III A COMPOSITIONAL SEMANTICS FOR NESTED SYNCHRONOUS TRANSITION DIAGRAMS

7.4 A Compositional Proof Method for Nested Parallelism

In this section we extend the compositional proof method of Section 7.3 and show how one can reason compositionally about systems which are constructed from sequential synchronous transition diagrams by means of sequential and parallel composition. Such *composite* systems give rise to *nested parallelism* and play a dominant rôle in more advanced chapters such as Chapter 12 on layered design. Formally, we have the following definition of composite systems.

Definition 7.14 We assume as given a set $\mathcal{B}$, with typical element B, of *basic systems*, that is, sequential synchronous transition diagrams. We define the set of *composite systems*, with typical element P, inductively as follows:

$$P ::= B \mid P_1;P_2 \mid P_1 \| P_2. \qquad \square$$

Compositional Semantics for Synchronous Message Passing

Let $P = (L, T, s, t)$ be a sequential synchronous transition diagram. We describe its semantics as a labelled transition relation.

- $\langle l;\sigma\rangle \xrightarrow{\langle\rangle} \langle l';f(\sigma)\rangle$ if $l \xrightarrow{b\to f} l' \in T$ and $\sigma \models b$.
- $\langle l;\sigma\rangle \xrightarrow{\langle(C,e(\sigma))\rangle} \langle l';f(\sigma)\rangle$ if $l \xrightarrow{b;C!e\to f} l' \in T$ and $\sigma \models b$.
- $\langle l;\sigma\rangle \xrightarrow{\langle(C,v)\rangle} \langle l';f(\sigma : x \mapsto v)\rangle$ if $l \xrightarrow{b;C?x\to f} l' \in T$ and $\sigma \models b$. Note that v is an arbitrary value!

Compositional Semantics . . . cont'd

Rules for completing the reflexive, transitive closure of the transition relation generated by $\xrightarrow{\langle\rangle}$ and $\xrightarrow{\langle(C,v)\rangle}$:

$$\langle l;\sigma\rangle \xrightarrow{\langle\rangle} \langle l;\sigma\rangle$$

$$\frac{\langle l;\sigma\rangle \xrightarrow{\theta} \langle l';\sigma'\rangle \quad \langle l';\sigma'\rangle \xrightarrow{\theta'} \langle l'';\sigma''\rangle}{\langle l;\sigma\rangle \xrightarrow{\theta\cdot\theta'} \langle l'';\sigma''\rangle}$$

Define

$$\mathcal{O}_l(P) = \left\{ (\sigma,\sigma',\theta) \;\middle|\; \langle s;\sigma\rangle \xrightarrow{\theta} \langle l;\sigma'\rangle \right\}$$

So the initial/final state semantics of P is $\mathcal{O}_t(P)$.

Definition 4.14 Let P be a sequential synchronous transition diagram, and l occur in P. We define

$$O_l(P) \overset{\text{def}}{=} \{(\sigma,\sigma',\theta) \mid \langle s;\sigma\rangle \xrightarrow{\theta} \langle l;\sigma'\rangle\}.$$

Note that we can now define the initial-final state semantics of P as $O_t(P)$, also simply expressed as $O(P)$. $\square$

For a sequence of communications θ and a set of channels $cset \in CHAN$, we define the *projection* of θ onto $cset$, expressed by $\theta{\downarrow}cset$, as the sequence obtained from θ by deleting all records with channels not in $cset$.

Definition 4.15 (Projection of a sequence of communications to a set of channels) One can define $\theta{\downarrow}cset$, the projection of θ onto a set of channels $cset$, by induction on the length of θ:

$$\langle\rangle{\downarrow}cset \overset{\text{def}}{=} \langle\rangle,$$

$$(\langle(C,\mu)\rangle\cdot\theta'){\downarrow}cset \overset{\text{def}}{=} \begin{cases} \langle(C,\mu)\rangle\cdot\theta'{\downarrow}cset, & \text{if } C \in cset, \\ \theta'{\downarrow}cset, & \text{otherwise.} \end{cases}$$

$\square$

Also we need to define the set of channels occurring in a trace θ.

Definition 4.16 (Channels occurring in a trace) The set of channels occurring in a sequence of communications, or *trace* θ, notation $Chan(\theta)$, is defined by

- $Chan(\langle\rangle) \overset{\text{def}}{=} \emptyset$
- $Chan(\theta\cdot(C,\mu)) \overset{\text{def}}{=} Chan(\theta)\cup\{C\}$. $\square$

Definition 7.15 The semantics $O(B)$ of a basic synchronous transition diagram $B \equiv (L, T, s, t)$ is simply defined as $O_t(B)$.

For $P \equiv P_1 ; P_2$ we define

$$O(P) \overset{\text{def}}{=} \{(\sigma, \sigma', \theta) \mid \text{There exist } \sigma_1, \theta_1, \theta_2 \text{ such that } (\sigma, \sigma_1, \theta_1) \in O(P_1), (\sigma_1, \sigma', \theta_2) \in O(P_2) \text{ and } \theta = \theta_1 \cdot \theta_2\}.$$

For $P \equiv P_1 \parallel P_2$ we define

$$O(P) \overset{\text{def}}{=} \{(\sigma, \sigma', \theta) \mid i = 1, 2,\ (\sigma, \sigma'_i, \theta{\downarrow}P_i) \in O(P_i) \wedge \theta = \theta{\downarrow}Chan(P_1 \| P_2),$$

$$\text{where } \sigma'(x) \overset{\text{def}}{=} \begin{cases} \sigma'_1(x), & \text{if } x \in var(P_1), \\ \sigma'_2(x), & \text{if } x \in var(P_2), \\ \sigma(x), & \text{otherwise}\}. \end{cases}$$

$\square$

Remark 7.16 For a composite system we have that $\sigma(x) = \sigma'(x)$ for all $x \notin var(P)$ and $(\sigma, \sigma', \theta) \in O(P)$.