FORMAL METHODS FOR SYSTEM VERIFICATION

Syntax of PEPA

Sabina Rossi

DAIS
Università Ca' Foscari
Venezia

Introduction and Motivation

- It is based on formalisms originally developed to model concurrency.
- It falls within the broad class of discrete event modelling formalisms and incorporate timing and probabilistic information with the events in the system.
- It has a formal semantics which can be used to automatically derive an underlying Markov process (when durations are assumed to be exponentially distributed).
- It provides a compositional modelling formalism.

Advantages of compositionality

For model construction:

- when a system consists of interacting components, the components, and the interactions, can each be modelled separately;
- models have a clear structure and are easy to understand;
- models can be constructed systematically, by either elaboration or refinement;
- the possibility of maintaining a library of model components, supporting model reusability, is introduced.

Performance Evaluation Process Algebra: PEPA

PEPA is based on:

- components that are active units within a system;
- activities that capture the actions of those units;
- cooperation that expresses the interaction between components.

Activities

- Models are constructed from components which engage in activities.
- Every activity in PEPA has an associated duration which is a random variable with an exponential distribution.

Activities

- Each activity has an action type (or simply type or name) and an activity rate.
- Each activity has the form

$$(\alpha, r)$$

where

  - α is the action type of the activity
  - r is the activity rate.

- Each system action is uniquely typed and there is a countable set $\mathcal{A}$ of all possible such types.
- Activities with the same action type represent different instances of the same action by the system.

Action type τ

- There is a special action type, denoted τ and named unknown type:
  - it represents an unknown or unimportant system action.
- Activities with unknown type will be private to the component in which they occur.

Duration of an activity

- Each activity (also those with action type τ) has an associated duration.
- The duration of an activity is an exponentially distributed random variable.
- Since an exponential distribution is uniquely determined by its parameter, the duration of an activity is represented by a single real number parameter.
- This parameter is called the activity rate (or simply rate) of the activity: it may be
  - any positive real number,
  - or the distinguished symbol $\top$ which should be read as unspecified.

Some notations

- $\mathcal{A}$: set of all actions types, including τ
- $\mathcal{R}^+$: set of all positive real numbers, including $\top$
- $\mathcal{A}ct = \mathcal{A} \times \mathcal{R}^+$: set of all activities

Hence, an activity is represented as:

$$a = (\alpha, r)$$

where

- $a \in \mathcal{A}ct = \mathcal{A} \times \mathcal{R}^+$ denotes the activity
- $\alpha \in \mathcal{A}$ is the action type
- $r \in \mathcal{R}^+$ is the activity rate.

Duration of an activity

- When enabled an activity $a = (\alpha, r)$ will delay for a period determined by its associated distribution function.
- The probability that the activity $a = (\alpha, r)$ happens within a period of time of length t is

$$F_a(t) = 1 - e^{-r\,t}.$$

Syntax of PEPA

- Components are denoted by: $P, C, C_i, C_j, S, System, \ldots$
- Activities are denoted by: $a, b, c, \ldots$
- Action types are denoted by: $\alpha, \beta, \gamma, \ldots$ or names like *task*, *request*, *use*, ...
- Activity rates are denoted by: $r, s, t, r_i, s_i \ldots$ sometimes we use the greek letters μ and λ

Syntax of PEPA

- The combinators of the language allow expressions, or terms, to be constructed defining the behaviour of components via the activities they undertake and the interactions between them.
- The syntax for terms in PEPA is defiend as follows:
  - sequential components:

$$S ::= (\alpha, r).S \mid S_1 + S_2 \mid A$$

  - cooperating components:

$$C ::= C_1 \underset{L}{\bowtie} C_2 \mid C/L \mid S$$

Informal semantics

Prefix $(\alpha, r).S$

- The component $(\alpha, r).S$ carries out activity (α, r) which has action type α and a duration which is exponentially distributed with parameter r (mean $1/r$).
- The time taken for the activity to complete will be some Δt, drawn from the distribution.
- The component subsequently behaves as component S.
- If the system is in the state $(\alpha, r).S$ at some time t, the time at which it completes (α, r) and becomes S will be $t + \Delta t$.

