Software Design, Modelling and Analysis in UML

Lecture 12: Core State Machines III

2011-12-11

Prof. Dr. Andreas Podelski, Dr. Bernd Westphal

Albert-Ludwigs-Universität Freiburg, Germany
Contents & Goals

Last Lecture:
- The basic causality model
- Ether

This Lecture:
- Educational Objectives: Capabilities for following tasks/questions.
  - What does this State Machine mean? What happens if I inject this event?
  - Can you please model the following behaviour.
  - What is: Signal, Event, Ether, Transformer, Step, RTC.

- Content:
  - System Configuration, Transformer
  - Examples for transformer
  - Run-to-completion Step
  - Putting It All Together
...:
- We have to formally define what **event occurrence** is.
- We have to define where events are stored – what the event pool is.
- We have to explain how **transitions are chosen** – “matching”.
- We have to explain what the **effect of actions** is – on state and event pool.
- We have to decide on the **granularity** — micro-steps, steps, run-to-completion steps (aka. super-steps)?
- We have to formally define a notion of **stability** and RTC-step **completion**.

- And then: hierarchical state machines.
Roadmap: Chronologically

(i) What do we (have to) cover?
  UML State Machine Diagrams Syntax.

(ii) Def.: Signature with signals.

(iii) Def.: Core state machine.

(iv) Map UML State Machine Diagrams to core state machines.

Semantics:
  The Basic Causality Model

(v) Def.: Ether (aka. event pool)

(vi) Def.: System configuration.

(vii) Def.: Event.

(viii) Def.: Transformer.

(ix) Def.: Transition system, computation.

(x) Transition relation induced by core state machine.

(xi) Def.: step, run-to-completion step.

(xii) Later: Hierarchical state machines.
System Configuration, Ether, Transformer
**Ether aka. Event Pool**

**Definition.** Let $\mathcal{S} = (T, C, V, atr)$ be a signature with signals and $\mathcal{D}$ a structure. We call a structure $(Eth, ready, \oplus, \ominus, [\cdot])$ an ether over $\mathcal{S}$ and $\mathcal{D}$ if and only if it provides

- a **ready** operation which yields a set of events that are ready for a given object, i.e.
  
  \[
  \text{ready} : Eth \times \mathcal{D}(C) \rightarrow 2^{\mathcal{D}(\mathcal{E})}
  \]

- a operation to **insert** an event destined for a given object, i.e.
  
  \[
  \oplus : Eth \times \mathcal{D}(C) \times \mathcal{D}(\mathcal{E}) \rightarrow Eth
  \]

- a operation to **remove** an event, i.e.
  
  \[
  \ominus : Eth \times \mathcal{D}(\mathcal{E}) \rightarrow Eth
  \]

- an operation to clear the ether for a given object, i.e.
  
  \[
  [\cdot] : Eth \times \mathcal{D}(C) \rightarrow Eth.
  \]
Ether and [OMG, 2007b]

The standard distinguishes (among others)

- **SignalEvent** [OMG, 2007b, 450] and **Reception** [OMG, 2007b, 447].

On **SignalEvents**, it says

A signal event represents the receipt of an asynchronous signal instance. A signal event may, for example, cause a state machine to trigger a transition. [OMG, 2007b, 449]

[...]

**Semantic Variation Points**

The means by which requests are transported to their target depend on the type of requesting action, the target, the properties of the communication medium, and numerous other factors.

In some cases, this is instantaneous and completely reliable while in others it may involve transmission delays of variable duration, loss of requests, reordering, or duplication.

(See also the discussion on page 421.) [OMG, 2007b, 450]

Our **ether** is a general representation of the possible choices.

