models_{\beta} e(x)$
  - $\sigma_{\ell} \models_{\beta} e(x)$ , or
- $\sigma_m \models_{\beta} b(y) \wedge \neg c$



## Back to Main Track: Live Sequence Charts Semantics

### Recall Idea: Accepting Words by Advancing the Cut

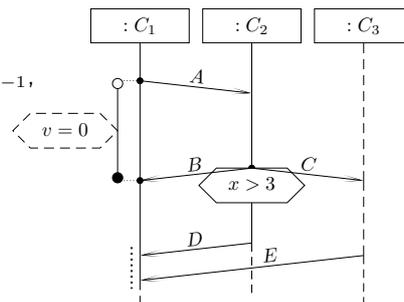
Let  $w = (\sigma_i, cons_i, Snd_i)_{i \in \mathbb{N}_0}$  be a word over  $\mathcal{S}$  and  $\mathcal{D}$ .

**Intuitively** (and for now **disregarding** cold conditions), an LSC body  $(I, (\mathcal{L}, \preceq), \sim, \mathcal{S}, \text{Msg}, \text{Cond}, \text{LocInv})$  is **supposed** to **accept**  $w$  (under valuation  $\beta$ ) 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  $i_1 < \cdots < i_n$  such that

- $C_0$  consists of the instance heads,
- for all  $1 \leq j < n$ ,
  - for all  $i_j \leq k < i_{j+1}$ ,  $(\sigma_k, cons_k, Snd_k)$  satisfies (under  $\beta$ ) the **hold condition** of  $C_{j-1}$ ,
  - $(\sigma_{i_j}, cons_{i_j}, Snd_{i_j})$  satisfies (under  $\beta$ ) the **transition condition** of  $F_j$ ,
- $C_n$  is cold,
- for all  $i_n < k$ ,  $(\beta_k, \mu_{i_j}, t_{i_j})$  satisfies (under  $\beta$ ) the **hold condition** of  $C_n$ .



## Language of LSC Body

The **language** of the body

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

of LSC  $L$  is the language of the TBA

$$\mathcal{B}_L = (\text{Expr}_{\mathcal{B}}, X, Q, q_{ini}, \rightarrow, Q_F)$$

with

- $\text{Expr}_{\mathcal{B}} = \text{Expr}_{\mathcal{S}}(V, \mathcal{E}(\mathcal{S}))$
- $Q$  is the set of cuts of  $(\mathcal{L}, \preceq)$ ,  $q_{ini}$  is the **instance heads cut**,
- $Q_F = \{C \in Q \mid \theta(C) = \text{cold}\}$  is the set of cold cuts of  $(\mathcal{L}, \preceq)$ ,
- $\rightarrow$  as defined in the following, consisting of
  - **loops**  $(q, \psi, q)$ ,
  - **progress transitions**  $(q, \psi, q')$ , and
  - **legal exits**  $(q, \psi, \mathcal{L})$ .

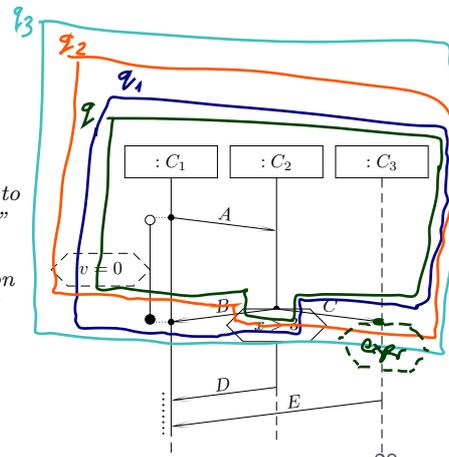
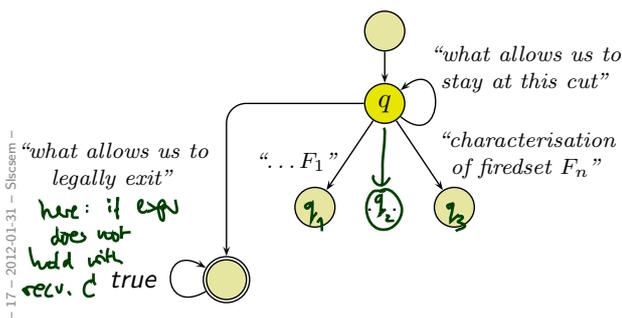
- 17 - 2012-01-31 - Skrzem -

27/47

## Language of LSC Body: Intuition

$\mathcal{B}_L = (\text{Expr}_{\mathcal{B}}, X, Q, q_{ini}, \rightarrow, Q_F)$  with

- $\text{Expr}_{\mathcal{B}} = \text{Expr}_{\mathcal{S}}(V, \mathcal{E}(\mathcal{S}))$
- $Q$  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,
- $\rightarrow$  consists of
  - **loops**  $(q, \psi, q)$ ,
  - **progress transitions**  $(q, \psi, q')$ , and
  - **legal exits**  $(q, \psi, \mathcal{L})$ .



- 17 - 2012-01-31 - Skrzem -

28/47

## Signal and Integer Expressions

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

The **signal and integer expressions**  $Expr_{\mathcal{S}}(V, \mathcal{E}(\mathcal{S}))$  over  $\mathcal{S}$  are defined by the grammar:

$$\psi ::= true \mid expr \mid E_{x,y}^! \mid E_x^? \mid \neg\psi \mid \psi_1 \vee \psi_2,$$

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

*send(x, E, y)*  
*consumes(x, E)*

## Satisfaction of Signal and Integer Expressions

Let  $(\sigma, cons, Snd) \in (\Sigma_{\mathcal{S}}^{\mathcal{D}} \times 2^{\mathcal{D}(\mathcal{C}) \times Evs(\mathcal{E}, \mathcal{D})} \times 2^{\mathcal{D}(\mathcal{C}) \times Evs(\mathcal{E}, \mathcal{D}) \times \mathcal{D}(\mathcal{C})})$  be a letter of a word over  $\mathcal{S}$  and  $\mathcal{D}$  and let  $\beta : X \rightarrow \mathcal{D}(\mathcal{C})$  be a valuation of the logical variables in  $X$ .