Informal semantics

Prefix $(\alpha, r).S$

- When $a = (\alpha, r)$ the component $(\alpha, r).S$ may be written as $a.S$
- We write

$$(\alpha, r).S \xrightarrow{(\alpha,r)} S \qquad\qquad a.S \xrightarrow{a} S$$

to denote the completion of activity (α, r) (resp. a) and the subsequent behaviour of the system as component S.

Timing behaviour and uncertainty

- A delay is thus inherent in each activity in the model and the timing behaviour of the system is captured.
- Moreover, since the duration is a random variable, temporal uncertainty, the uncertainty of how long an action will take, is represented.
- It is like each activity sets a timer whenever it becomes enabled.

Competing activities

- If several activities are enabled at some time then each will have its own associated timer.
- When the first timer finishes that activity takes place and it is said to complete or succeed.
- An activity is said to be preempted or aborted if another one complete first.

Implicit resource

- It is assumed that there is always an implicit resource.
- Thus the time elapsed before activity completion represents the use of this resource by the component.
- For example, this resource might be:
  - bandwidth on a communication channel
  - processor time or CPU cycles within a processor.

Informal semantics

Choice $S_1 + S_2$

- The component $S_1 + S_2$ represents a system which may behave either as component S_1 or as component S_2.
- $S_1 + S_2$ enables all the current activities of S_1 and all the current activities of S_2.
- The first activity to complete distinguishes one of the components S_1 or S_2. The other component of the choice is discarded.

Informal semantics

Choice $S_1 + S_2$

- Suppose that

$$S_1 = (\alpha, r).S_1' \qquad S_2 = (\beta, s).S_2'.$$

- At the time t_0 the enabled activities of $S_1 + S_2$ are both (α, r) and (β, s).
- Let Δ_α and Δ_β drawn from the exponential distributions of α and β, respectively. For $x \in \{\alpha, \beta\}$:
  - Δ_x represents the time taken for the activity x.
  - $F_x(t)$ is the probability that $\Delta_x \leq t$.
- If $\Delta_\alpha < \Delta_\beta$ then activity (α, r) is enabled and at the time $t_0 + \Delta_\alpha$ the system behaves as S_1'.

Informal semantics

Choice $S_1 + S_2$

- Notice that the probability that $\Delta_\alpha = \Delta_\beta$ is 0.
- Indeed, the continuous nature of the probability distributions ensures that the probability that S_1 and S_2 both completing an activity at the same time is 0, i.e., $\Delta_\alpha \neq \Delta_\beta$.

Informal semantics

Choice $S_1 + S_2$

- Notice that there is an underlying assumption that S_1 and S_2 are competing for the same implicit resource.
- Thus the choice combinator $+$ represents the competition between components.

Informal semantics

Cooperation $C_1 \underset{L}{\bowtie} C_2$

- This is in fact an indexed family of combinators, one for each possible set of action types $L \subseteq \mathcal{A}$.
- L is named cooperation set and defines the action types on which the components must synchronize or cooperate.

Informal semantics

Cooperation $C_1 \underset{L}{\bowtie} C_2$

- In contrast to choice, it is assumed that each component in a cooperation has its own implicit resource and that they proceed independently with any activities whose types do not occur in the cooperation set.
- Activities with action types in L require the simultaneous involvement of both components (both resources) in an activity of that type.
- The unknown action type τ, may not appear in any cooperation set, i.e., $\tau \notin L$.

Informal semantics

Cooperation $C_1 \underset{L}{\bowtie} C_2$

We distinguish:

Individual activities : activities of C_1 and C_2 whose action types do not occur in L. They proceed unaffected.

Shared activities : activities of C_1 and C_2 whose action types do occur in L. They will only be enabled in $C_1 \underset{L}{\bowtie} C_2$ when they are enabled in both C_1 and C_2.

- Shared activities need to work together to achieve an action.
- Thus one component may become blocked, waiting for the other component to be ready to partecipate.

Informal semantics

Cooperation $C_1 \underset{L}{\bowtie} C_2$

Example:

$$C_1 = (\alpha, r).(\beta, s).C_1' \qquad C_2 = (\beta, t).C_2'$$

$$C_1 \underset{L}{\bowtie} C_2$$

where $L = \{\beta\}$.