**Often seen minimal requirement**: order of sending **by one object** is preserved. But: we’ll later briefly discuss “discarding” of events.
**Definition.** Let $\mathcal{S}_0 = (\mathcal{T}_0, \mathcal{C}_0, V_0, atr_0, \mathcal{E})$ be a signature with signals, $\mathcal{D}_0$ a structure of $\mathcal{S}_0$, $(\text{Eth}, \text{ready}, \oplus, \ominus, [\cdot])$ an ether over $\mathcal{S}_0$ and $\mathcal{D}_0$. Furthermore assume there is one core state machine $M_C$ per class $C \in \mathcal{C}$.

A system configuration over $\mathcal{S}_0$, $\mathcal{D}_0$, and $\text{Eth}$ is a pair $(\sigma, \varepsilon) \in \Sigma_\mathcal{D} \times \text{Eth}$ where

- $\mathcal{I} = (\mathcal{T}_0 \cup \{S_{M_C} \mid C \in \mathcal{C}\}, \mathcal{C}_0,$
  $V_0 \cup \{(\text{stable} : \text{Bool}, -, \text{true}, \emptyset)\}$
  $\cup \{(\text{st}_C : S_{M_C}, +, s_0, \emptyset) \mid C \in \mathcal{C}\}$
  $\cup \{(\text{params}_E : E_0, 1, +, \emptyset, \emptyset) \mid E \in \mathcal{E}_0\}$,
  $\{C \mapsto atr_0(C)\}$
  $\cup \{\text{stable}, \text{st}_C\} \cup \{\text{params}_E \mid E \in \mathcal{E}_0\} \mid C \in \mathcal{C}\}$, and
  $\mathcal{D} = \mathcal{D}_0 \cup \{S_{M_C} \mapsto S(M_C) \mid C \in \mathcal{C}\}$, and
- $\sigma(u)(r) \cap \mathcal{D}(\mathcal{E}_0) = \emptyset$ for each $u \in \text{dom}(\sigma)$ and $r \in V_{0,\text{attr}}$, e.g. $r : C_0$. 

If $\text{bool} \in \mathcal{J}_0$ then add it here, and have $\mathcal{D}(\text{bool}) = \text{B}$. If $\text{bool} \in \mathcal{J}_0$ then add it here, and have $\mathcal{D}(\text{bool}) = \text{B}$
$C$

$x: \text{int}$  
$y: \text{int}$

$\text{if} \ x < y \text{ return } 1$

$\text{if} \ x > y \text{ return } 2$

$\text{return } 3$

$S_1$

$S_2$

$S_3$

$D_0(\text{Int}) = 2$

$\mathcal{F}_0 = (\{\text{Int}\}, \{C, E, F\}, \{x: \text{Int}, y: \text{Int}\}, \{C(\text{Int}, x, y), E(x, y), F(x, y)\})$

$\mathcal{F} = (\{\text{Int}, S_{nc}\}, \{C, E, F\}, \{x, y, a: \text{Int}\}, \text{stable: bool, } st_c: S_{nc}, \text{params}_E: E_0, \text{params}_F: F_0)$

$D(\text{Int}) = D(\text{Int})$

$D(S_{nc}) = \{s_0, s_1, s_2, s_3\}$

$0: v = C$

$v = 1$

$w = C$

$v = 2$

$w = 0$

$st_c = s_2$

$a = 3$

$v = 3$

$w = E$

$v = E$

$w = F$

$w = V$

$w = V'$

$w = V''$

not reachable from $s_0$, but $s_1$ is a semantical issue

if $E_{ll}$ is shared FIFO queue

$E$: $u, v, v'$

Instance of $F$ is ready for $w$.
System Configuration Step-by-Step

- We start with some signature with signals $S_0 = (I_0, E_0, V_0, atr_0, E)$.

- A **system configuration** is a pair $(\sigma, \varepsilon)$ which comprises a system state $\sigma$ wrt. $S$ (not wrt. $S_0$).

