Modeling and Verification of Probabilistic Systems

Joost-Pieter Katoen

Lehrstuhl für Informatik 2
Software Modeling and Verification Group

http://moves.rwth-aachen.de/teaching/ss-14/movep14/

July 10, 2014

Overview

Model-based performance evaluation

- Analyse performance metrics based on an abstract system model
  - formalisms: stochastic Petri nets, queueing networks, SANs, ...
- The prevailing paradigm is continuous-time randomness
  - exponential distributions, i.e., continuous-time Markov processes
- Complexity of systems requires compositional approach
  - reflecting system architecture
- Enormous model sizes require compositional abstraction mechanisms
  - like bisimulation minimization
- Nondeterminism is at heart of compositionality

We need: Compositional Continuous-Time Markov Chains

Markov automata

A Markov automaton M is a tuple $(S, Act, \longrightarrow, \Longrightarrow, s_0)$ where

- S is a nonempty set of states with initial state $s_0 \in S$
- Act is a set of actions; τ is an internal action
- $\longrightarrow \subseteq S \times Act \times Distr(S)$ is a set of action transitions
- $\Longrightarrow \subseteq S \times \mathbb{R}_{>0} \times S$ is a set of Markovian transitions

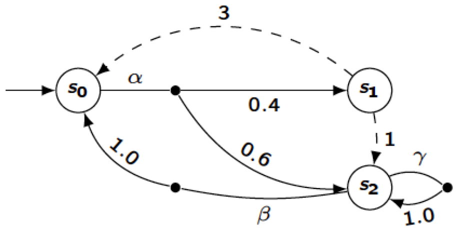
  such that there is at most one $r \in \mathbb{R}_{>0}$ with $s \stackrel{r}{\Longrightarrow} s'$

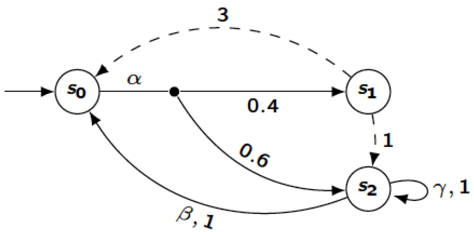
Thus:

MA are probabilistic automata (with action-labeled transitions) extended with Markovian transitions that are labeled with rates of exponential distributions. Any CTMC is an MA; any PA is an MA.

Markov automata

[Eisentraut et al., 2010]





Markov automata

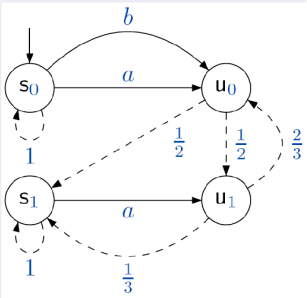
A Markov automaton M is a tuple $(S, Act, \longrightarrow, \Longrightarrow, s_0)$ where
- S is a nonempty set of states with initial state $s_0 \in S$
- Act is a set of actions; τ is an internal action
- $\longrightarrow \subseteq S \times Act \times Distr(S)$ is a set of action transitions
- $\Longrightarrow \subseteq S \times \mathbb{R}_{>0} \times S$ is a set of Markovian transitions such that there is at most one $r \in \mathbb{R}_{>0}$ with $s \overset{r}{\Longrightarrow} s'$

1. $IT(s)$ is the set of interactive transitions that leave s.
2. $MT(s)$ is the set of Markovian transitions that leave s.

Markov automata

Classification of states

- s is Markovian if $MT(s) \neq \varnothing$ and $IT(s) = \varnothing$
- s is interactive if $MT(s) = \varnothing$ and $IT(s) \neq \varnothing$
- s is hybrid if $MT(s) \neq \varnothing$ and $IT(s) \neq \varnothing$
- s is timelock if $MT(s) = IT(s) = \varnothing$



For Markovian state s, let:
- $\mathbf{R}(s, s') = \sum \left\{ \lambda \mid s \overset{\lambda}{\Longrightarrow} s' \right\}$ be the rate to move from s to s',
- $r(s) = \sum_{s' \in S} \mathbf{R}(s, s')$ be the exit rate of s
- $\mathbf{P}(s, s') = \frac{\mathbf{R}(s,s')}{r(s)}$ is the probability to move from s to s'

Maximal progress assumption

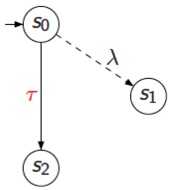
Maximal progress

1. Internal (action) transitions are labeled with the action τ.
2. These transitions will not be subject to interaction.
3. They cannot be delayed by other components.
4. Thus, internal interactive transitions can trigger immediately.
5. But, the probability to execute Markovian transitions immediately is zero.

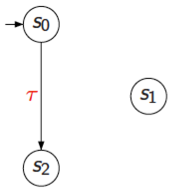
Maximal progress assumption

Internal transitions take precedence over Markovian ones.

