Pnueli & Shalev's declarative semantics

- Given a config C and set of env events E, a set of trans. T is separable for C and E if ∃ T'≠T s.t. T' ⊂ T and enabled(C,E,T')∩(T\T') = ∅
- T is admissable for C and E if T is inseparable (not sep.) for C and E and T = enabled(C,E,T), i.e., the declarative sem. is a fixed-point sem.
- Since enabled (C,E, .) may involve transitions with a negative trigger, it is in general non-monotonic, and a unique least fixed point may not exist.
- The notion of separability chooses distinguished fixed points that reflect causality
- A separable set of transitions points to a break in the causality chain when firing these transitions
- Thm 1 (Pnueli & Shalev). For all configs C and event sets E, a set T of trans. is admissable for C and E iff T is constructable for C and E

3.1 Configuration Syntax

This paper focuses on the semantics of single Statecharts steps, since the semantics across steps is clear and well understood. It will therefore be convenient to reduce the Statecharts notation to the bare essentials and identify a Statecharts configuration with its set of leaving transitions, to which we — by abuse of terminology — also refer as *configuration*. We formalise configurations using the following, simple syntax, where $I \subseteq \Pi \cup \overline{\Pi}$ and $A \subseteq \Pi$:

$$C \quad ::= \quad 0 \mid I/A \mid C \| C \,.$$

Intuitively, 0 stands for the configuration with the empty behaviour. Configuration I/A encodes a transition t with $\mathsf{trg}(t) = I$ and $\mathsf{act}(t) = A$. When triggered, transition t fires and generates the events in A. Transitions I/A with empty trigger, i.e., $I = \emptyset$, are simply written as A below. If we wish to emphasise that trigger I consists of the positive events $P \subseteq \Pi$ and the negative events $\overline{N} \subseteq \overline{\Pi}$, i.e., $I = P \cup \overline{N}$, then we denote transition I/A by $P, \overline{N}/A$. Finally, configuration $C_1 \| C_2$ describes the parallel composition of configurations C_1 and C_2. Observe that 0 coincides semantically with a transition with empty action; nevertheless, it seems natural to include 0. Using this syntax, we may encode the initial configuration C_1 of our example Statechart of Fig. 1 as

$$a/b \parallel b, \overline{c}, \overline{e_3}, \overline{e_4}/a, e_2 \parallel c, \overline{e_2}, \overline{e_4}/a, e_3 \parallel \overline{b}, \overline{e_2}, \overline{e_3}/c, e_4 \,.$$

- For simplicity, in this expo we focus on Statecharts w.r.t. the empty environment only
- This is no restriction, since considering a set E of events from env for a config C is equivalent to considering C//E relative to the empty set of events

New Perspective: Order-Theoretic Perspective

- Statecharts are viewed as process terms in process algebra, whose sem. is given by a compositional transl. into labelled trans. systs
- A transition represents a config. step decorated by an ACTION LABEL, specifying the synchr. causal interaction with the env.
- (Causality) labels are ordered (globally) consistent sets to encode causal info
- A causality label (or basic action) is a pair $(l, <)$ where
  - $l \subseteq \Pi \cup \Pi^{co}$ is a consistent set of pos. or neg. evnts, i.e., $l \cap l^{co} = \emptyset$
  - $A < B$ is an irreflexive and transitive causality ordering on subsets $A, B \subseteq l$, with $B = \emptyset$ or $B = \{b\}$ for $b \in \Pi$, where
  - irreflexivity means that $A < \{b\}$ implies $b \notin A$ and,
  - transitivity that if $A < \{b\}$ and $b \in C < D$ then $((C \setminus \{b\}) \cup A) < D$

- Causality labels represent globally consistent and causally closed interactions that are composed from Statechart transitions
- Every transition $t \in trans(C)$ leaving config C induces a causality label , where
  - $l_t =_{def} trg(t) \cup act(t)$
  - $<_t =_{def} \{trg(t) <_t \{e'\} : e' \in act(t)\}$
  - $trg(t) \cap act(t) = \emptyset$ and for no $e \in \Pi$ both $e, e^{co} \in trg(t) \cup act(t)$
- Then l_t is consistent, irreflexive and transitive