- $(\sigma, cons, Snd) \models_{\beta} true$
- $(\sigma, cons, Snd) \models_{\beta} \neg\psi$  if and only if not  $(\sigma, cons, Snd) \models_{\beta} \psi$
- $(\sigma, cons, Snd) \models_{\beta} \psi_1 \vee \psi_2$  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  $I[expr](\sigma, \beta) = 1$
- $(\sigma, cons, Snd) \models_{\beta} E_{x,y}^!$  if and only if  $(\beta(x), (E, \vec{d}), \beta(y)) \in Snd$
- $(\sigma, cons, Snd) \models_{\beta} E_x^?$  if and only if  $(\beta(x), (E, \vec{d})) \in cons$

*eg. d.x > 5*

## Satisfaction of Signal and Integer Expressions

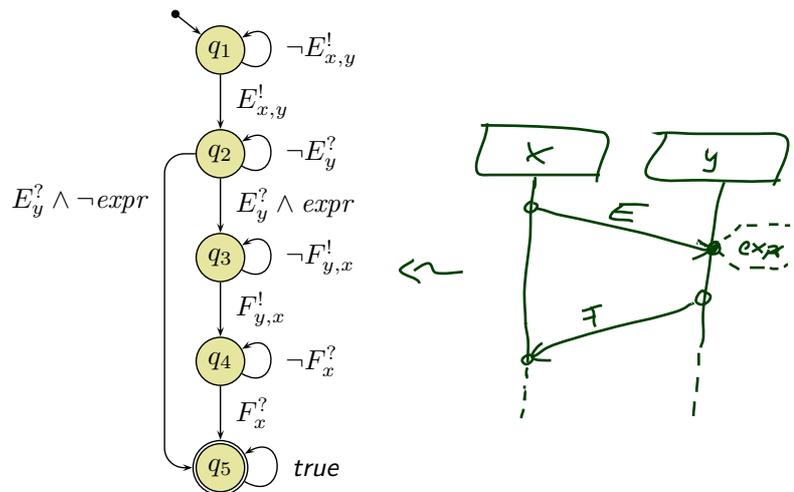
Let  $(\sigma, cons, Snd) \in (\Sigma_{\mathcal{S}}^{\mathcal{D}} \times 2^{\mathcal{D}(\mathcal{C}) \times Evs(\mathcal{E}, \mathcal{D})} \times 2^{\mathcal{D}(\mathcal{C}) \times Evs(\mathcal{E}, \mathcal{D}) \times \mathcal{D}(\mathcal{C})})$  be a letter of a word over  $\mathcal{S}$  and  $\mathcal{D}$  and let  $\beta : X \rightarrow \mathcal{D}(\mathcal{C})$  be a valuation of the logical variables in  $X$ .

- $(\sigma, cons, Snd) \models_{\beta} true$
- $(\sigma, cons, Snd) \models_{\beta} \neg\psi$  if and only if not  $(\sigma, cons, Snd) \models_{\beta} \psi$
- $(\sigma, cons, Snd) \models_{\beta} \psi_1 \vee \psi_2$  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  $I[expr](\sigma, \beta) = 1$
- $(\sigma, cons, Snd) \models_{\beta} E_{x,y}^!$  if and only if  $(\beta(x), (E, \vec{d}), \beta(y)) \in Snd$
- $(\sigma, cons, Snd) \models_{\beta} E_x^?$  if and only if  $(\beta(x), (E, \vec{d})) \in cons$

**Observation:** if the semantics has “**forgotten**” the sender at consumption time, then we have to disregard it here (straightforwardly fixed if desired).

Other view: we could choose to disregard the sender.

## Example: TBA over Signal and Integer Expressions

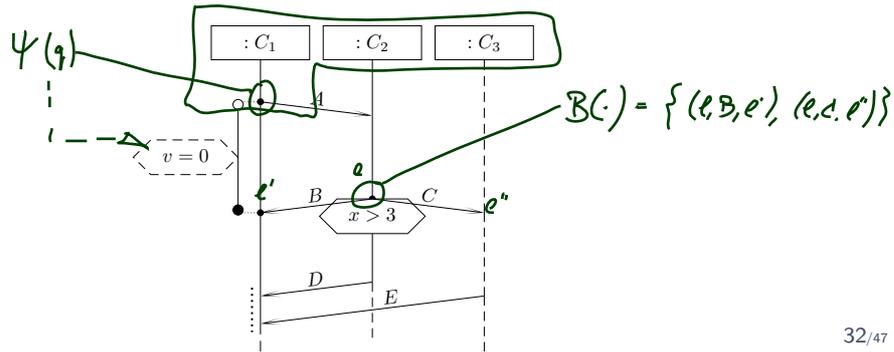


## Some Helper Functions

- Messages of a location: starting or ending  $\{(e', b, e'') \in \text{Msg} \mid e' = e \vee e'' = e\}$   
 $B(l) := \{b \in B \mid \exists l' : (l, b, l') \in \text{Msg} \vee (l', b, l) \in \text{Msg}\},$   
 $B(\{l_1, \dots, l_n\}) := B(l_1) \cup \dots \cup B(l_n).$

- Constraints relevant at cut  $q$ :

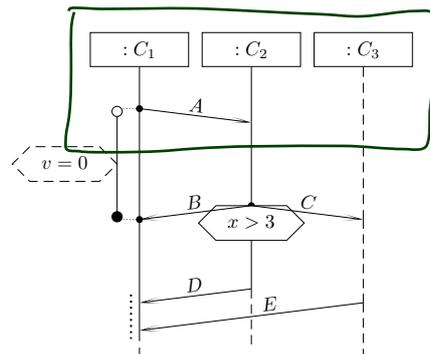
$$\psi(q) = \{\psi \mid \exists l \in q, l' \notin q \mid (l, \psi, \theta, l') \in \text{LocInv} \vee (l', \psi, \theta, l) \in \text{LocInv}\},$$



## Some More Helper Functions

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

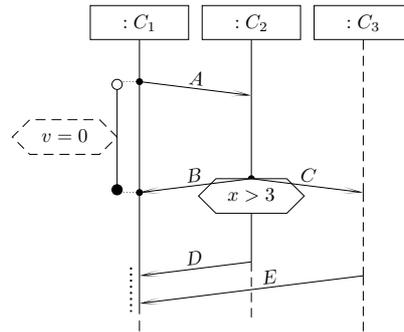
$$\begin{aligned} \psi(q, q') = & \{\psi \mid \exists l \in q' \setminus q, l' \in \mathcal{L}, \theta \in \Theta \mid \\ & (l, \bullet, \text{expr}, \theta, l') \in \text{LocInv} \vee (l', \text{expr}, \theta, l, \bullet) \in \text{LocInv}\} \\ & \cup \{\psi \mid \exists l \in q, l' \notin q', \theta \in \Theta \mid \\ & (l, \text{expr}, \theta, l') \in \text{LocInv} \vee (l', \text{expr}, \theta, l) \in \text{LocInv}\} \\ & \cup \{\psi \mid \exists L \subseteq \mathcal{L}, \theta \in \Theta \mid (L, \psi, \theta) \in \text{Cond} \wedge L \cap (q' \setminus q) \neq \emptyset\} \end{aligned}$$



## Even More Helper Functions

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

$$\begin{aligned} \psi_{\text{cold}}(q, q') = & \{ \psi \mid \exists l \in q' \setminus q, l' \in \mathcal{L} \mid \\ & (l, \bullet, \text{expr}, \text{cold}, l') \in \text{LocInv} \vee (l', \text{expr}, \text{cold}, l, \bullet) \in \text{LocInv} \} \\ & \cup \{ \psi \mid \exists l \in q, l' \notin q' \mid \\ & (l, \text{expr}, \text{cold}, l') \in \text{LocInv} \vee (l', \text{expr}, \text{cold}, l) \in \text{LocInv} \} \\ & \cup \{ \psi \mid \exists L \subseteq \mathcal{L} \mid (L, \psi, \text{cold}) \in \text{Cond} \wedge L \cap (q' \setminus q) \neq \emptyset \} \end{aligned}$$