- (α, r) is an individual activity.
- (β, s) and (β, t) are shared activities.
- C_2 is blocked, waiting for C_1 to be ready to partecipate.
- Action type β is enabled only when it is enabled in C_1 and C_2.

Informal semantics

Cooperation $C_1 \underset{L}{\bowtie} C_2$

- When two shared activities cooperate then a new shared activity is formed by the cooperation. This activity will have the same action type as the two contributing activities and a rate reflecting the rate of the slower participant.
- The expected duration of a shared activity will be greater than or equal to the expected durations of the corresponding activities in the cooperating components.

Informal semantics

Cooperation $C_1 \underset{L}{\bowtie} C_2$

Example:

$$(\alpha, r).C_1 \underset{\{\alpha\}}{\bowtie} (\alpha, s).C_2 \xrightarrow{(\alpha,t)} C_1 \underset{\{\alpha\}}{\bowtie} C_2$$

- t represents the expected duration of the shared activity α.
- How can we determine t?

Informal semantics

Cooperation $C_1 \underset{L}{\bowtie} C_2$

- If an activity has an unspecified rate in a component, then the component is said to be passive with respect to that action type, and it does not contribute to the work involved.

  Example:

$$(\alpha, r).C_1 \underset{\{\alpha\}}{\bowtie} (\alpha, \top).C_2 \xrightarrow{(\alpha, r)} C_1 \underset{\{\alpha\}}{\bowtie} C_2$$

- Component $(\alpha, \top).C_2$ is passive w.r.t. α.
- An example might be the role of a channel in a message passing system: the cooperation of the channel is essential if a transfer is to take place but the transfer involves no work (consumption of implicit resource) on the part of the channel. This may be regarded as one component coopting another.

Informal semantics

Cooperation $C_1 \underset{L}{\bowtie} C_2$

- When $L = \emptyset$ is empty then $\underset{L}{\bowtie}$ has the effect of parallel composition, allowing components to proceed concurrently without any interaction between them.
- We use the notation $C_1 \| C_2$ to represent $C_1 \underset{\emptyset}{\bowtie} C_2$ where $\|$ is the parallel combinator.

Informal semantics

Example: Parallel composition

- Consider the system $P \| S$ where

$$P = (\alpha, r_1).Q \quad Q = (\beta, r_2).R_1 + (\gamma, r_3).R_2 \quad S = (\delta, r_4).S$$

- Let t_0 be the initial time, $\mathcal{A}ct(P \| S) = \{\alpha, \delta\}$ and $x \in \{\alpha, \delta\}$.
  - Δ_x represents the time taken for the activity x to complete.
  - $F_x(t)$ is the probability that $\Delta_x \leq t$.
- Suppose that $\Delta_\alpha < \Delta_\delta$. Then the activity (α, r_1) is enabled and at the time $t_0 + \Delta_\alpha$ the system behaves ad $Q \| S$.
- Now $\mathcal{A}ct(Q \| S) = \{\beta, \gamma, \delta\}$. Consider Δ_β, Δ_γ, Δ'_δ (which may be different from Δ_δ). Suppose that $\Delta'_\delta < \Delta_\beta$ and $\Delta'_\delta < \Delta_\gamma$ then at the time $t_0 + \Delta_\alpha + \Delta'_\delta$ the system behaves as $Q \| S$.

Informal semantics

Hiding C/L

- C/L behaves as C except that any activities of type within the set L are hidden and they appear as the unknown type τ.
- τ can be regarded as an internal delay by the component.
- Example: let $C = (\alpha, r).C'$ then

$$((\alpha, r).C')/\{\alpha\} \xrightarrow{(\tau,r)} C'/\{\alpha\}$$

Informal semantics

Hiding C/L

- Normally, when an activity is completed an external observer can see the type of the completed activity. The observer is also aware of the delay while the activity takes place.
- A hidden activity is witnessed only by its delay and the unknown type τ:
  - The action type of a hidden activity is no longer externally accessible to an observer or to another component.
  - The duration of an activity is unaffected if it is hidden.
- Moreover such an activity cannot be carried out in cooperation with any other component.

