FORMAL METHODS FOR SYSTEM VERIFICATION

Structured Operational Semantics

Sabina Rossi

DAIS
Università Ca' Foscari
Venezia

Passive activities

Description

- A component may be passive with respect to an action type.
- This means that all activities of that type enabled by the component will have the unspecified activity rate $\top$.
- These activities must be shared with another component, the other component determining the rate of this shared activity.
- A model is said to be incomple if it has a component which is passive with respect to an individual action type.

Passive activities

Probabilities of passive activities

- If more than one activity of a given passive type can be simultaneously enabled by a component, each unspecified activity rate must also be assigned a weight.
- Weights are natural numbers used to determine the relative probabilities of the possible outcomes of the activities of that action type.

Passive activities

Example

- Consider a component which is passive with respect to action type α.
- Suppose that when α is completed, the component may:
  - behave as P with probability $\frac{w_1}{w_1+w_2}$, or
  - behave as Q with probability $\frac{w_2}{w_1+w_2}$.
- Then the component will be represented as:

$$(\alpha, w_1\top).P + (\alpha, w_2\top).Q$$

If no weights are assigned we assume that multiple instances have equal probabilities of occurring.

Comparing unspecified activity rates

- The following inequalities and equations define the comparison and manipulation of unspecified activity rates:

$$
\begin{array}{rcll}
r & < & w\top & \text{for all } r \in \mathbb{R}^+ \text{ and for all } w \in \mathbb{N} \\
w_1\top & < & w_2\top & \text{if } w_1 < w_2 \text{ for all } w_1, w_2 \in \mathbb{N} \\
w_1\top + w_2\top & = & (w_1 + w_2)\top & \text{for all } w_1, w_2 \in \mathbb{N} \\
\frac{w_1\top}{w_2\top} & = & \frac{w_1}{w_2} & \text{for all } w_1, w_2 \in \mathbb{N}
\end{array}
$$

Apparent rate

Intuition

- There are situations in which it is convinient to represent a single action of the system by more than one activity in the model.
- To an external observer of the system the apparent rate of activities of that type will be the same.
- The race condition ensures that the rate at which an activity α is done is the sum of the rates of all the enabled type α activities.

Apparent rate

Definition

- The apparent rate of action of type α in a component P, denoted $r_\alpha(P)$, is the sum of the rates of all activities of type α enabled in P.

$$r_\alpha((\beta, r).P) = \begin{cases} r & \text{if } \beta = \alpha \\ 0 & \text{if } \beta \neq \alpha \end{cases}$$

$$r_\alpha(P + Q) = r_\alpha(P) + r_\alpha(Q)$$

$$r_\alpha(P/L) = \begin{cases} r_\alpha(P) & \text{if } \alpha \notin L \\ 0 & \text{if } \alpha \in L \end{cases}$$

$$r_\alpha(P \underset{L}{\bowtie} Q) = \begin{cases} min(r_\alpha(P), r_\alpha(Q)) & \text{if } \alpha \in L \\ r_\alpha(P) + r_\alpha(Q) & \text{if } \alpha \notin L \end{cases}$$

Apparent rate

Unspecified apparent rate

- The apparent rate of an action type α may be unspecified.
- If P is defined as:

$$P \stackrel{\text{def}}{=} (\alpha, w_1\top).P_1 + (\alpha, w_2\top).P_2$$

then the apparent rate of α in P is:

$$r_\alpha(P) = (w_1 + w_2)\top\,.$$

Current action types

Definition

- The set of current action types enabled by a component P, denoted by $\mathcal{A}(P)$, is defined as follows:

$$
\begin{aligned}
\mathcal{A}((\alpha, r).P) &= \{\alpha\} \\
\mathcal{A}(P + Q) &= \mathcal{A}(P) \cup \mathcal{A}(Q) \\
\mathcal{A}(P/L) &= \begin{cases} \mathcal{A}(P) & \text{if } \mathcal{A}(P) \cap L = \emptyset \\ (\mathcal{A}(P) \setminus L) \cup \{\tau\} & \text{if } \mathcal{A}(P) \cap L \neq \emptyset \end{cases} \\
\mathcal{A}(P \underset{L}{\bowtie} Q) &= (\mathcal{A}(P) \setminus L) \cup (\mathcal{A}(Q) \setminus L) \cup (\mathcal{A}(P) \cap \mathcal{A}(Q) \cap L)
\end{aligned}
$$

Current activities

Definition

- The multiset of current activities of a component P, denoted by $\mathcal{A}ct(P)$, is defined as follows.
- First we adopt the following abbreviations:

$$\begin{aligned} \mathcal{A}ct_{\setminus L}(P) &= \{\!|(\beta, r) \in \mathcal{A}ct(P) |\ \beta \notin L|\!\} \\ \mathcal{A}ct_{\cap L}(P) &= \{\!|(\beta, r) \in \mathcal{A}ct(P) |\ \beta \in L|\!\} \end{aligned}$$