Ex. $a/b \mathbin{//} b,c^{co}/d$

- Thus, $t_1 =_{def} a/b$ and $t_2 =_{def} b,c^{co}/d$ correspond to labels $l_1=\{a,b\}$, $\{a\}<_1\{b\}$, and $l_2=\{b,c^{co},d\}$ with $\{b,c^{co}\}<_2 \{d\}$
- Their joint execution would be label $l_3=\{a,b,c^{co},d\}$ with causalities $\{a\} <_3 \{b\}$, $\{b,c^{co}\} <_3 \{d\}$ and $\{a,c^{co}\}<_3 \{d\}$
- Here, the last pair arises from the combined reaction of t_1 triggering t_2; its presence is enforced by transitivity of $<_3$
- Note that this ex. composes causality labels in parallel
- In general, the parallel composition of causality labels $\sigma_1=(l_1,<_1)$ and $\sigma_2=(l_2,<_2)$ is the set $\sigma_1 \times \sigma_2$ of all maximal, irreflexive and transitive suborderings of the transitive closure $(<_1 \cup <_2)^+$

Next we define the operation of parallel composition between causality labels $\sigma_1 = (\ell_1, \prec_1)$ and $\sigma_2 = (\ell_2, \prec_2)$ to form the full causal and concurrent closure of all interactions coded in two orderings. Due to nondeterminism, the composition $\sigma_1 \times \sigma_2$ does not yield a single causality label but rather a set of them. They are obtained as the maximal irreflexive and transitive sub-orderings of the transitive closure $(\prec_1 \cup \prec_2)^+$. Here, the transitive closure of $\prec_1 \cup \prec_2$ is the smallest relation $\prec$ with $\prec_1 \cup \prec_2 \subseteq \prec$ such that, if $A \prec \{b\}$ and $b \in B \prec C$, then $(B \setminus \{b\}) \cup A \prec C$. Now, $(\ell, \prec) \in \sigma_1 \times \sigma_2$ if (i) $\ell = \ell_1 \cup \ell_2$, (ii) $(\ell, \prec)$ is a causality label, and (iii) $\prec$ is maximal in $(\prec_1 \cup \prec_2)^+$.

Theorem 2 (Correctness & Completeness). *If C is a configuration and $A \subseteq \Pi$, then A is a Pnueli-Shalev step response of C if and only if there exists a causality label σ with $C \mapsto \sigma$ such that $\emptyset$ enables σ and $A = \mathsf{act}(\sigma)$.*

Compositional, Fully Abstract and Denotational Semantics

- The Pnueli & Shalev semantics lacks compositionality because an interaction with the environment is only allowed at the beginning of a step but NOT during a step
- Compositionality can only be achieved by exhausting the communication potential of a step
- This is done by regarding interaction steps, basically, sequences of monotonically increasing fixed-points of the enabledness function, extending until this potential is exhausted

Interaction steps

- Read a configuration C of a Statechart as a specification of a set of interaction steps between a Statechart and all its possible environments
- This set is nonempty since one may always construct an environment that disables those transitions is C that would cause global consistency and, thus, failure in the sense of Pnueli and Shalev
- An interaction step is a monotonically increasing sequence $M = (M_0, M_1, \ldots, M_n)$ of reactions $M_i \subseteq \prod$, where $M_{i-1} \subsetneq M_i$ for all i , and each reaction contains events representing both the environmental input and the Statecharts response.
- By the requirement for monotonicity, such a sequence extends the communication potential between the Statechart and its environment, until this potential is exhausted

Interaction steps (cont'd)

- An interaction step is best understood as a separation of a Pnueli-Shalev step response M_n in its n properly contained causally closed sub-fixed-points
- Each M_i extends M_{i-1} by new environmental stimuli plus the Statecharts response to these
- Here, responses are computed according to Pnueli and Shalev, except that events not contained in M_n are assumed to be absent in M_i
- Thus, global consistency is interpreted as a logical specification over the full interaction step M, and NOT only relative to a single reaction M_i

Interaction steps (cont'd)

- Thus, each interaction step separates a Pnueli-Shalev step response into causally-closed sets of events
- Each passage from M_{i-1} to M_i represents a non-causal "step" triggered by th environment
- This creates a separation between M_{i-1} and M_i in the spirit of P-S: as all events generated by the transitions enabled under M_{i-1} are contained in M_{i-1}, their intersection with $M_i \backslash M_{i-1}$ is empty

Interpreting configurations , logically

- Transitions $P,N^{co}/A$ of a config are interpreted on interaction steps $M = (M_0,\ldots,M_n)$ as follows: For each M_i, either
- (1) all events in A are also in M_i (the transition is enabled and thus fires), or
- (2) one or more events in A are not in M_i and $P \not\subseteq M_i$ (not all positive trigger events are present, disabling the transition), or
- (3) one or more events in A are not in M_i, and some event $e \in N$ is in M_j for some $i \leq j \leq n$ (global consistency is enforced over the whole interaction step M, disabling the transition)