FORMAL METHODS FOR SYSTEM VERIFICATION

The Stochastic Model underlying a PEPA component

Sabina Rossi

DAIS
Università Ca' Foscari
Venezia

The stochastic process underlying a PEPA component

Generating the Markov Process

- The derivation graph of a PEPA model may be used to generate a Continuous Time Markov Chain.
- To form the stochastic process:
  - a state is associated to each node of the graph,
  - there is a transition between two states if there is an arc in the graph between the corresponding nodes,
  - the transition rate between two states is the sum of the activity rates labelling arcs connecting the corresponding nodes in the derivation graph.

The stochastic process underlying a PEPA component

Theorem

For any finite PEPA model $P \stackrel{\text{def}}{=} P_0$, if we define the stochastic process $X(t)$, such that $X(t) = P_i$ indicates that the system behaves as component P_i at time t, then $X(t)$ is a Markov process.

Sojourn time of a component P

- The sojourn time of a component P is an exponentially distributed random variable, whose parameter is the sum of the activity rates of the activities enabled by P.
- The mean, or expected, sojourn time will therefore be

$$\left(\sum_{a \in \mathcal{A}ct(P)} r_a \right)^{-1}$$

Exit rate from a component P

- The exit rate from a component P is the rate at which the system leaves the state corresponding to the component P.
- It is denoted by $q(P)$, and is defined as:

$$q(P) = \sum_{a \in \mathcal{A}ct(P)} r_a$$

- This can be regarded as the rate at which the component P does something, or equivalently, the rate at which it completes an arbitrary activity.

Transition rate

- The transition rate between two components P_i and P_j is denoted by $q(P_i, P_j)$.
- This is the rate at which the system changes from behaving as P_i to behaving as P_j, or the rate at which transitions between the states corresponding to P_i and P_j occur.
- It is the sum of the activity rates labelling arcs which connect the node corresponding to P_i to the node corresponding to P_j in the derivation graph, i.e.,

$$q(P_i, P_j) = \sum_{a \in \mathcal{A}ct(P_i|P_j)} r_a$$

  where $\mathcal{A}ct(P_i|P_j) = \{\!|a \in \mathcal{A}ct(P_i)|\ P_i \xrightarrow{a} P_j|\!\}$.
- Clearly, if P_j is not a one-step derivative of P_i, $q(P_i, P_j) = 0$.

Conditional transition rate

- The conditional transition rate from P_i to P_j via an action type α is denoted by $q(P_i, P_j, \alpha)$.
- This is the sum of the activity rates labelling arcs connecting the corresponding nodes in the derivation graph which are also labelled by the action type α.
- It is the rate at which a system behaving as component P_i evolves to behaving as component P_j as the result of completing a type α activity.

Conditional exit rate

- The conditional exit rate from a component P, denoted by $q(P, \alpha)$, is the rate of leaving P via an activity of a given action type α.
- It is the sum of all activity rates for type α activities enabled in P.
- It is clear that the conditional exit rate of P via α is the same as the apparent rate of α in P, i.e.,

$$q(P, \alpha) = r_\alpha(P)\,.$$

Conditional probabilities

- The conditional probabilities of a component P ending a sojourn by completing a given activity a, or any activity of a given action type α, are denoted by $Pr(P, a)$ and $Pr(P, \alpha)$, respectively.
- There are defiend by:

$$Pr(P, a) = \frac{r_a}{\sum_{b \in Act(P)} r_b}$$

$$Pr(P, \alpha) = \frac{r_\alpha(P)}{\sum_{(\beta, r) \in Act(P)} r_\beta(P)}$$

Transition probabilities

- The transition probability that a component P_i completes an activity and then the system behaves as P_j is denoted by $Pr(P_i, P_j)$.
- This is defined as:

$$Pr(P_i, P_j) = \frac{q(P_i, P_j)}{q(P_i)}$$

Infinitesimal generator matrix

- The infinitesimal generator matrix $\mathbf{Q}$ of the Markov process underlying a PEPA component $P \stackrel{\text{def}}{=} P_0$ is defined as: let $ds(P) = \{P_0, \ldots, P_n\}$,
  - the off-diagonal elements q_{ij} are defined by:

$$q_{ij} = q(P_i, P_j) \quad \text{for all } P_i, P_j \in ds(P)$$

  - the diagonal elements are formed as the negative sum of the non-diagonal elements of each row, i.e.,

$$q_{ii} = -q(P_i)\,.$$

Definitions

Steady state probability

- We are interested in analyzing the behaviour of systems over an extended period of time.
- The system should have settled into some "normal" pattern of behaviour in which the rate of flow out of any state is balanced by the rate of flow into the state.
- This situation is called steady state or equilibrium.