Definition

$$
\begin{aligned}
\mathcal{A}ct((\alpha, r).P) &= \{\!|(\alpha, r)|\!\} \\
\mathcal{A}ct(P + Q) &= \mathcal{A}ct(P) \uplus \mathcal{A}ct(Q) \\
\mathcal{A}ct(P/L) &= \mathcal{A}ct_{\setminus L}(P) \uplus \{\!|(\tau, r)|\ (\alpha, r) \in \mathcal{A}ct_{\cap L}(P)|\!\} \\
\mathcal{A}ct(P \underset{L}{\bowtie} Q) &= \mathcal{A}ct_{\setminus L}(P) \uplus \mathcal{A}ct_{\setminus L}(Q) \uplus \{\!|(\alpha, r)|\ \alpha \in L, \\
&\quad \exists (\alpha, r_1) \in \mathcal{A}ct_{\cap L}(P), \exists (\alpha, r_2) \in \mathcal{A}ct_{\cap L}(Q), \\
&\quad r = \frac{r_1}{r_\alpha(P)} \frac{r_2}{r_\alpha(Q)} min(r_\alpha(P), r_\alpha(Q))|\!\}
\end{aligned}
$$

Dynamic behaviour

Definition

- The behaviour of a model is dictated by the semantic rules governing the combinators of the language.
- The possible evolutions of a model are captured by applying these rules exhaustively, generating a labelled transition system.
- This can be viewed as a graph in which each node is a state of the model (comprised of the local states of each of the components) and the arcs represent the actions which can cause the move from one state to another.

Process algebra model $\xrightarrow{\text{SOS rules}}$ Labelled multi-transition system

Structured Operational Semantics

Definition

- PEPA is defined using a Plotkin-style structured operational rules (a "small step" semantics).
- Time is not represented explicitly in the rules but it is assumed that an activity takes some time to complete and consequently each transition represents some advance of time.
- The operational rules are to be read as follows:

  if the transitions above the inference line can be inferred, then we can infer the transition below the line.

Prefix, Constant, Choice and Hiding

Prefix $$\frac{}{(\alpha, r).P \xrightarrow{(\alpha,r)} P}$$

Constant $$\frac{P \xrightarrow{(\alpha,r)} P'}{A \xrightarrow{(\alpha,r)} P'} \; (A \stackrel{\text{def}}{=} P)$$

Choice $$\frac{P \xrightarrow{(\alpha,r)} P'}{P + Q \xrightarrow{(\alpha,r)} P'} \qquad \frac{Q \xrightarrow{(\alpha,r)} Q'}{P + Q \xrightarrow{(\alpha,r)} Q'}$$

Hiding $$\frac{P \xrightarrow{(\alpha,r)} P'}{P/L \xrightarrow{(\alpha,r)} P'/L} \; (\alpha \notin L) \qquad \frac{P \xrightarrow{(\alpha,r)} P'}{P/L \xrightarrow{(\tau,r)} P'/L} \; (\alpha \in L)$$

Cooperation

(Cooperation) $(\alpha \notin L)$

$$\frac{P \xrightarrow{(\alpha,r)} P'}{P \underset{L}{\bowtie} Q \xrightarrow{(\alpha,r)} P' \underset{L}{\bowtie} Q} \ (\alpha \notin L) \qquad \frac{Q \xrightarrow{(\alpha,r)} Q'}{P \underset{L}{\bowtie} Q \xrightarrow{(\alpha,r)} P \underset{L}{\bowtie} Q'} \ (\alpha \notin L)$$

(Cooperation) $(\alpha \in L)$

$$\frac{P \xrightarrow{(\alpha,r_1)} P' \quad Q \xrightarrow{(\alpha,r_2)} Q'}{P \underset{L}{\bowtie} Q \xrightarrow{(\alpha,r)} P' \underset{L}{\bowtie} Q'} \ (\alpha \in L)$$

where $\quad r = \dfrac{r_1}{r_\alpha(P)} \dfrac{r_2}{r_\alpha(Q)} \min(r_\alpha(P), r_\alpha(Q))$

Cooperation and shared activities

- The apparent rate of a shared action type in the component $P \underset{L}{\bowtie} Q$, i.e., $\alpha \in L$, is taken to be the slower of the apparent rates of that action type in P and Q.
- It is assumed that in general both components of a cooperation will need to complete some work for the shared activity to be completed.
- In the case where the apparent rate is unspecified in one component the apparent rate will be completely determined by the other component.