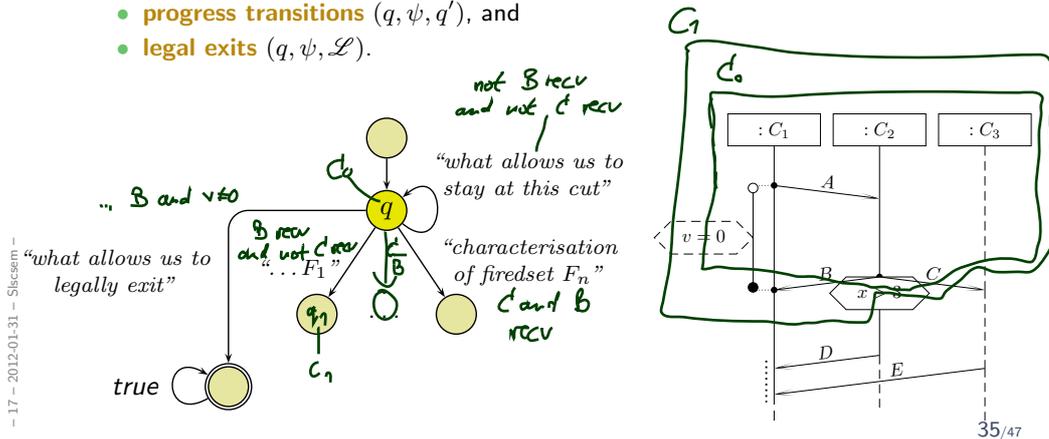


34/47

## Recall: Intuition

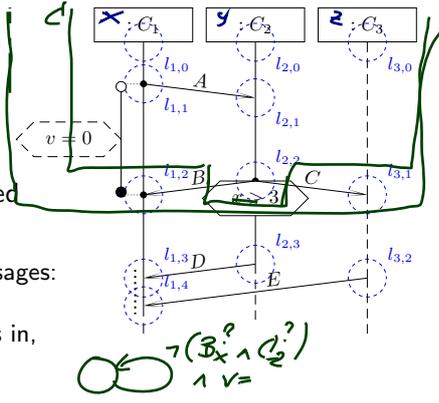
$\mathcal{B}_L = (\text{Expr}_{\mathcal{B}}, X, Q, q_{\text{ini}}, \rightarrow, Q_F)$  with

- $\text{Expr}_{\mathcal{B}} = \text{Expr}_{\mathcal{F}}(V, \mathcal{L}(\mathcal{S}))$
- $Q$  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**  $(q, \psi, q')$ , and
  - **legal exits**  $(q, \psi, \mathcal{L})$ .



# 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: (permissive)**  
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  $F := F_1 \cup \dots \cup F_n$  be the union of the firedsets of  $q$ .

$$\psi := \underbrace{\neg(\bigvee F)}_{= \text{true if } F = \emptyset} \wedge \bigwedge \psi(q). \quad \text{weak mode}$$

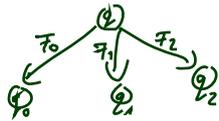
*conjoin all constraints in the set  $\Psi(q)$*

*strict: add  $\neg(\bigvee M_{sq})$  (no message from LSC is allowed)*

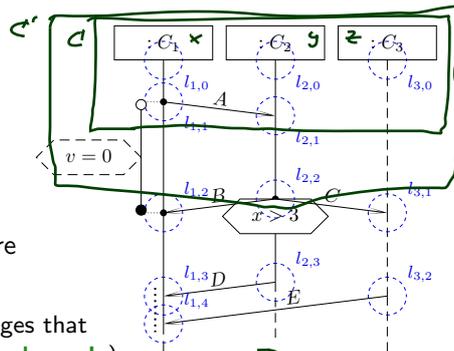
*$\bigvee_{i=1}^n (l_{i,2}, s, l_{i,2}), (l_{i,2}, c', l_{i,2})$*

*$B_i(l_{i,2}, i, l_{i,2}) \vee C_i(l_{i,2}, i, l_{i,2})$*

# Progress



- 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  $F_0, F_1, \dots, F_n$  be the firedset of  $q$  and  $q \rightsquigarrow_F q'$  (unique).

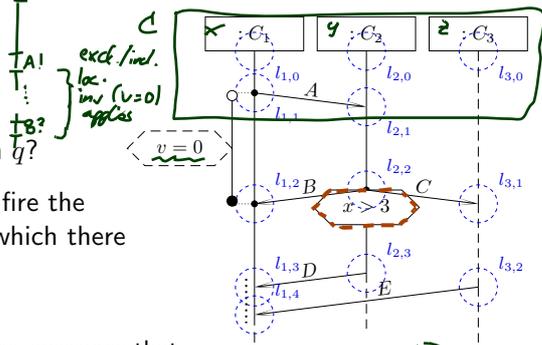


$$\psi := \underbrace{\bigwedge B(F_0)}_{\text{the msgs. in firedset } F_0} \wedge \underbrace{\neg(\bigvee (B(F_1) \cup \dots \cup B(F_n)) \setminus B(F_0))}_{\text{and no other firedset}} \wedge \underbrace{\bigwedge \psi(q, q')}_{\text{respect conditions and loc. invariants relevant at } q'}$$

*weak mode*

# Legal Exits

$$w = (\sigma_0, cons_0, Snd_0) \\ (\sigma_1, cons_1, Snd_1) \\ \vdots$$

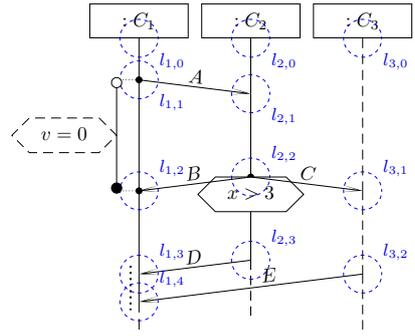


- When do we take a legal exit from  $q$ ?
- **Intuition:** those  $(\sigma_i, cons_i, Snd_i)$  fire the legal exit transition  $(q, \psi, \mathcal{L})$  for which there exists a firedset  $F$  and some  $q'$  such that  $q \rightsquigarrow_F q'$  and
  - $cons_i \cup Snd_i$  comprises exactly the messages 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**).
  - $\sigma_i$  does not satisfy any cold constraint (or loc. inv)
- **Formally:** Let  $F_1, \dots, F_n$  be the firedset of  $q$  with  $q \rightsquigarrow_{F_i} q'_i$ .
  - $\psi := \bigvee_{i=1}^n \bigwedge B(F_i) \wedge \neg(\bigvee (B(F_1) \cup \dots \cup B(F_n)) \setminus B(F_i)) \wedge \bigvee \psi_{cold}(q, q'_i)$

