Excursus: Symbolic Büchi Automata (over Signature)

Symbolic Büchi Automata

Definition. A Symbolic Büchi Automaton (TBA) is a tuple $B = (\mathcal{E}, \mathcal{X}, Q, q_{\text{ini}}, \rightarrow, Q_F)$ where
- $\mathcal{X}$ is a set of logical variables,
- $\mathcal{E} = \mathcal{E}(\mathcal{X})$ is a set of Boolean expressions over $\mathcal{X}$,
- $Q$ is a finite set of states,
- $q_{\text{ini}} \in Q$ is the initial state,
- $\rightarrow \subseteq Q \times \mathcal{E} \times Q$ is the transition relation.

Transitions $(q, \psi, q')$ from $q$ to $q'$ are labelled with an expression $\psi \in \mathcal{E}(\mathcal{X})$.

- $Q_F \subseteq Q$ is the set of fair (or accepting) states.
For the connection between models and interactions, we disregard time.

Let $A \in \{\text{M}, \text{C}, \text{B}\}$. Then $\sigma \vdash (\text{A} =: \tilde{\text{A}})$.

Example: The Language of a Model
Example

LSC:

**AC:** actcond

**AM:** invariant

**Environment:**

- LightsCtrl
- Operational
- CrossingCtrl
- BarrierCtrl

- CrossingCtrl
  - LightsCtrl
  - BarrierCtrl

1 1 1 1 1

- CrossingCtrl
- LightsCtrl
- BarrierCtrl

1 1 1 1 1

Let \( \Theta = \{ \text{hot}, \text{cold} \} \). An LSC body is a tuple \((I, (/C4, \preceq), \sim, /CB, \text{Msg}, \text{Cond}, \text{LocInv})\).

- **I** is a finite set of instance lines.
- \((/C4, \preceq)\) is a finite, non-empty, partially ordered set of locations; each \(l \in /C4\) is associated with a temperature \(\theta(l) \in \Theta\) and an instance line \(i_l \in I\).
- \(\sim \subseteq /C4 \times /C4\) is an equivalence relation on locations, the simultaneity relation.

---

**Diagram:**

- Diagram illustrating the relationships between \(I\), \((/C4, \preceq)\), \(\sim\), \(/CB\), \text{Msg}, \text{Cond}, \text{LocInv}\), and the corresponding instance lines and location temperatures.
Let \( \text{local invariants} \) be defined as follows:

\[ \text{LSCBody:AbstractSyntax} \]

This definition includes the following conditions:

1. **Well-Formedness**
2. **Bondedness**
3. **Cyclicality**
4. **Bonding**
5. **Simultaneity**

Each condition can be linked to method/operation calls to enforce the specified behaviors.
Plan:

• Given an LSC $L$ with body $(I, (C_4, \preceq), \sim, CB, Msg, Cond, LocInv)$,

• construct a TBA $B_L$, and

• define $L(L)$ in terms of $L(B_L)$, in particular taking activation condition and activation mode into account.

Then $M|\models L$ (universal) if and only if $L(M) \subseteq L(L)$.

Recall: Intuitive Semantics

(i) Strictly After: $a \overset{b}{\rightarrow} a$

(ii) Simultaneously: $a \overset{b}{\sim} c$

(iii) Explicitly Unordered: $a \overset{b}{\sim} c$

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

Examples: Semantics?

$C_1$: $C_2$ $x > 3$

$A$ $B$ $C$ $D$ $E$

$v = 0$

$l_1, 0$ $l_1, 1$ $l_1, 2$ $l_1, 3$

$l_2, 0$ $l_2, 1$ $l_2, 2$ $l_2, 3$

$l_3, 0$ $l_3, 1$ $l_3, 2$

Formal LSC Semantics: It’s in the Cuts!