Cooperation and shared activities

- We assume independence between the choice of outcome made by each of the cooperating components and choose the rate of each shared activity to maintain the same probability of outcome on each of the components.
- Example: consider $P \underset{L}{\bowtie} Q$.
  - Let $(\alpha, r_1) \in \mathcal{A}ct(P)$, i.e., α occurs in P with probability $\frac{r_1}{r_{\alpha(P)}}$.
  - Let $(\alpha, r_2) \in \mathcal{A}ct(Q)$, i.e., α occurs in Q with probability $\frac{r_2}{r_{\alpha(Q)}}$.
  - Assuming independence of choice in P and Q, the probability of $(\alpha, r) \in \mathcal{A}ct(P \underset{L}{\bowtie} Q)$ is

$$\frac{r_1}{r_{\alpha(P)}} \times \frac{r_2}{r_{\alpha(Q)}}.$$

Cooperation and shared activities

- PEPA assumes bounded capacity: that is, a component cannot be made to perform an activity faster by cooperation, so the rate of a shared activity is the minimum of the apparent rates of the activity in the cooperating components.
- The apparent rate of a component P with respect to action type α is the total capacity of component P to carry out activities of type α, denoted $r_\alpha(P)$.
- When enabled an activity, $a = (\alpha, \lambda)$, will delay for a period determined by its associated distribution function, i.e., the probability that the activity a happens within a period of time of length t is $F_a(t) = 1 - e^{-\lambda t}$.

Multi-way cooperation

- Cooperation in PEPA is multi-way. Two, three, four or more partners may cooperate, and they all need to synchronise for the activity to happen.
- For example the system

$$((\alpha, r).P \underset{\alpha}{\bowtie} (\alpha, s).Q) \underset{\alpha}{\bowtie} (\alpha, t).R$$

will have a three-way synchronization between P, Q and R on the activity of type α.

Multi-way cooperation

- The cooperation sets can make a big difference in the behaviour.
- Example 1:

$$((\alpha, r).P \| (\alpha, s).Q) \underset{\alpha}{\bowtie} (\alpha, t).R$$

will have P and Q competing to cooperate with R giving rise to two possible α type activities, only one of which can proceed.

- Example 2:

$$((\alpha, r).P \underset{\alpha}{\bowtie} (\alpha, s).Q) \| (\alpha, t).R$$

will have two α type activities: one synchronising P and Q and one in R alone, both of which can proceed.

Labelled Multi-Transition System

Definition

- A labelled transition system is a triple

$$(S, T, \{\xrightarrow{t} \mid t \in T\})$$

where

  - S is a set of states
  - T is a set of transition labels
  - $\xrightarrow{t} \subseteq S \times S$ is a transition relation for each $t \in T$.

- A labelled multi-transition system is a triple as above where $\xrightarrow{t}$ is a multi-relation in which the number of instances of a relation between states is recognized.

Labelled Multi-Transition System

Definition

- PEPA may be regarded as a labelled multi-transition system

$$(\mathcal{C}, \mathcal{A}ct, \{\xrightarrow{(\alpha,r)} \mid (\alpha, r) \in \mathcal{A}ct\})$$

where

- $\mathcal{C}$ is the set of all components
- $\mathcal{A}ct$ is the set of all activities
- $\xrightarrow{(\alpha,r)} \subseteq \mathcal{C} \times \mathcal{C}$ is the multi-transition relation given by the rules of PEPA operational semantics.

Derivatives of a PEPA component P

Definition

- If $P \xrightarrow{(\alpha,r)} P'$ then P' is called a one-step derivative of P.
- More generally, if $P \xrightarrow{(\alpha_1,r_1)} \ldots \xrightarrow{(\alpha_n,r_n)} P'$ then P' is called a derivative of P.
- The derivative set of a PEPA component P, denoted $ds(P)$, is defined as the smallest set of components such that:
  - if $P \stackrel{\text{def}}{=} P_0$ then $P_0 \in ds(P)$,
  - if $P_i \in ds(P)$ and there exists $a \in \mathcal{A}ct(P_i)$ such that $P_i \xrightarrow{a} P_j$ then $P_j \in ds(P)$.

Derivatives of a PEPA component P

Definition

- The derivative set of a component P is the set of all PEPA components representing all the reachable states of the system modeled by P.
- The derivatives of P are the states of the labelled multi-transition system (or derivation graph) of P.

Derivation graph for a component P

Definition

- Given a PEPA component P and its derivative set $ds(P)$, the derivation graph of P, denoted $\mathcal{D}(P)$, is the labelled directed multigraph whose set of nodes is $ds(P)$ and whose multiset of arcs A is defined by:
  - The elements of A are taken from the set $ds(P) \times ds(P) \times \mathcal{A}ct$
  - $\langle P_i, P_j, a \rangle$ occurs in A with the same multiplicity as the number of distinct inference trees which infer $P_i \xrightarrow{a} P_j$.
- The initial component P_0, where $P \stackrel{\text{def}}{=} P_0$, is taken to be the initial node of the graph.

Complete set of action types

Definition

- The complete set of action types of a component P, denoted by $\vec{\mathcal{A}}(P)$ is the set of action types which are used within the derivation graph of a system and is defined as:

$$\vec{\mathcal{A}}(P) = \bigcup_{P_i \in ds(P)} \mathcal{A}(P_i)\,.$$