- Such a **system state** $\sigma$ wrt. $S$ provides, for each object $u \in \text{dom}(\sigma)$,
  - values for the **explicit attributes** in $V_0$,
  - values for a number of **implicit attributes**, namely
    - a **stability flag**, i.e. $\sigma(u)(\text{stable})$ is a boolean value,
    - a **current (state machine) state**, i.e. $\sigma(u)(st)$ denotes one of the states of core state machine $M_C$,
    - a temporary association to access **event parameters** for each class, i.e. $\sigma(u)(\text{params}_E)$ is defined for each $E \in E$.

- For convenience require: there is **no link to an event** except for $\text{params}_E$. 
Stability

Definition.
Let \((\sigma, \varepsilon)\) be a system configuration over some \(\mathcal{S}_0, \mathcal{D}_0, Eth\).

We call an object \(u \in \text{dom}(\sigma) \cap \mathcal{D}(\mathcal{C}_0)\) \textbf{stable in} \(\sigma\) if and only if

\[\sigma(u)(\text{stable}) = true.\]
**Events Are Instances of Signals**

**Definition.** Let $\mathcal{D}_0$ be a structure of the signature with signals $\mathcal{I}_0 = (\mathcal{T}_0, \mathcal{C}_0, V_0, atr_0, \mathcal{E})$ and let $E \in \mathcal{E}_0$ be a signal.

Let $atr(E) = \{v_1, \ldots, v_n\}$. We call

$$e = (E, \{v_1 \mapsto d_1, \ldots, v_n \mapsto d_n\}),$$

or shorter (if mapping is clear from context)

$$(E, (d_1, \ldots, d_n))$$ or $$(E, \vec{d})$$,

an event (or an instance) of signal $E$ (if type-consistent).

We use $Ev_{\mathcal{S}}(\mathcal{E}_0, \mathcal{D}_0)$ to denote the set of all events of all signals in $\mathcal{I}_0$ wrt. $\mathcal{D}_0$.

As we always try to maximize confusion...:

- By our existing naming convention, $u \in \mathcal{D}(E)$ is also called instance of the (signal) class $E$ in system configuration $(\sigma, \varepsilon)$ if $u \in \text{dom}(\sigma)$.
- The corresponding event is then $(E, \sigma(u))$. 
The idea is the following:

- **Signals** are **types** (classes).

- **Instances of signals** (in the standard sense) are kept in the **system state** component \( \sigma \) of system configurations \((\sigma, \varepsilon)\).

- **Identities** of signal instances are kept in the **ether**.

- Each signal instance is in particular an **event** — somehow “a recording that this signal occurred” (without caring for its identity)

- The main difference between **signal instance** and **event**: Events don’t have an identity.

- Why is this useful? In particular for **reflective** descriptions of behaviour, we are typically not interested in the identity of a signal instance, but only whether it is an “\(E\)” or “\(F\)” , and which parameters it carries.
**Where are we?**

- **Wanted**: a labelled transition relation

\[(\sigma, \varepsilon) \xrightarrow{(\text{cons}, \text{Snd})} (\sigma', \varepsilon')\]

on system configuration, labelled with the **consumed** and **sent** events, 
\((\sigma', \varepsilon')\) being the result (or effect) of **one object** \(u_x\) taking a transition of **its** state machine from the current state mach. state \(\sigma(u_x)(st_C)\).

- **Have**: system configuration \((\sigma, \varepsilon)\) comprising current state machine state and stability flag for each object, and the ether.

- **Plan**:

  (i) Introduce **transformer** as the semantics of action annotations.

  **Intuitively**, \((\sigma', \varepsilon')\) is the effect of applying the transformer of the taken transition.

  (ii) Explain how to choose transitions depending on \(\varepsilon\) and when to stop taking transitions — the **run-to-completion “algorithm”**.
Transformer

Definition.
Let $\Sigma_0$ the set of system configurations over some $\mathcal{S}_0$, $\mathcal{D}_0$, $\mathcal{E}_0$.
We call a relation $t \subseteq \mathcal{D}(\mathcal{C}) \times (\Sigma_0 \times \mathcal{E}_0) \times (\Sigma_0 \times \mathcal{E}_0)$ a (system configuration) transformer.