*we could move from  $q$  to  $q'$  with firedset  $F_i$*

*$B_i^1$   $B_i^2$   $B_i^3$   $B_i^4$   $B_i^5$   $B_i^6$   $B_i^7$   $B_i^8$   $B_i^9$   $B_i^{10}$   $B_i^{11}$   $B_i^{12}$   $B_i^{13}$   $B_i^{14}$   $B_i^{15}$   $B_i^{16}$   $B_i^{17}$   $B_i^{18}$   $B_i^{19}$   $B_i^{20}$   $B_i^{21}$   $B_i^{22}$   $B_i^{23}$   $B_i^{24}$   $B_i^{25}$   $B_i^{26}$   $B_i^{27}$   $B_i^{28}$   $B_i^{29}$   $B_i^{30}$   $B_i^{31}$   $B_i^{32}$   $B_i^{33}$   $B_i^{34}$   $B_i^{35}$   $B_i^{36}$   $B_i^{37}$   $B_i^{38}$   $B_i^{39}$   $B_i^{40}$   $B_i^{41}$   $B_i^{42}$   $B_i^{43}$   $B_i^{44}$   $B_i^{45}$   $B_i^{46}$   $B_i^{47}$   $B_i^{48}$   $B_i^{49}$   $B_i^{50}$   $B_i^{51}$   $B_i^{52}$   $B_i^{53}$   $B_i^{54}$   $B_i^{55}$   $B_i^{56}$   $B_i^{57}$   $B_i^{58}$   $B_i^{59}$   $B_i^{60}$   $B_i^{61}$   $B_i^{62}$   $B_i^{63}$   $B_i^{64}$   $B_i^{65}$   $B_i^{66}$   $B_i^{67}$   $B_i^{68}$   $B_i^{69}$   $B_i^{70}$   $B_i^{71}$   $B_i^{72}$   $B_i^{73}$   $B_i^{74}$   $B_i^{75}$   $B_i^{76}$   $B_i^{77}$   $B_i^{78}$   $B_i^{79}$   $B_i^{80}$   $B_i^{81}$   $B_i^{82}$   $B_i^{83}$   $B_i^{84}$   $B_i^{85}$   $B_i^{86}$   $B_i^{87}$   $B_i^{88}$   $B_i^{89}$   $B_i^{90}$   $B_i^{91}$   $B_i^{92}$   $B_i^{93}$   $B_i^{94}$   $B_i^{95}$   $B_i^{96}$   $B_i^{97}$   $B_i^{98}$   $B_i^{99}$   $B_i^{100}$   $B_i^{101}$   $B_i^{102}$   $B_i^{103}$   $B_i^{104}$   $B_i^{105}$   $B_i^{106}$   $B_i^{107}$   $B_i^{108}$   $B_i^{109}$   $B_i^{110}$   $B_i^{111}$   $B_i^{112}$   $B_i^{113}$   $B_i^{114}$   $B_i^{115}$   $B_i^{116}$   $B_i^{117}$   $B_i^{118}$   $B_i^{119}$   $B_i^{120}$   $B_i^{121}$   $B_i^{122}$   $B_i^{123}$   $B_i^{124}$   $B_i^{125}$   $B_i^{126}$   $B_i^{127}$   $B_i^{128}$   $B_i^{129}$   $B_i^{130}$   $B_i^{131}$   $B_i^{132}$   $B_i^{133}$   $B_i^{134}$   $B_i^{135}$   $B_i^{136}$   $B_i^{137}$   $B_i^{138}$   $B_i^{139}$   $B_i^{140}$   $B_i^{141}$   $B_i^{142}$   $B_i^{143}$   $B_i^{144}$   $B_i^{145}$   $B_i^{146}$   $B_i^{147}$   $B_i^{148}$   $B_i^{149}$   $B_i^{150}$   $B_i^{151}$   $B_i^{152}$   $B_i^{153}$   $B_i^{154}$   $B_i^{155}$   $B_i^{156}$   $B_i^{157}$   $B_i^{158}$   $B_i^{159}$   $B_i^{160}$   $B_i^{161}$   $B_i^{162}$   $B_i^{163}$   $B_i^{164}$   $B_i^{165}$   $B_i^{166}$   $B_i^{167}$   $B_i^{168}$   $B_i^{169}$   $B_i^{170}$   $B_i^{171}$   $B_i^{172}$   $B_i^{173}$   $B_i^{174}$   $B_i^{175}$   $B_i^{176}$   $B_i^{177}$   $B_i^{178}$   $B_i^{179}$   $B_i^{180}$   $B_i^{181}$   $B_i^{182}$   $B_i^{183}$   $B_i^{184}$   $B_i^{185}$   $B_i^{186}$   $B_i^{187}$   $B_i^{188}$   $B_i^{189}$   $B_i^{190}$   $B_i^{191}$   $B_i^{192}$   $B_i^{193}$   $B_i^{194}$   $B_i^{195}$   $B_i^{196}$   $B_i^{197}$   $B_i^{198}$   $B_i^{199}$   $B_i^{200}$   $B_i^{201}$   $B_i^{202}$   $B_i^{203}$   $B_i^{204}$   $B_i^{205}$   $B_i^{206}$   $B_i^{207}$   $B_i^{208}$   $B_i^{209}$   $B_i^{210}$   $B_i^{211}$   $B_i^{212}$   $B_i^{213}$   $B_i^{214}$   $B_i^{215}$   $B_i^{216}$   $B_i^{217}$   $B_i^{218}$   $B_i^{219}$   $B_i^{220}$   $B_i^{221}$   $B_i^{222}$   $B_i^{223}$   $B_i^{224}$   $B_i^{225}$   $B_i^{226}$   $B_i^{227}$   $B_i^{228}$   $B_i^{229}$   $B_i^{230}$   $B_i^{231}$   $B_i^{232}$   $B_i^{233}$   $B_i^{234}$   $B_i^{235}$   $B_i^{236}$   $B_i^{237}$   $B_i^{238}$   $B_i^{239}$   $B_i^{240}$   $B_i^{241}$   $B_i^{242}$   $B_i^{243}$   $B_i^{244}$   $B_i^{245}$   $B_i^{246}$   $B_i^{247}$   $B_i^{248}$   $B_i^{249}$   $B_i^{250}$   $B_i^{251}$   $B_i^{252}$   $B_i^{253}$   $B_i^{254}$   $B_i^{255}$   $B_i^{256}$   $B_i^{257}$   $B_i^{258}$   $B_i^{259}$   $B_i^{260}$   $B_i^{261}$   $B_i^{262}$   $B_i^{263}$   $B_i^{264}$   $B_i^{265}$   $B_i^{266}$   $B_i^{267}$   $B_i^{268}$   $B_i^{269}$   $B_i^{270}$   $B_i^{271}$   $B_i^{272}$   $B_i^{273}$   $B_i^{274}$   $B_i^{275}$   $B_i^{276}$   $B_i^{277}$   $B_i^{278}$   $B_i^{279}$   $B_i^{280}$   $B_i^{281}$   $B_i^{282}$   $B_i^{283}$   $B_i^{284}$   $B_i^{285}$   $B_i^{286}$   $B_i^{287}$   $B_i^{288}$   $B_i^{289}$   $B_i^{290}$   $B_i^{291}$   $B_i^{292}$   $B_i^{293}$   $B_i^{294}$   $B_i^{295}$   $B_i^{296}$   $B_i^{297}$   $B_i^{298}$   $B_i^{299}$   $B_i^{300}$   $B_i^{301}$   $B_i^{302}$   $B_i^{303}$   $B_i^{304}$   $B_i^{305}$   $B_i^{306}$   $B_i^{307}$   $B_i^{308}$   $B_i^{309}$   $B_i^{310}$   $B_i^{311}$   $B_i^{312}$   $B_i^{313}$   $B_i^{314}$   $B_i^{315}$   $B_i^{316}$   $B_i^{317}$   $B_i^{318}$   $B_i^{319}$   $B_i^{320}$   $B_i^{321}$   $B_i^{322}$   $B_i^{323}$   $B_i^{324}$   $B_i^{325}$   $B_i^{326}$   $B_i^{327}$   $B_i^{328}$   $B_i^{329}$   $B_i^{330}$   $B_i^{331}$   $B_i^{332}$   $B_i^{333}$   $B_i^{334}$   $B_i^{335}$   $B_i^{336}$   $B_i^{337}$   $B_i^{338}$   $B_i^{339}$   $B_i^{340}$   $B_i^{341}$   $B_i^{342}$   $B_i^{343}$   $B_i^{344}$   $B_i^{345}$   $B_i^{346}$   $B_i^{347}$   $B_i^{348}$   $B_i^{349}$   $B_i^{350}$   $B_i^{351}$   $B_i^{352}$   $B_i^{353}$   $B_i^{354}$   $B_i^{355}$   $B_i^{356}$   $B_i^{357}$   $B_i^{358}$   $B_i^{359}$   $B_i^{360}$   $B_i^{361}$   $B_i^{362}$   $B_i^{363}$   $B_i^{364}$   $B_i^{365}$   $B_i^{366}$   $B_i^{367}$   $B_i^{368}$   $B_i^{369}$   $B_i^{370}$   $B_i^{371}$   $B_i^{372}$   $B_i^{373}$   $B_i^{374}$   $B_i^{375}$   $B_i^{376}$   $B_i^{377}$   $B_i^{378}$   $B_i^{379}$   $B_i^{380}$   $B_i^{381}$   $B_i^{382}$   $B_i^{383}$   $B_i^{384}$   $B_i^{385}$   $B_i^{386}$   $B_i^{387}$   $B_i^{388}$   $B_i^{389}$   $B_i^{390}$   $B_i^{391}$   $B_i^{392}$   $B_i^{393}$   $B_i^{394}$   $B_i^{395}$   $B_i^{396}$   $B_i^{397}$   $B_i^{398}$   $B_i^{399}$   $B_i^{400}$   $B_i^{401}$   $B_i^{402}$   $B_i^{403}$   $B_i^{404}$   $B_i^{405}$   $B_i^{406}$   $B_i^{407}$   $B_i^{408}$   $B_i^{409}$   $B_i^{410}$   $B_i^{411}$   $B_i^{412}$   $B_i^{413}$   $B_i^{414}$   $B_i^{415}$   $B_i^{416}$   $B_i^{417}$   $B_i^{418}$   $B_i^{419}$   $B_i^{420}$   $B_i^{421}$   $B_i^{422}$   $B_i^{423}$   $B_i^{424}$   $B_i^{425}$   $B_i^{426}$   $B_i^{427}$   $B_i^{428}$   $B_i^{429}$   $B_i^{430}$   $B_i^{431}$   $B_i^{432}$   $B_i^{433}$   $B_i^{434}$   $B_i^{435}$   $B_i^{436}$   $B_i^{437}$   $B_i^{438}$   $B_i^{439}$   $B_i^{440}$   $B_i^{441}$   $B_i^{442}$   $B_i^{443}$   $B_i^{444}$   $B_i^{445}$   $B_i^{446}$   $B_i^{447}$   $B_i^{448}$   $B_i^{449}$   $B_i^{450}$   $B_i^{451}$   $B_i^{452}$   $B_i^{453}$   $B_i^{454}$   $B_i^{455}$   $B_i^{456}$   $B_i^{457}$   $B_i^{458}$   $B_i^{459}$   $B_i^{460}$   $B_i^{461}$   $B_i^{462}$   $B_i^{463}$   $B_i^{464}$   $B_i^{465}$   $B_i^{466}$   $B_i^{467}$   $B_i^{468}$   $B_i^{469}$   $B_i^{470}$   $B_i^{471}$   $B_i^{472}$   $B_i^{473}$   $B_i^{474}$   $B_i^{475}$   $B_i^{476}$   $B_i^{477}$   $B_i^{478}$   $B_i^{479}$   $B_i^{480}$   $B_i^{481}$   $B_i^{482}$   $B_i^{483}$   $B_i^{484}$   $B_i^{485}$   $B_i^{486}$   $B_i^{487}$   $B_i^{488}$   $B_i^{489}$   $B_i^{490}$   $B_i^{491}$   $B_i^{492}$   $B_i^{493}$   $B_i^{494}$   $B_i^{495}$   $B_i^{496}$   $B_i^{497}$   $B_i^{498}$   $B_i^{499}$   $B_i^{500}$   $B_i^{501}$   $B_i^{502}$   $B_i^{503}$   $B_i^{504}$   $B_i^{505}$   $B_i^{506}$   $B_i^{507}$   $B_i^{508}$   $B_i^{509}$   $B_i^{510}$   $B_i^{511}$   $B_i^{512}$   $B_i^{513}$   $B_i^{514}$   $B_i^{515}$   $B_i^{516}$   $B_i^{517}$   $B_i^{518}$   $B_i^{519}$   $B_i^{520}$   $B_i^{521}$   $B_i^{522}$   $B_i^{523}$   $B_i^{524}$   $B_i^{525}$   $B_i^{526}$   $B_i^{527}$   $B_i^{528}$   $B_i^{529}$   $B_i^{530}$   $B_i^{531}$   $B_i^{532}$   $B_i^{533}$   $B_i^{534}$   $B_i^{535}$   $B_i^{536}$   $B_i^{537}$   $B_i^{538}$   $B_i^{539}$   $B_i^{540}$   $B_i^{541}$   $B_i^{542}$   $B_i^{543}$   $B_i^{544}$   $B_i^{545}$   $B_i^{546}$   $B_i^{547}$   $B_i^{548}$   $B_i^{549}$   $B_i^{550}$   $B_i^{551}$   $B_i^{552}$   $B_i^{553}$   $B_i^{554}$   $B_i^{555}$   $B_i^{556}$   $B_i^{557}$   $B_i^{558}$   $B_i^{559}$   $B_i^{560}$   $B_i^{561}$   $B_i^{562}$   $B_i^{563}$   $B_i^{564}$   $B_i^{565}$   $B_i^{566}$   $B_i^{567}$   $B_i^{568}$   $B_i^{569}$   $B_i^{570}$   $B_i^{571}$   $B_i^{572}$   $B_i^{573}$   $B_i^{574}$   $B_i^{575}$   $B_i^{576}$   $B_i^{577}$   $B_i^{578}$   $B_i^{579}$   $B_i^{580}$   $B_i^{581}$   $B_i^{582}$   $B_i^{583}$   $B_i^{584}$   $B_i^{585}$   $B_i^{586}$   $B_i^{587}$   $B_i^{588}$   $B_i^{589}$   $B_i^{590}$   $B_i^{591}$   $B_i^{592}$   $B_i^{593}$   $B_i^{594}$   $B_i^{595}$   $B_i^{596}$   $B_i^{597}$   $B_i^{598}$   $B_i^{599}$   $B_i^{600}$   $B_i^{601}$   $B_i^{602}$   $B_i^{603}$   $B_i^{604}$   $B_i^{605}$   $B_i^{606}$   $B_i^{607}$   $B_i^{608}$   $B_i^{609}$   $B_i^{610}$   $B_i^{611}$   $B_i^{612}$   $B_i^{613}$   $B_i^{614}$   $B_i^{615}$   $B_i^{616}$   $B_i^{617}$   $B_i^{618}$   $B_i^{619}$   $B_i^{620}$   $B_i^{621}$   $B_i^{622}$   $B_i^{623}$   $B_i^{624}$   $B_i^{625}$   $B_i^{626}$   $B_i^{627}$   $B_i^{628}$   $B_i^{629}$   $B_i^{630}$   $B_i^{631}$   $B_i^{632}$   $B_i^{633}$   $B_i^{634}$   $B_i^{635}$   $B_i^{636}$   $B_i^{637}$   $B_i^{638}$   $B_i^{639}$   $B_i^{640}$   $B_i^{641}$   $B_i^{642}$   $B_i^{643}$   $B_i^{644}$   $B_i^{645}$   $B_i^{646}$   $B_i^{647}$   $B_i^{648}$   $B_i^{649}$   $B_i^{650}$   $B_i^{651}$   $B_i^{652}$   $B_i^{653}$   $B_i^{654}$   $B_i^{655}$   $B_i^{656}$   $B_i^{657}$   $B_i^{658}$   $B_i^{659}$   $B_i^{660}$   $B_i^{661}$   $B_i^{662}$   $B_i^{663}$   $B_i^{664}$   $B_i^{665}$   $B_i^{666}$   $B_i^{667}$   $B_i^{668}$   $B_i^{669}$   $B_i^{670}$   $B_i^{671}$   $B_i^{672}$   $B_i^{673}$   $B_i^{674}$   $B_i^{675}$   $B_i^{676}$   $B_i^{677}$   $B_i^{678}$   $B_i^{679}$   $B_i^{680}$   $B_i^{681}$   $B_i^{682}$   $B_i^{683}$   $B_i^{684}$   $B_i^{685}$   $B_i^{686}$   $B_i^{687}$   $B_i^{688}$   $B_i^{689}$   $B_i^{690}$   $B_i^{691}$   $B_i^{692}$   $B_i^{693}$   $B_i^{694}$   $B_i^{695}$   $B_i^{696}$   $B_i^{697}$   $B_i^{698}$   $B_i^{699}$   $B_i^{700}$   $B_i^{701}$   $B_i^{702}$   $B_i^{703}$   $B_i^{704}$   $B_i^{705}$   $B_i^{706}$   $B_i^{707}$   $B_i^{708}$   $B_i^{709}$   $B_i^{710}$   $B_i^{711}$   $B_i^{712}$   $B_i^{713}$   $B_i^{714}$   $B_i^{715}$   $B_i^{716}$   $B_i^{717}$   $B_i^{718}$   $B_i^{719}$   $B_i^{720}$   $B_i^{721}$   $B_i^{722}$   $B_i^{723}$   $B_i^{724}$   $B_i^{725}$   $B_i^{726}$   $B_i^{727}$   $B_i^{728}$   $B_i^{729}$   $B_i^{730}$   $B_i^{731}$   $B_i^{732}$   $B_i^{733}$   $B_i^{734}$   $B_i^{735}$   $B_i^{736}$   $B_i^{737}$   $B_i^{738}$   $B_i^{739}$   $B_i^{740}$   $B_i^{741}$   $B_i^{742}$   $B_i^{743}$   $B_i^{744}$   $B_i^{745}$   $B_i^{746}$   $B_i^{747}$   $B_i^{748}$   $B_i^{749}$   $B_i^{750}$   $B_i^{751}$   $B_i^{752}$   $B_i^{753}$   $B_i^{754}$   $B_i^{755}$   $B_i^{756}$   $B_i^{757}$   $B_i^{758}$   $B_i^{759}$   $B_i^{760}$   $B_i^{761}$   $B_i^{762}$   $B_i^{763}$   $B_i^{764}$   $B_i^{765}$   $B_i^{766}$   $B_i^{767}$   $B_i^{768}$   $B_i^{769}$   $B_i^{770}$   $B_i^{771}$   $B_i^{772}$   $B_i^{773}$   $B_i^{774}$   $B_i^{775}$   $B_i^{776}$   $B_i^{777}$   $B_i^{778}$   $B_i^{779}$   $B_i^{780}$   $B_i^{781}$   $B_i^{782}$   $B_i^{783}$   $B_i^{784}$   $B_i^{785}$   $B_i^{786}$   $B_i^{787}$   $B_i^{788}$   $B_i^{789}$   $B_i^{790}$   $B_i^{791}$   $B_i^{792}$   $B_i^{793}$   $B_i^{794}$   $B_i^{795}$   $B_i^{796}$   $B_i^{797}$   $B_i^{798}$   $B_i^{799}$   $B_i^{800}$   $B_i^{801}$   $B_i^{802}$   $B_i^{803}$   $B_i^{804}$   $B_i^{805}$   $B_i^{806}$   $B_i^{807}$   $B_i^{808}$   $B_i^{809}$   $B_i^{810}$   $B_i^{811}$   $B_i^{812}$   $B_i^{813}$   $B_i^{814}$   $B_i^{815}$   $B_i^{816}$   $B_i^{817}$   $B_i^{818}$   $B_i^{819}$   $B_i^{820}$   $B_i^{821}$   $B_i^{822}$   $B_i^{823}$   $B_i^{824}$   $B_i^{825}$   $B_i^{826}$   $B_i^{827}$   $B_i^{828}$   $B_i^{829}$   $B_i^{830}$   $B_i^{831}$   $B_i^{832}$   $B_i^{833}$   $B_i^{834}$   $B_i^{835}$   $B_i^{836}$   $B_i^{837}$   $B_i^{838}$   $B_i^{839}$   $B_i^{840}$   $B_i^{841}$   $B_i^{842}$   $B_i^{843}$   $B_i^{844}$   $B_i^{845}$   $B_i^{846}$   $B_i^{847}$   $B_i^{848}$   $B_i^{849}$   $B_i^{850}$   $B_i^{851}$   $B_i^{852}$   $B_i^{853}$   $B_i^{854}$   $B_i^{855}$   $B_i^{856}$   $B_i^{857}$   $B_i^{858}$   $B_i^{859}$   $B_i^{860}$   $B_i^{861}$   $B_i^{862}$   $B_i^{863}$   $B_i^{864}$   $B_i^{865}$   $B_i^{866}$   $B_i^{867}$   $B_i^{868}$   $B_i^{869}$   $B_i^{870}$   $B_i^{871}$   $B_i^{872}$   $B_i^{873}$   $B_i^{874}$   $B_i^{875}$   $B_i^{876}$   $B_i^{877}$   $B_i^{878}$   $B_i^{879}$   $B_i^{880}$   $B_i^{881}$   $B_i^{882}$   $B_i^{883}$   $B_i^{884}$   $B_i^{885}$   $B_i^{886}$   $B_i^{887}$   $B_i^{888}$   $B_i^{889}$   $B_i^{890}$   $B_i^{891}$   $B_i^{892}$   $B_i^{893}$   $B_i^{894}$   $B_i^{895}$   $B_i^{896}$   $B_i^{897}$   $B_i^{898}$   $B_i^{899}$   $B_i^{900}$   $B_i^{901}$   $B_i^{902}$   $B_i^{903}$   $B_i^{904}$   $B_i^{905}$   $B_i^{906}$   $B_i^{907}$   $B_i^{908}$   $B_i^{909}$   $B_i^{910}$   $B_i^{911}$   $B_i^{912}$   $B_i^{913}$   $B_i^{914}$   $B_i^{915}$   $B_i^{916}$   $B_i^{917}$   $B_i^{918}$   $B_i^{919}$   $B_i^{920}$   $B_i^{921}$   $B_i^{922}$   $B_i^{923}$   $B_i^{924}$   $B_i^{925}$   $B_i^{926}$   $B_i^{927}$   $B_i^{928}$   $B_i^{929}$   $B_i^{930}$   $B_i^{931}$   $B_i^{932}$   $B_i^{933}$   $B_i^{934}$   $B_i^{935}$   $B_i^{936}$   $B_i^{937}$   $B_i^{938}$   $B_i^{939}$   $B_i^{940}$   $B_i^{941}$   $B_i^{942}$   $B_i^{943}$   $B_i^{944}$   $B_i^{945}$   $B_i^{946}$   $B_i^{947}$   $B_i^{948}$   $B_i^{949}$   $B_i^{950}$   $B_i^{951}$   $B_i^{952}$   $B_i^{953}$   $B_i^{954}$   $B_i^{955}$   $B_i^{956}$   $B_i^{957}$   $B_i^{958}$   $B_i^{959}$   $B_i^{960}$   $B_i^{961}$   $B_i^{962}$   $B_i^{963}$   $B_i^{964}$   $B_i^{965}$   $B_i^{966}$   $B_i^{967}$   $B_i^{968}$   $B_i^{969}$   $B_i^{970}$   $B_i^{971}$   $B_i^{972}$   $B_i^{973}$   $B_i^{974}$   $B_i^{975}$   $B_i^{976}$   $B_i^{977}$   $B_i^{978}$   $B_i^{979}$   $B_i^{980}$   $B_i^{981}$   $B_i^{982}$   $B_i^{983}$   $B_i^{984}$   $B_i^{985}$   $B_i^{986}$   $B_i^{987}$   $B_i^{988}$   $B_i^{989}$   $B_i^{990}$   $B_i^{991}$   $B_i^{992}$   $B_i^{993}$   $B_i^{994}$   $B_i^{995}$   $B_i^{996}$   $B_i^{997}$   $B_i^{998}$   $B_i^{999}$   $B_i^{1000}$*