Steady state probability

- A steady state probability distribution for the process undelying a PEPA component P, $\boldsymbol{\pi}$, if it exists, can be computed by solving the matrix equation

$$\boldsymbol{\pi}\mathbf{Q} = \mathbf{0}$$

subject to the normalization condition

$$\sum_{P_i \in ds(P)} \pi(P_i) = 1$$

Definitions

Finite models

- A PEPA model is finite if its derivative set contains a finite number of components.
- This does not restrict the behaviour of the model to be finite in the sense of operating for only a finite time. Instead the process exhibit infinite behaviour over a finite number of states.

PEPA models with equilibrium behaviour

Cyclic, or irreducible, PEPA component

- A PEPA component is cyclic, or irreducible, if it is a derivative of all the components in its derivative set, i.e.,

$$P \in ds(P_i) \text{ for all } i \text{ such that } P_i \in ds(P)$$

- A cyclic component is one in which behaviour may always be repeated, i.e., how ever the model evolves from this component it will always eventually return to this component.
- In particular, this means that for every choice, whichever component is choosen the model must eventually return to the point where the choice can be made again, possibly with a different outcome.
- This implies that choice combinators may only be introduced at the lowest level of a cyclic component.

PEPA models with equilibrium behaviour

Cyclic, or irreducible, PEPA component

- A PEPA component which involves a choice combinator may subsequently be used in a cooperation, but a component involving a cooperation may not subsequently used in a chooice.

Cyclic, or irreducible, PEPA component

- Example: consider the component: $C \stackrel{\text{def}}{=} C_1 + C_2$ where

$$C_1 \stackrel{\text{def}}{=} P_0 \underset{L}{\bowtie} Q_0 \qquad C_2 \stackrel{\text{def}}{=} R_0 \underset{K}{\bowtie} S_0$$

- Whichever component C_i first completes an activity, the component will then behave as C_i, C_1 say.
- All derivaties of C_1 must have the form $C_1' \stackrel{\text{def}}{=} P_i \underset{L}{\bowtie} Q_j$ for some $P_i \in ds(P_0)$ and $Q_j \in ds(Q_0)$.
- The component C is cyclic only if $C_1 + C_2 \in ds(C)$.
- This implies that there is some derivative of C_1 which is syntactically equivalent to $(P_0 \underset{L}{\bowtie} Q_0) + (R_0 \underset{K}{\bowtie} S_0)$, i.e., some P_i and Q_j such that $P_i \underset{L}{\bowtie} Q_j \equiv (P_0 \underset{L}{\bowtie} Q_0) + (R_0 \underset{K}{\bowtie} S_0)$. However this is not possible and then C cannot be cyclic.

PEPA models with equilibrium behaviour

Cyclic, or irreducible, PEPA component

- If a PEPA component is irreducible then all choices must occur within cooperating components.
- This jiustifies the two-leyer syntax for terms in PEPA:
  - sequential components:

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

  - cooperating components:

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

- The Markov process undelying a PEPA component is irreducible if, and only if, the initial component of the model is cyclic.

PEPA models with equilibrium behaviour

Assumptions

- We assume that all PEPA models are time homogeneous, finite and cyclic.
- If a Markov process that is irreducible has a finite state space then all its states are positive recurrent.
- Thus the PEPA models we consider represent systems with steady state behavoiur.

Steady state distribution

- The steady state distribution of a PEPA component is interpreted as the equilibrium probability (or the long run relative frequency) of the model behaving as each of its derivatives.
- The probability, when the system has settled into a regular pattern of behaviour, that the system is behaving in the way characterized by some component of the PEPA model P_i, is $\pi(P_i)$.
- We can regard $\pi(P_i)$ as the proportion of time that the system will spend behaving as component P_i.