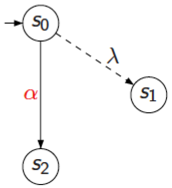
Maximal progress



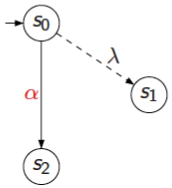
reduces to



But as visible actions may be subject to delaying by other components:



remains



Overview

Parallel composition

The *composition* of M_1 and M_2 with $A = (Act_1 \cap Act_2) \setminus \{ \tau \}$ is:

$$M_1 \,||\, M_2 = (S_1 \times S_2, Act_1 \cup Act_2, \longrightarrow, \Longrightarrow, (s_{0,1}, s_{0,2}))$$

where $\longrightarrow$ and $\Longrightarrow$ are defined as the smallest relations satisfying:

$$\text{(SYNC)} \ \frac{s_1 \xrightarrow{\alpha}_1 \mu_1 \text{ and } s_2 \xrightarrow{\alpha}_2 \mu_2 \text{ and } \alpha \in A}{(s_1, s_2) \xrightarrow{\alpha} \mu_1 \cdot \mu_2}$$

$$\text{(ASYNC)} \ \frac{s_1 \xrightarrow{\alpha}_1 \mu_1 \text{ and } \alpha \notin A}{(s_1, s_2) \xrightarrow{\alpha} \mu_1 \cdot \{ s_2 \mapsto 1 \}}$$

$$\text{(DELAY)} \ \frac{s_1 \xRightarrow{\lambda}_1 s_1'}{(s_1, s_2) \xRightarrow{\lambda} (s_1', s_2)} \quad \text{AND} \quad \frac{s_1 \xRightarrow{\lambda}_1 s_1 \text{ and } s_2 \xRightarrow{\lambda'}_2 s_2}{(s_1, s_2) \xRightarrow{\lambda + \lambda'} (s_1, s_2)}$$

Compatibility

Parallel composition is compatible with parallel composition on PA:

$||$ is PA-composition, if the MAs are PAs

Parallel composition: examples

Hiding

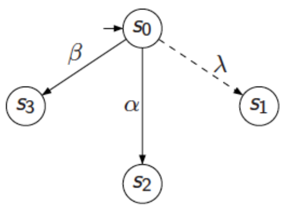
Hiding

The *hiding* of MA $M = (S, Act, \longrightarrow, \Longrightarrow, s_0)$ wrt. the set $A \subseteq Act \setminus \{ \tau \}$ of actions is the MA $M \setminus A = (S, Act \setminus A, \longrightarrow', \Longrightarrow, s_0)$ where $\longrightarrow'$ is the smallest relation defined by:

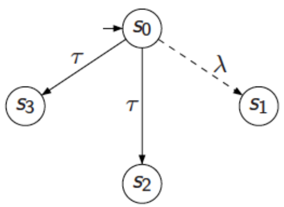
1. $s \xrightarrow{\alpha} \mu$ and $\alpha \notin A$ implies $s \xrightarrow{\alpha}' \mu$, and
2. $s \xrightarrow{\alpha} \mu$ and $\alpha \in A$ implies $s \xrightarrow{\tau}' \mu$.

- Hiding transforms α-transitions with $\alpha \in A$ into τ-transitions.
- Turning an α-transition emanating from state s into a τ-transition may change the semantics of the MA, as now —due to maximal progress— never a Markovian transition in s will be taken.

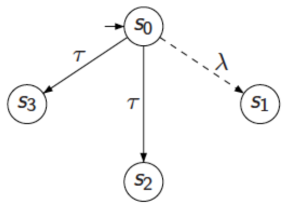
Hiding



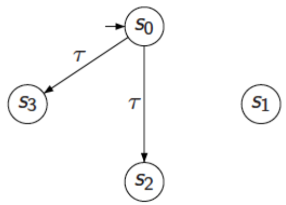
hiding $\{ \alpha, \beta \}$ yields



Applying maximal progress reduction yields:

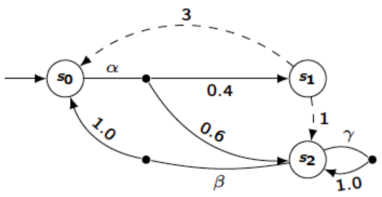


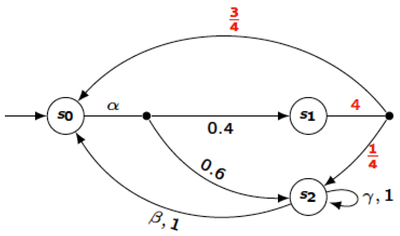
reduces to



Overview

Bisimulation





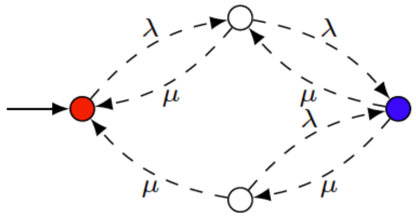
Bisimulation

Equivalence $R \subseteq S \times S$ is a *bisimulation* if for all $(s, t) \in R$:

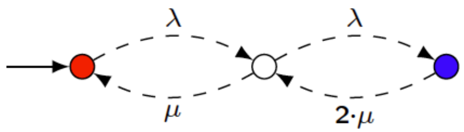
$\forall \delta \in Act \cup \mathbb{R}_{>0}$: $s \xrightarrow{\delta} \mu$ implies $t \xrightarrow{\delta} \nu$ with $\forall C \in S/R : \mu(C) = \nu(C)$.

Let $\sim$ be the largest bisimulation relation.

Bisimulation – Example



is bisimilar to



Bisimulation – Congruence

Congruence

$\sim$ is a congruence wrt. parallel composition and hiding. Thus:

1. $M \sim M'$ implies $\forall N.\, M \,||\, N \;\sim\; M' \,||\, N$
2. $M \sim M'$ implies $\forall A \subseteq Act \setminus \{\tau\}.\, M \setminus A \;\sim M' \setminus A$.

Compatibility

$\sim$ is compatible with bisimilarity ($\sim_p$) on PA:

$\sim$ equals $\sim_p$, if the MAs are PAs

Overview

1. What are Markov automata?
2. Parallel composition and hiding
3. Bisimulation
4. A process algebra for Markov automata

A process algebra for MA