- In the following, we assume that each application of a transformer $t$ to some system configuration $(\sigma, \varepsilon)$ for object $u_x$ is associated with a set of observations

$$
Obst[u_x](\sigma, \varepsilon) \in 2^{\mathcal{D}(\mathcal{C}) \times \mathcal{D}(\mathcal{C}) \times Evs(\mathcal{E} \cup \{*, +\}, \mathcal{D}) \times \mathcal{D}(\mathcal{C})}.
$$

- An observation $(u_{src}, u_e, (E, \vec{d}), u_{dst}) \in Obst[u_x](\sigma, \varepsilon)$ represents the information that, as a “side effect” of $u_x$ executing $t$, an event (!) $(E, \vec{d})$ has been sent from $u_{src}$ to $u_{dst}$.

Special cases: creation/destruction.
Why Transformers?

- **Recall** the (simplified) syntax of transition annotations:
  
  $$annot ::= \langle event \rangle \ [ \ ']' \ [ \ ']' \ [ \ ']' \ [ \ '/'] \ [ \ ']' \ [ \ ']'$$

- **Clear**: $\langle event \rangle$ is from $\mathcal{E}$ of the corresponding signature.

- **But**: What are $\langle guard \rangle$ and $\langle action \rangle$?
  
  - UML can be viewed as being **parameterized** in **expression language** (providing $\langle guard \rangle$) and **action language** (providing $\langle action \rangle$).

- **Examples**:
  
  - **Expression Language**:
    - OCL
    - Java, C++, ... expressions
    - ...
  
  - **Action Language**:
    - UML Action Semantics, “Executable UML”
    - Java, C++, ... statements (plus some event send action)
    - ...
In the following, we consider:

\[ A_{\text{ty}} = \{ \text{skip} \} \]

\[ \forall \{ \text{ update } (\text{expr}_1, v, \text{expr}_2) / \text{expr}_1, \text{expr}_2 \in \text{OCLExp}, v \in V \} \]

\[ \forall \{ \text{ send } (\text{expr}_1, E, \text{expr}_2) / \text{expr}_1, \text{expr}_2 \in \text{OCLExp}, E \in E \} \]

\[ \forall \{ \text{ create } (C, \text{expr}, v) / \text{expr} \in \text{OCLExp}, C \in C, v \in V \} \]

\[ \forall \{ \text{ destroy } (\text{expr}) / \text{expr} \in \text{OCLExp} \} \]

**Expr:** OCL expressions over \( V \)
(Transformers as Abstract Actions!)

In the following, we assume that we’re given

- an expression language $\text{Expr}$ for guards, and
- an action language $\text{Act}$ for actions,

and that we’re given

- a semantics for boolean expressions in form of a partial function

$$I[\cdot](\cdot, \cdot) : \text{Expr} \rightarrow ((\Sigma_{\text{D}} \times (\text{this} \rightarrow \mathcal{D}(\mathcal{C}))) \rightarrow \mathbb{B})$$

which evaluates expressions in a given system configuration,

Assuming $I$ to be partial is a way to treat “undefined” during runtime. If $I$ is not defined (for instance because of dangling-reference navigation or division-by-zero), we want to go to a designated “error” system configuration.

- a transformer for each action: for each $\text{act} \in \text{Act}$, we assume to have

$$t_{\text{act}} \subseteq \mathcal{D}(\mathcal{C}) \times (\Sigma_{\text{D}} \times \text{Eth}) \times (\Sigma_{\text{D}} \times \text{Eth})$$
We can make the assumptions from the previous slide because \textbf{instances exist}:

- for OCL, we have the OCL semantics from Lecture 03. Simply remove the pre-images which map to "⊥".
- for Java, the operational semantics of the SWT lecture uniquely defines transformers for sequences of Java statements.