Informal semantics

Constant $A \stackrel{\text{def}}{=} C$

- We assume that there is a countable set of constants.
- Constants are components whose meaning is given by a defining equation such as $A \stackrel{\text{def}}{=} C$.
- If $A \stackrel{\text{def}}{=} C$ then A denotes a components behaving as C.

Notations

- Suppose that E is a component expression which contains a variable X.
- $E\{P/X\}$ denotes the component formed when every occurrence of X in E is replaced by the component P.
- More generally, an indexed set of variables $\tilde{X}$ may be replaced by an indexed set of components $\tilde{P}$, as in $E\{\tilde{P}/\tilde{X}\}$.

Precedence of PEPA operators

- Hiding has highest precedence with prefix next, followed by cooperation. Choice has the lowest precedence.
  1. P/L
  2. $(\alpha, r).P$
  3. $P \underset{L}{\bowtie} Q$
  4. $P + Q$
- We can use brackets to clarify the meaning of a combination of components.

Precedence of PEPA operators: Example

- The component $P \underset{L_1}{\bowtie} Q \underset{L_2}{\bowtie} R$ may be interpreted as

$$(P \underset{L_1}{\bowtie} Q) \underset{L_2}{\bowtie} R \quad \text{or} \quad P \underset{L_1}{\bowtie} (Q \underset{L_2}{\bowtie} R).$$

- When brackets are missing we assume that the cooperation associates to the left, i.e., the above component behaves as $(P \underset{L_1}{\bowtie} Q) \underset{L_2}{\bowtie} R$.

Precedence of PEPA operators: Example

- The cooperation between several different components may be ragarded as being built up in layers or levels, each cooperation combining just two components.
- For example, the component:

$$((P_1 \underset{L}{\bowtie} P_2) \underset{M}{\bowtie} P_3) \underset{K}{\bowtie} (P_4 \underset{N}{\bowtie} P_5)$$

  can be regarded at the top level as $Q_1 \underset{K}{\bowtie} Q_2$ where:
  - $Q_1 \stackrel{\text{def}}{=} Q_3 \underset{M}{\bowtie} P_3$
  - $Q_2 \stackrel{\text{def}}{=} P_4 \underset{N}{\bowtie} P_5$
  - $Q_3 \stackrel{\text{def}}{=} P_1 \underset{L}{\bowtie} P_2$
- Components at the lowest level, which do not contain a cooperation are referred to as atomic, while those at the top level are referred to as top-level components.

Race condition

- A race condition governs the dynamic behaviour of a model whenever more than one activity is enabled: when many activities attempt to proceed only the fastest succeed.
- Of course which activity is fastest on successive computations will vary due to the nature of the random variables determining the duration of activities.
- The probability that a particular activity completes will be given by the ratio of the activity rate of that activity to the sum of the activity rates of all the enabled activities.
- We may represent a single action in a system by more than one activity in the corresponding PEPA model, if the action has more than one possible outcome.

Probabilities of the different outcomes of an action

- Consider a componet engaging in an action of type α with activity rate r.
- Suppose that such an action may have two different possible outcomes.
- Then this single action would be represented by two separate activities.
- The activity rates of these activities would be adjusted to capture the probabilities of the different outcomes.

Example

- Suppose that our system performs the action α at rate r and then, with probability $\frac{1}{3}$, behaves as component P and, with probability $\frac{2}{3}$, behaves as component Q.
- This system will be represented by a PEPA component as

$$(\alpha, \frac{r}{3}).P + (\alpha, \frac{2r}{3}).Q$$

- The probability of the first activity is:

$$\frac{\frac{r}{3}}{(\frac{r}{3} + \frac{2r}{3})} = \frac{\frac{r}{3}}{r} = \frac{r}{3} \cdot \frac{1}{r} = \frac{1}{3}$$

- The probability of the second activity is:

$$\frac{\frac{2r}{3}}{(\frac{r}{3} + \frac{2r}{3})} = \frac{\frac{2r}{3}}{r} = \frac{2r}{3} \cdot \frac{1}{r} = \frac{2}{3}$$