Derivation of Performance Measures

Performance measures

- Performance measures such as throughput, average delay time and queue lengths can be derived from the steady state distribution.
- We associate rewards with certain activities within the system. The reward associated with a component, and the corresponding state, is then the sum of the rewards attached to the activities it enables.
- Performance measures are then derived from the total reward based on the steady state probability distribution.
- If ρ_i is the reward associated with component P_i and π is the steady state distribution, then the total reward R is

$$R = \sum_i \rho_i \pi(P_i)$$

Example 1: Simple resource usage as two cooperating components

Description

- The system has two components: *Process* and *Resource*.
- The *Process* will undertake two activities consecutively: *use* with some rate r_1 in cooperation with the resource, and *task* at some rate r_2.
- The *Resource* will engage in two activities consecutively: *use* at some rate r_3 and *update* at a rate r_4.

Example 1: Simple resource usage as two cooperating components

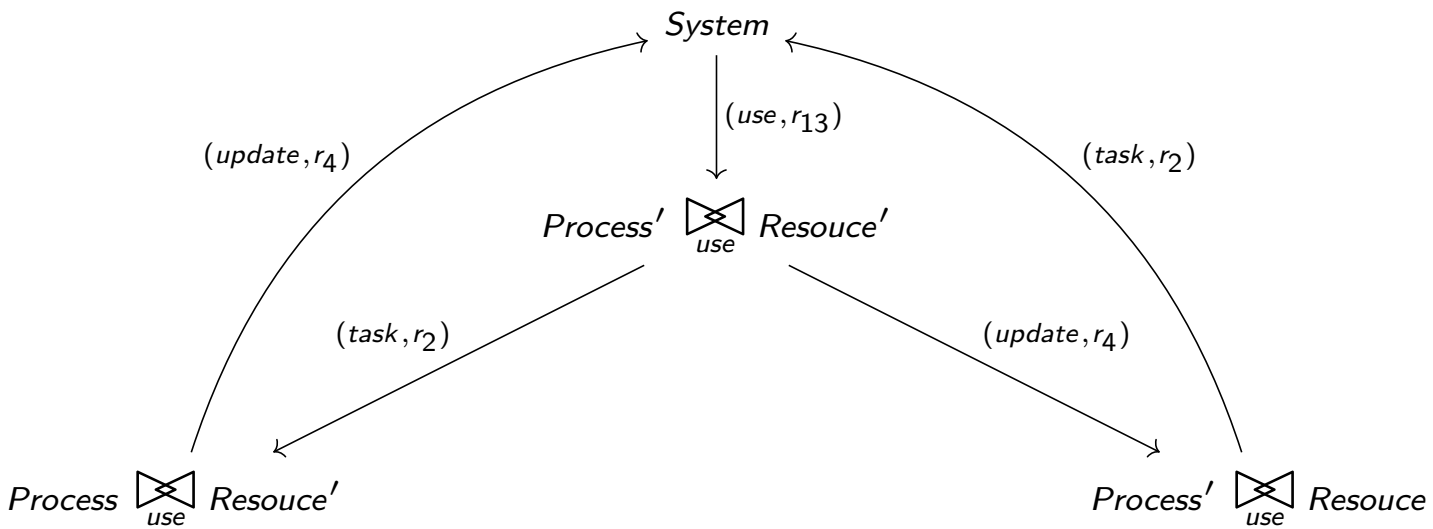
PEPA model

$$
\begin{array}{lcl}
\mathit{Process} & \stackrel{\text{def}}{=} & (\mathit{use}, r_1).\mathit{Process}' \\
\mathit{Process}' & \stackrel{\text{def}}{=} & (\mathit{task}, r_2).\mathit{Process} \\
\mathit{Resource} & \stackrel{\text{def}}{=} & (\mathit{use}, r_3).\mathit{Resource}' \\
\mathit{Resource}' & \stackrel{\text{def}}{=} & (\mathit{update}, r_4).\mathit{Resource} \\
\mathit{System} & \stackrel{\text{def}}{=} & \mathit{Process} \underset{\{\mathit{use}\}}{\bowtie} \mathit{Resource}
\end{array}
$$

Example 1: Simple resource usage as two cooperating components

Derivation graph

Let $r_{13} = min(r_1, r_2)$.