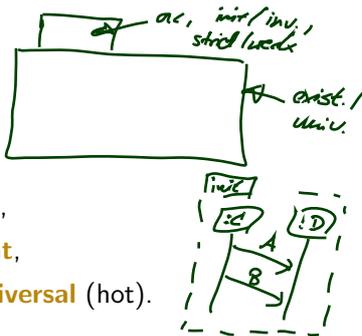
# Example



# Finally: The LSC Semantics

A full LSC  $L$  consist of

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

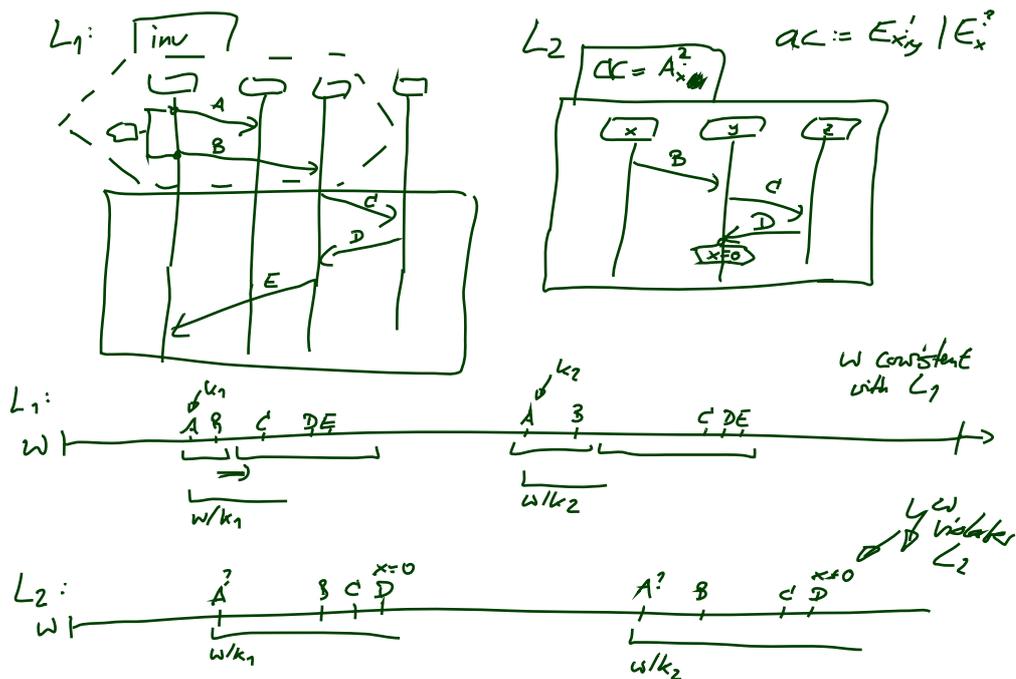


A set  $W$  of timed words over  $B$  and  $V$  **satisfies**  $L$ , denoted  $W \models L$ , iff  $L$

- **universal** (= hot), **initial**, and  
 $\forall w \in W \forall \beta : X \rightarrow \text{dom}(w_0) \bullet w \text{ activates } L \implies w \in \mathcal{L}(B_L)$ .
- **universal** (= hot), **invariant**, and  
 $\forall w \in W \forall k \in \mathbb{N}_0 \forall \beta : X \rightarrow \text{dom}(w_k) \bullet w/k \text{ activates } L \implies w/k \in \mathcal{L}(B_L)$ .
- **existential** (= cold), **initial**, and  
 $\exists w \in W \exists \beta : X \rightarrow \text{dom}(w_0) \bullet w \text{ activates } L \wedge w \in \mathcal{L}(B_L)$ .
- **existential** (= cold), **invariant**, and  
 $\exists w \in W \exists k \in \mathbb{N}_0 \exists \beta : X \rightarrow \text{dom}(w_k) \bullet w/k \text{ activates } L \wedge w/k \in \mathcal{L}(B_L)$ .

suffix of  $w$   
including  $w_k$   
element

- 17 - 2012-01-31 - Skeseem -





## Back to UML: Interactions

### Interactions as Reflective Description

- In UML, reflective (temporal) descriptions are subsumed by **interactions**.
- A UML model  $\mathcal{M} = (\mathcal{CD}, \mathcal{SM}, \mathcal{OD}, \mathcal{I})$  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).