We distinguish the following kinds of transformers:

- \textbf{skip}: do nothing — recall: this is the default action
- \textbf{send}: modifies $\varepsilon$ — interesting, because state machines are built around sending/consuming events
- \textbf{create}/\textbf{destroy}: modify domain of $\sigma$ — not specific to state machines, but let’s discuss them here as we’re at it
- \textbf{update}: modify own or other objects’ local state — boring
<table>
<thead>
<tr>
<th>abstract syntax</th>
<th>concrete syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>op</code></td>
<td></td>
</tr>
</tbody>
</table>

**intuitive semantics**

...  

**well-typedness**

...  

**semantics**

\[ ((\sigma, \varepsilon), (\sigma', \varepsilon')) \in t_{op}[u_x] \iff \ldots \]

or

\[ t_{op}[u_x](\sigma, \varepsilon) = \{(\sigma', \varepsilon')\} \text{ where } \ldots \]

**observables**

\[ Obs_{op}[u_x] = \{\ldots\}, \text{ not a relation, depends on choice} \]

**(error) conditions**

Not defined if \ldots
## Transformer: Skip

<table>
<thead>
<tr>
<th>abstract syntax</th>
<th>concrete syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>skip</td>
<td>skip</td>
</tr>
</tbody>
</table>

**intuitive semantics**

- *do nothing*

**well-typedness**

- \( ./ . \)  

**semantics**

\[
t[u_x](\sigma, \varepsilon) = \{ (\sigma, \varepsilon) \}
\]

**observables**

\[
Obs_{skip}[u_x](\sigma, \varepsilon) = \emptyset
\]

**(error) conditions**

- "if \( u_x \) executes \( skip \) on \((\sigma, \varepsilon)\), this results in \((\sigma, \varepsilon)\)"
**Transformer: Update**

<table>
<thead>
<tr>
<th><strong>abstract syntax</strong></th>
<th><strong>concrete syntax</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>update(expr_1, v, expr_2)</code></td>
<td><code>v := expr_2</code> (def. <code>this.v := expr_2</code>)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>intuitive semantics</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Update attribute <code>v</code> in the object denoted by <code>expr_1</code> to the value denoted by <code>expr_2</code>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>well-typedness</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>expr_1 : τ_C</code> and <code>v : τ ∈ attr(C)</code>; <code>expr_2 : τ</code>; <code>expr_1, expr_2</code> obey visibility and navigability</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>semantics</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>t_{update}(expr_1, v, expr_2)[u_x](σ, ε) = \{ (σ', ε) \}</code></td>
<td></td>
</tr>
<tr>
<td>where <code>σ' = σ[u ↦ σ(u)[v ↦ I[expr_2](σ, β)]]</code> with <code>u = I[expr_1](σ, β), β = \{ this ↦ u_x \}</code>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>observables</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Obs_{update}(expr_1, v, expr_2)[u_x] = ∅</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>(error) conditions</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Not defined if <code>I[expr_1](σ, β)</code> or <code>I[expr_2](σ, β)</code> not defined.</td>
<td></td>
</tr>
</tbody>
</table>

\[ i.e. \ t_{update} \cup \{u_x\}(σ, ε) = ∅ \]
Update Transformer Example

\[ SM_C: \]

\[
\begin{align*}
  & \frac{s_1}{x := x + 1} \\
  & \text{thus } x := \text{this } x + 1
\end{align*}
\]

\[
\text{update}(expr_1, v, expr_2)
\]

\[
t_{\text{update}}(expr_1, v, expr_2)[u_x](\sigma, \varepsilon) = (\sigma[u \mapsto \sigma(u)[v \mapsto I[expr_2](\sigma, \beta)]], \varepsilon),
\]

\[
u = I[expr_1](\sigma, \beta)
\]
References
References