Example 1: Simple resource usage as two cooperating components

The underlying CTMC

- Let the states of the underlying Markov process be labelled X_0, X_1, X_2, X_3, idenfied as follows:

$$X_0 \leftrightarrow Process \underset{use}{\bowtie} Resouce \qquad X_1 \leftrightarrow Process' \underset{use}{\bowtie} Resouce'$$
$$X_2 \leftrightarrow Process \underset{use}{\bowtie} Resouce' \qquad X_3 \leftrightarrow Process' \underset{use}{\bowtie} Resouce$$

- The infinitesimal generator matrix $\mathbf{Q}$ has the following form:

$$\mathbf{Q} = \begin{pmatrix} -r_{13} & r_{13} & 0 & 0 \\ & -(r_2 + r_4) & r_2 & r_4 \\ r_4 & 0 & -r_4 & 0 \\ r_2 & 0 & 0 & -r_2 \end{pmatrix}$$

Example 1: Simple resource usage as two cooperating components

Steady state distribution

- Solving the global balance equations with the normalization condition

$$\boldsymbol{\pi}\mathbf{Q} = \mathbf{0} \qquad \sum_{i=0}^{3} \pi(X_i) = 1$$

- we obtain:

$$\begin{aligned}
\pi(X_0) &= \frac{r_2 r_4 (r_2 + r_4)}{(r_2+r_4) r_2 r_4 + r_{13} r_2 r_4 + r_{13} r_2^2 + r_{13} r_4^2} \\
\pi(X_1) &= \frac{r_2 r_4 r_{13}}{(r_2+r_4) r_2 r_4 + r_{13} r_2 r_4 + r_{13} r_2^2 + r_{13} r_4^2} \\
\pi(X_2) &= \frac{r_{13} r_2^2}{(r_2+r_4) r_2 r_4 + r_{13} r_2 r_4 + r_{13} r_2^2 + r_{13} r_4^2} \\
\pi(X_3) &= \frac{r_{13} r_4^2}{(r_2+r_4) r_2 r_4 + r_{13} r_2 r_4 + r_{13} r_2^2 + r_{13} r_4^2}
\end{aligned}$$

Example 1: Simple resource usage as two cooperating components

Steady state distribution

- Suppose that the activities have the following rates:

$$\begin{array}{lcllcl} (use, r_1) : r_1 & = & 2 & (task, r_2) : r_2 & = & 2 \\ (use, r_3) : r_3 & = & 6 & (update, r_4) : r_4 & = & 8 \\ (use, r_{13}) : r_{13} & = & min(2, 6) = 2 & & & \end{array}$$

- With these values we obtain

$$\pi(X_0) = \frac{20}{41} \qquad \pi(X_1) = \frac{4}{41} \qquad \pi(X_2) = \frac{1}{41} \qquad \pi(X_3) = \frac{16}{41}$$

Example 1: Simple resource usage as two cooperating components

Performance measures: Utilisation of the resource

- The resource will be utilised whenever it is engaged in a use activity or an update activity.
- Therefore to derive the utilisation we associate a *reward* of 1 with each of these activities. Then, if ρ_i denotes the reward associated with state X_i, then

$$\rho_0 = 1 \quad \rho_1 = 1 \quad \rho_2 = 1 \quad \rho_3 = 0\,.$$

- The utilisation U_{res} is the total probability that the model is in one of the states in which the resource is in use, i.e., it is equal to the total reward:

$$U_{res} = \rho_0\ \pi(X_0) + \rho_1\ \pi(X_1) + \rho_2\ \pi(X_2) = \frac{25}{41} = 60.98\%$$

Example 1: Simple resource usage as two cooperating components

Performance measures: Throughput of the process

- The throughput of the process will be the expected number of completed $(use, task)$ pairs of activities to be completed per unit time.
- Since each activity is visited only once, this throughput will be the same as the throughput of either of the activities.
- The throughput T_{use} of activity *use* is found by associating a reward equal to the activity rate with each instance of the activity. Thus, the rewards associated with states are:

$$\rho_0 = 2 \quad \rho_1 = 0 \quad \rho_2 = 0 \quad \rho_3 = 0$$

$$T_{use} = \rho_0 \times \pi(X_0) = 2 \times \pi(X_0) = \frac{40}{41} = 0.975$$

or, since $1/0.975 \sim 1.025$, approximately 1 activity every 1.025 milliseconds.