Definition. Let $(I, (C_4, \preceq), \sim, CB, Msg, Cond, LocInv)$ be an LSC body. An non-empty set $\emptyset \neq C \subseteq C_4$ is called a cut of the LSC body iff

• it is downward closed, i.e. $\forall l, l': l' \in C \land l \preceq l' \Rightarrow l \in C$,

• it is closed under simultaneity, i.e. $\forall l, l': l' \in C \land l \sim l' \Rightarrow l \in C$,

• 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 $\exists l \in C: \theta(l) = \text{hot} \land \nexists l' \in C: l \preceq l'$. Otherwise, $C$ is called cold, denoted by $\theta(C) = \text{cold}$.
satisfies the transition condition

\[ \text{for all } i, j, \text{ and } k, \]

\[ i \leq 0 = v \Rightarrow i' \leq 0 = x' \Rightarrow C \rightarrow C'' \]

\[ \text{Definition.} \]

"Loosen Tied Heads in an UML Class"

A Secessor Relation on Cuts

\[ \text{Examples: Cuts Or Not Cuts? Hot/Cold?} \]
\[
q := \bigvee \text{betheunionofthefiredsetsof} \ n_1 F F \ :
\]

- Strict mode: no message from a direct successor cut in.
- Weak mode: allowed to fire the self-loop

Intuition

\[
\text{Language of LSC Body: Intuition}
\]
\[
\begin{align*}
\psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) &= \psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) \\
\psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) &= \psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) \\
\psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) &= \psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right)
\end{align*}
\]

In the process transition, \( q \mapsto \bar{q} \), those \( F_1, \ldots, F_{l_1} \) hit the fired sets of colds, hot and nothing else. Intuition: betheunionofthefiredsetsof

\[
\begin{align*}
\psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) &= \psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) \\
\psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) &= \psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) \\
\psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) &= \psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right)
\end{align*}
\]

Progress with Conditions

\[
\begin{align*}
\psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) &= \psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) \\
\psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) &= \psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) \\
\psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) &= \psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right)
\end{align*}
\]

Progress with Conditions

\[
\begin{align*}
\psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) &= \psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) \\
\psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) &= \psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) \\
\psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right) &= \psi \bigcap \left( \bigcup_{i=1}^{n} F_i \right)
\end{align*}
\]

Progress with Conditions
Step II: Cold Conditions and Cold Local Invariants

\[ F := \psi \lor \neg q \lor (\neg q \lor (\neg q \land \text{consistent})) \]

\[ q \mapsto q' \text{ if and only if } \exists i \text{ such that } q \text{ is violated, or } q' \text{ is violated.} \]

\[ \forall q \in S_{\text{cons}}(\text{cold}) \text{ or } \forall q \in S_{\text{cons}}(\text{strict}) \text{, } \]
Finally: The LSC Semantics

A full LSC consists of

- a body \((I, (C^4, \preceq, \sim, /CB, Msg, Cond, LocInv))\),
- an activation condition (here: event) \(ac = E ? i_1, i_2, E \in /BX, i_1, i_2 \in I\),
- an activation mode, either initial or invariant,
- a chart mode, either existential (cold) or universal (hot).

A set \(W\) of words over \(/CB\) and \(/BW\) satisfies \(L\), denoted \(W \models L\), iff

- universal (hot), initial, and \(\forall w \in W \forall \beta: I \to \text{dom}(\sigma(w_0)) \cdot w\) activates \(L\) \(\Rightarrow w \in L\beta(BL)\),
- existential (cold), initial, and \(\exists w \in W \exists \beta: I \to \text{dom}(\sigma(w_0)) \cdot w\) activates \(L\) \(\land w \in L\beta(BL)\),
- universal (hot), invariant, and \(\forall w \in W \forall k \in \mathbb{N}_0 \forall \beta: I \to \text{dom}(\sigma(w_k)) \cdot w/k\) activates \(L\) \(\Rightarrow w/k \in L\beta(BL)\),
- existential (cold), invariant, and \(\exists w \in W \exists k \in \mathbb{N}_0 \exists \beta: I \to \text{dom}(\sigma(w_k)) \cdot w/k\) activates \(L\) \(\land w/k \in L\beta(BL)\).

References