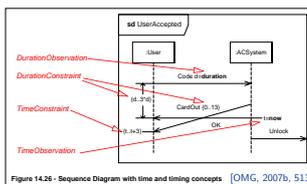


Figure 14.26 - Sequence Diagram with time and timing concepts [OMG, 2007b, 513]

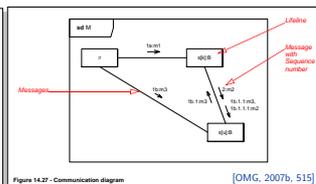


Figure 14.27 - Communication diagram [OMG, 2007b, 515]

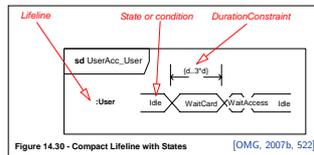


Figure 14.30 - Compact Lifeline with States [OMG, 2007b, 522]

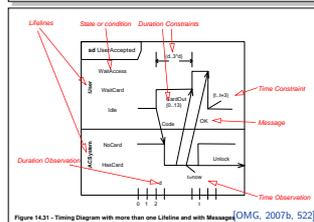
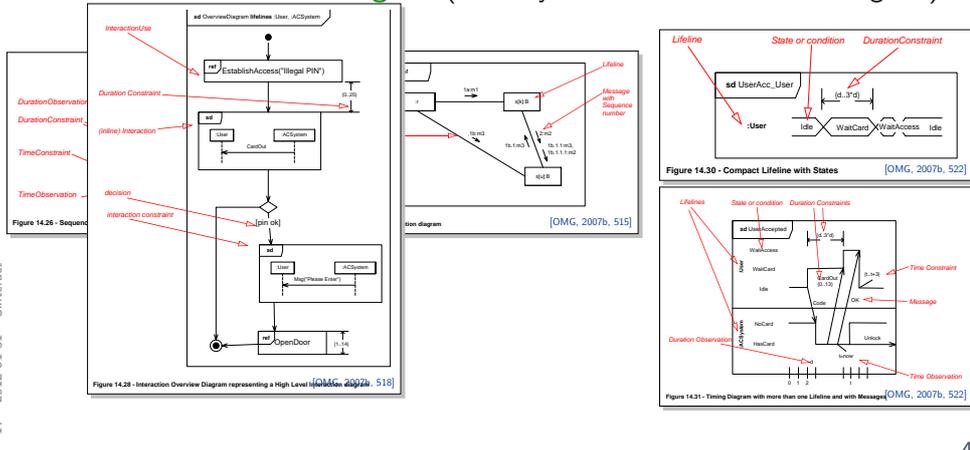


Figure 14.31 - Timing Diagram with more than one Lifeline and with Messages [OMG, 2007b, 522]

## Interactions as Reflective Description

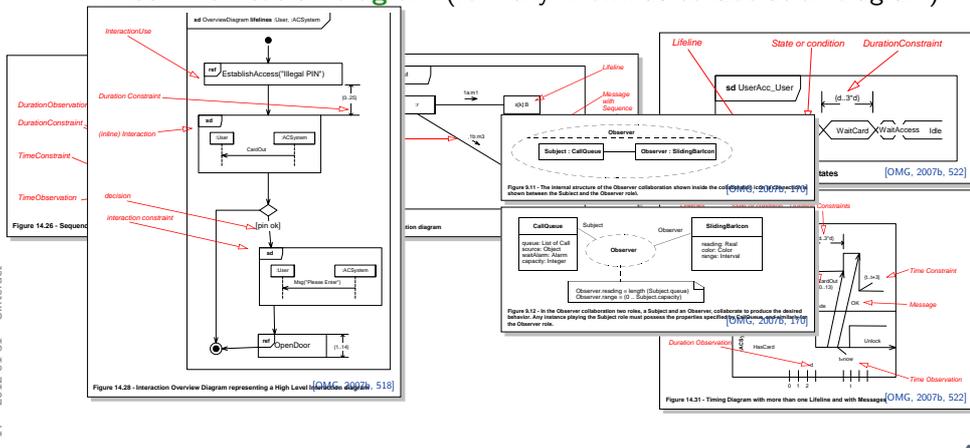
- In UML, reflective (temporal) descriptions are subsumed by **interactions**.
- A UML model  $\mathcal{M} = (\mathcal{CD}, \mathcal{SM}, \mathcal{OD}, \mathcal{I})$  has a set of interactions  $\mathcal{I}$ .
- An interaction  $\mathcal{I} \in \mathcal{I}$  can be (OMG claim: equivalently) **diagrammed**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



- 17 - 2012-01-31 - Sinteract -

## Interactions as Reflective Description

- In UML, reflective (temporal) descriptions are subsumed by **interactions**.
- A UML model  $\mathcal{M} = (\mathcal{CD}, \mathcal{SM}, \mathcal{OD}, \mathcal{I})$  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).



- 17 - 2012-01-31 - Sinteract -

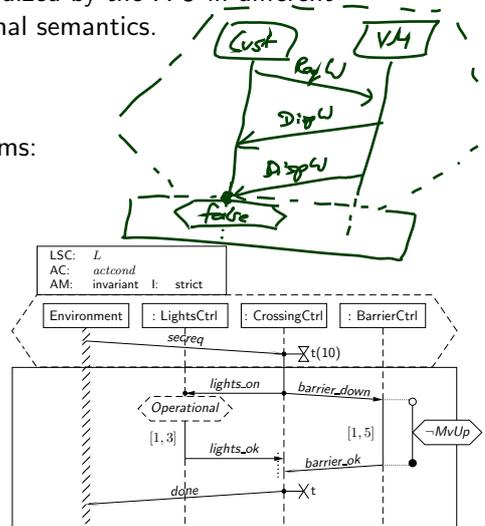
## Why Sequence Diagrams?

**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**



43/47

## Thus: Live Sequence Charts

- **SDs of UML 2.x** address **some** issues, yet the standard exhibits unclarity and even contradictions [Harel and Maoz, 2007, Störle, 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.

44/47

## Side Note: Protocol State Machines

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.

PSM:



## References

## 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.
- [Harel and Maoz, 2007] Harel, D. and Maoz, S. (2007). Assert and negate revisited: Modal semantics for UML sequence diagrams. *Software and System Modeling (SoSyM)*. To appear. (Early version in SCESM'06, 2006, pp. 13-20).
- [Harel and Marelly, 2003] Harel, D. and Marelly, 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/07-11-04.
- [OMG, 2007b] OMG (2007b). Unified modeling language: Superstructure, version 2.1.2. Technical Report formal/07-11-02.
- [Störrle, 2003] Störrle, H. (2003). Assert, negate and refinement in UML-2 interactions. In Jürjens, J., Rumpe, B., France, R., and Fernandez, E. B., editors, *CSDUML 2003*, number TUM-I0323. Technische Universität München.