Example 2: A faulty component in cooperation with a resource and a repairman

Description

- Consider a system consisting of the following components: *Comp*, *Res* and *Repman*.
- *Comp* is a faulty component which is also capable of completing a task satisfactorily.
- *Res* is a resource: the faulty component may need to cooperate with a resource in order to complete its task.
- *Repman* represents a repairman: the component also needs to cooperate with a repairman in order to be rapaired.
- the *System* consists of two components competing for access to the resource and the repairman.

Example 2: A faulty component in cooperation with a resource and a repairman

PEPA model

- Consider the following PEPA model for *System*:

$$
\begin{aligned}
\mathit{Comp} &\stackrel{\text{def}}{=} (\mathit{error}, \epsilon).(\mathit{repair}, \rho).\mathit{Comp} + (\mathit{task}, \mu).\mathit{Comp} \\
\mathit{Res} &\stackrel{\text{def}}{=} (\mathit{task}, \top).(\mathit{reset}, r).\mathit{Res} \\
\mathit{Repman} &\stackrel{\text{def}}{=} (\mathit{repair}, \top).\mathit{Repman} \\
\mathit{System} &\stackrel{\text{def}}{=} ((\mathit{Comp} \| \mathit{Comp}) \underset{\{\mathit{task}\}}{\bowtie} \mathit{Res}) \underset{\{\mathit{repair}\}}{\bowtie} \mathit{Repman}
\end{aligned}
$$

Example 2: A faulty component in cooperation with a resource and a repairman

Derivation graph

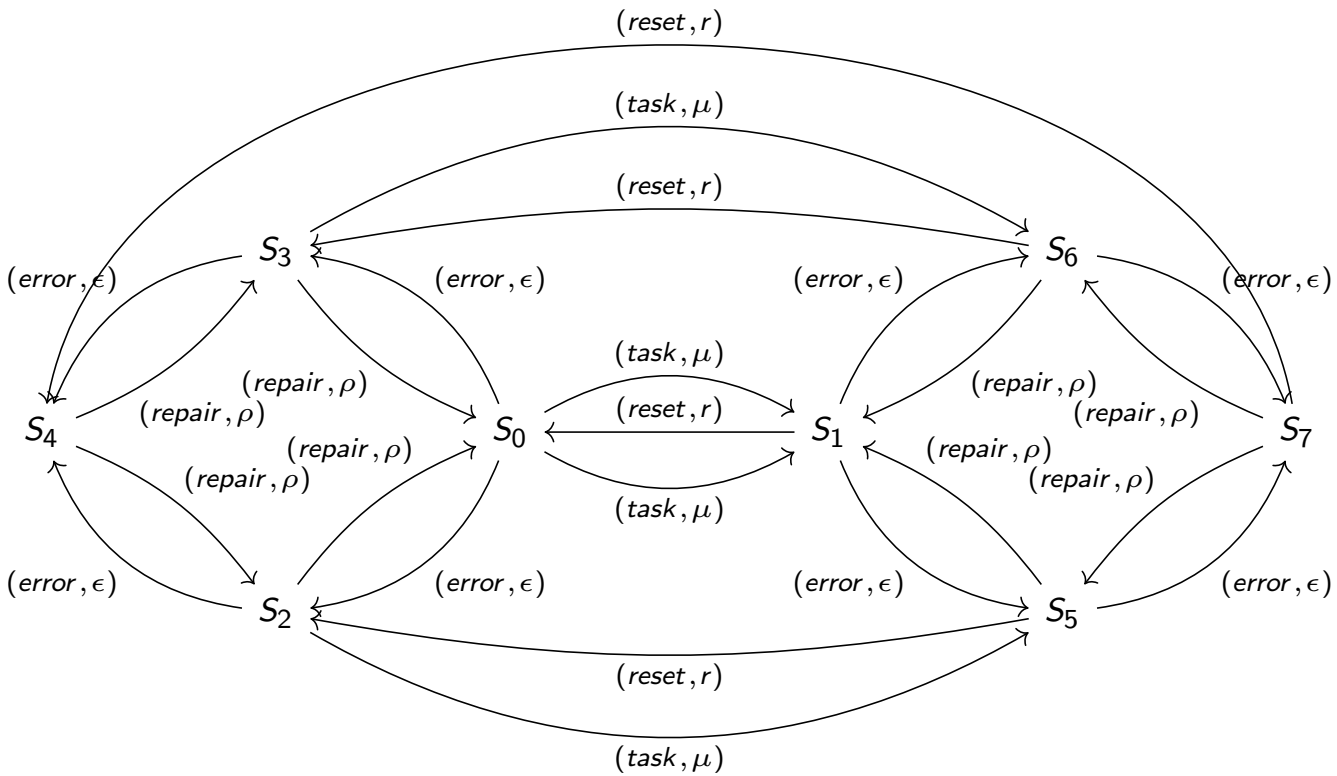
- Draw the derivation graph of *System*:

$$
\begin{aligned}
S_0 &\stackrel{\text{def}}{=} ((Comp \| Comp) \underset{\{task\}}{\bowtie} Res) \underset{\{repair\}}{\bowtie} Repman \\
S_1 &\stackrel{\text{def}}{=} ((Comp \| Comp) \underset{\{task\}}{\bowtie} (reset, r).Res) \underset{\{repair\}}{\bowtie} Repman \\
S_2 &\stackrel{\text{def}}{=} (((repair, \rho).Comp \| Comp) \underset{\{task\}}{\bowtie} Res) \underset{\{repair\}}{\bowtie} Repman \\
S_3 &\stackrel{\text{def}}{=} ((Comp \| (repair, \rho).Comp) \underset{\{task\}}{\bowtie} Res) \underset{\{repair\}}{\bowtie} Repman \\
S_4 &\stackrel{\text{def}}{=} (((repair, \rho).Comp \| (repair, \rho).Comp) \underset{\{task\}}{\bowtie} Res) \underset{\{repair\}}{\bowtie} Repman \\
S_5 &\stackrel{\text{def}}{=} (((repair, \rho).Comp \| Comp) \underset{\{task\}}{\bowtie} (reset, r).Res) \underset{\{repair\}}{\bowtie} Repman \\
S_6 &\stackrel{\text{def}}{=} ((Comp \| (repair, \rho).Comp) \underset{\{task\}}{\bowtie} (reset, r).Res) \underset{\{repair\}}{\bowtie} Repman \\
S_7 &\stackrel{\text{def}}{=} (((repair, \rho).Comp \| (repair, \rho).Comp) \underset{\{task\}}{\bowtie} (reset, r).Res) \underset{\{repair\}}{\bowtie} Repman
\end{aligned}
$$

Example 2: A faulty component in cooperation with a resource and a repairman

Derivation graph

- The derivation graph of *System* is:



Example 2: A faulty component in cooperation with a resource and a repairman

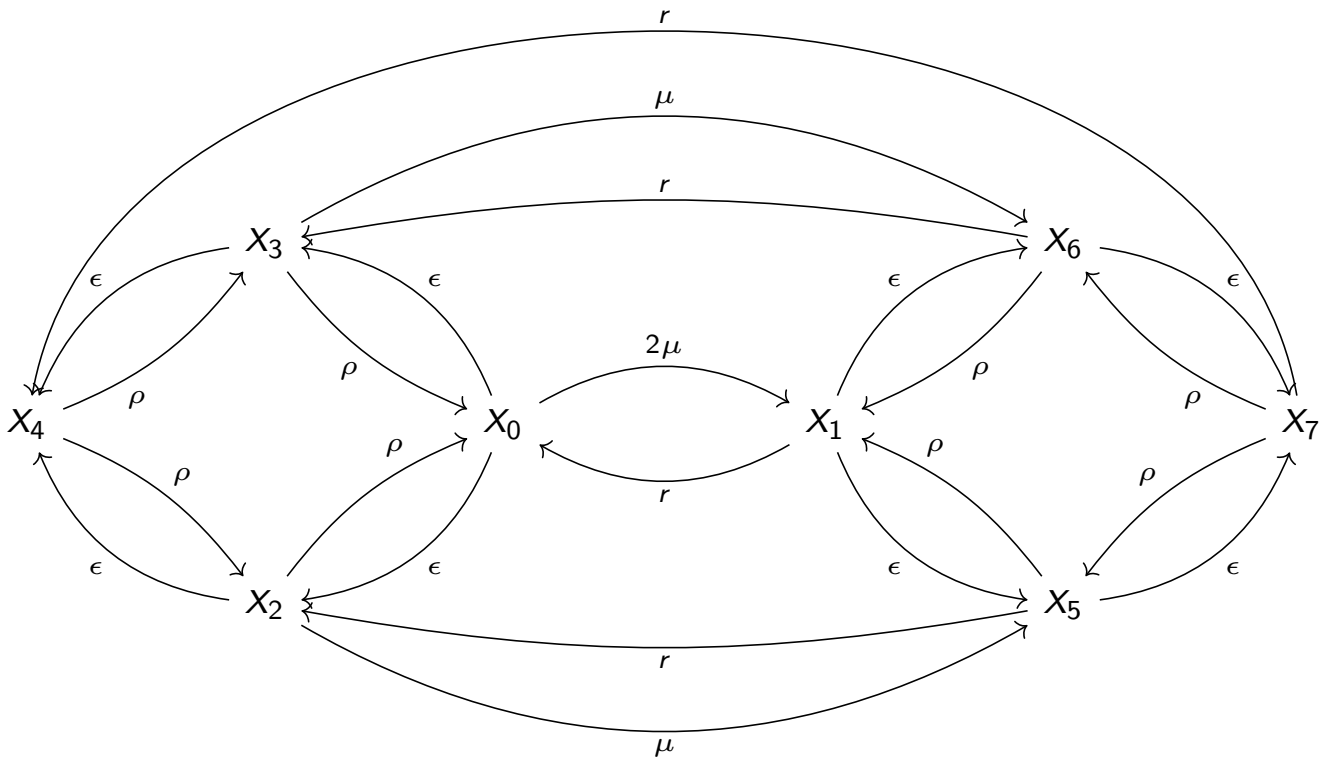
The underlying CTMC

- Note that there is a pair of arcs in the derivation graph between the initial state S_0 and its one-step derivative S_1.
- This captures the fact that there are two distinct derivations of the activity $(task, \mu)$ according to whether the first or second component completes the task in cooperation with the resource.
- The derivation graph is the basis of the underlying CTMC.

Example 2: A faulty component in cooperation with a resource and a repairman

The underlying CTMC

- The underlying CTMC is:



Example 2: A faulty component in cooperation with a resource and a repairman

The global balance equations of *System*

$$\pi_0(2\mu + 2\epsilon) = \pi_1 r + \pi_2 \rho + \pi_3 \rho$$
$$\pi_1(r + 2\epsilon) = \pi_0 2\mu + \pi_5 \rho + \pi_6 \rho$$
$$\pi_2(r + \mu + \epsilon) = \pi_0 \epsilon + \pi_4 \rho + \pi_5 r$$
$$\pi_3(r + \mu + \epsilon) = \pi_0 \epsilon + \pi_4 \rho + \pi_6 r$$
$$\pi_4(2\rho) = \pi_2 \epsilon + \pi_3 \epsilon + \pi_7 r$$
$$\pi_5(r + \rho + \epsilon) = \pi_1 \epsilon + \pi_2 \mu + \pi_7 \rho$$
$$\pi_6(r + \rho + \epsilon) = \pi_1 \epsilon + \pi_3 \mu + \pi_7 \rho$$
$$\pi_7(r + 2\rho) = \pi_6 \epsilon + \pi_7 \epsilon$$
$$\pi_0 + \pi_1 + \pi_2 + \pi_3 + \pi_4 + \pi_5 + \pi_6 + \pi_7 = 1$$

The normalization condition

$$\pi_0 + \pi_1 + \pi_2 + \pi_3 + \pi_4 + \pi_5 + \pi_6 + \pi_7 = 1$$

Example 2: A faulty component in cooperation with a resource and a repairman

Performance measures: Utilisation of the resource

- The utilisation of the resource is the total probability that the model is in one of the states in which the resource is in use:

$$U_{res} = \pi_0 + \pi_2 + \pi_3$$

Example 2: A faulty component in cooperation with a resource and a repairman

Performance measures: Throughput of *task*

- The throughput of *task* is the expected number of tasks completed per unit time.

$$T_{task} = 2\mu\pi_0 + \mu\pi_2 + \mu\pi_3$$