Using Stochastic Comparison for Efficient Model Checking of Uncertain Markov Chains [1]

Serge Haddad (LSV), Nihal Pekergin (LACL)

QEST'09, 15th september 2009

[1] partially supported by ANR project ANR-SETIN-002 CheckBound

Motivation

From probabilistic discrete-event systems to Markov chains (MCs)

- Probabilistic systems are not necessarily memoryless (timeouts, packet arrivals, etc.).
- However during the modeling and analysis process, one often encounters Markov chains (e.g. the embedded Markov chain of a semi-Markovian process).

Why Interval Markov Chains (IMCs)?

- Estimation of the transition rates through statistical experiences leading to confidence intervals.
- Abstraction of events during the modeling step or abstraction of states during the analysis step.

Motivation

From probabilistic discrete-event systems to Markov chains (MCs)

- Probabilistic systems are not necessarily memoryless (timeouts, packet arrivals, etc.).
- However during the modeling and analysis process, one often encounters Markov chains (e.g. the embedded Markov chain of a semi-Markovian process).

Why Interval Markov Chains (IMCs)?

- Estimation of the transition rates through statistical experiences leading to confidence intervals.
- Abstraction of events during the modeling step or abstraction of states during the analysis step.

Analysis of IMC

First works

- Introduction of the formalism and study of conformance relations between models.
  (Jonsson, Larsen LCS'91)
- Methods for computing the parameters of an IMC.
  (Kozine, Utkin Reliable Computing 2002)

Probabilistic model-checking

- Analysis of the model checking of PCTL over IMCs: in PSPACE (via the existential theory of reals), NP-hard and coNP-hard.
  (Sen, Wiswanathan, Agha TACAS'06)
- Generalization for a new logic ω-PCTL: still in PSPACE.
  (Chatterjee, Sen, Henzinger FOSSACS'08).

Handling efficiently model checking for IMC

Drawbacks: complexity and expressivity considerations

- Algorithms in PSPACE are impractical for large IMCs.
- Some useful properties cannot be expressed even with ω-PCTL.

Goal: semi-decision procedures based on stochastic comparison

- Generally different magnitude orders between the requirement and implementation probabilities.
  Thus the *don't know* case should seldom occur.
- The problem is reduced to the model checking of MCs.
  This should lead to a significant improvement w.r.t. time complexity.

Handling efficiently model checking for IMC

Drawbacks: complexity and expressivity considerations

- Algorithms in PSPACE are impractical for large IMCs.
- Some useful properties cannot be expressed even with ω-PCTL.

Goal: semi-decision procedures based on stochastic comparison

- Generally different magnitude orders between the requirement and implementation probabilities.
  Thus the *don't know* case should seldom occur.
- The problem is reduced to the model checking of MCs.
  This should lead to a significant improvement w.r.t. time complexity.

Outline

1. IMC model
2. PCTL
3. Efficient Model Checking PCTL for IMCs
4. Conclusion and perspectives

Outline

1. IMC model

PCTL

Efficient Model Checking PCTL for IMCs

Conclusion and perspectives

Interval Markov Chain

Syntax

An IMC $\mathcal{M}(\mathbf{P}^-, \mathbf{P}^+) = (\mathcal{S}, \mathbf{P}^-, \mathbf{P}^+, L)$ is defined by:

- $\mathcal{S}$, the finite set of states which are labelled by atomic properties through the mapping L;
- $\mathbf{P}^-$ (resp. $\mathbf{P}^+$ with $\mathbf{P}^+ \geq \mathbf{P}^-$), a sub-stochastic (resp. super-stochastic) matrix:

$$\forall s \in \mathcal{S} \;\; \sum_{t \in \mathcal{S}} \mathbf{P}^-[s,t] \leq 1 \leq \sum_{t \in \mathcal{S}} \mathbf{P}^+[s,t]$$

Semantic

A DTMC with transition probability matrix $\mathbf{P}$ over $\mathcal{S}$ is said to belong to $\mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$ (denoted $\mathbf{P} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$), if:

$$\forall s, t \in \mathcal{S} \quad \mathbf{P}^-[s,t] \leq \mathbf{P}[s,t] \leq \mathbf{P}^+[s,t]$$

W.l.o.g. we assume that:

$$\mathbf{P}^-[s,t] \geq 1 - \sum_{t' \neq t} \mathbf{P}^+[s,t'] \wedge \mathbf{P}^+[s,t] \leq 1 - \sum_{t' \neq t} \mathbf{P}^-[s,t']$$

Interval Markov Chain

Syntax

An IMC $\mathcal{M}(\mathbf{P}^-, \mathbf{P}^+) = (\mathcal{S}, \mathbf{P}^-, \mathbf{P}^+, L)$ is defined by:

- $\mathcal{S}$, the finite set of states which are labelled by atomic properties through the mapping L;
- $\mathbf{P}^-$ (resp. $\mathbf{P}^+$ with $\mathbf{P}^+ \geq \mathbf{P}^-$), a sub-stochastic (resp. super-stochastic) matrix:

$$\forall s \in \mathcal{S} \ \sum_{t \in \mathcal{S}} \mathbf{P}^-[s,t] \leq 1 \leq \sum_{t \in \mathcal{S}} \mathbf{P}^+[s,t]$$

Semantic

A DTMC with transition probability matrix $\mathbf{P}$ over $\mathcal{S}$ is said to belong to $\mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$ (denoted $\mathbf{P} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$), if:

$$\forall s, t \in \mathcal{S} \quad \mathbf{P}^-[s,t] \leq \mathbf{P}[s,t] \leq \mathbf{P}^+[s,t]$$

W.l.o.g. we assume that:

$$\mathbf{P}^-[s,t] \geq 1 - \sum_{t' \neq t} \mathbf{P}^+[s,t'] \wedge \mathbf{P}^+[s,t] \leq 1 - \sum_{t' \neq t} \mathbf{P}^-[s,t']$$

Interval Markov Chain

Syntax

An IMC $\mathcal{M}(\mathbf{P}^-, \mathbf{P}^+) = (\mathcal{S}, \mathbf{P}^-, \mathbf{P}^+, L)$ is defined by:

- $\mathcal{S}$, the finite set of states which are labelled by atomic properties through the mapping L;
- $\mathbf{P}^-$ (resp. $\mathbf{P}^+$ with $\mathbf{P}^+ \geq \mathbf{P}^-$), a sub-stochastic (resp. super-stochastic) matrix:

$$\forall s \in \mathcal{S} \ \sum_{t \in \mathcal{S}} \mathbf{P}^-[s,t] \leq 1 \leq \sum_{t \in \mathcal{S}} \mathbf{P}^+[s,t]$$

Semantic

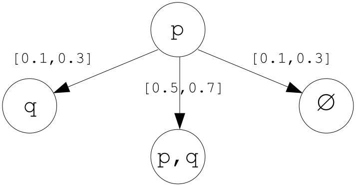
A DTMC with transition probability matrix $\mathbf{P}$ over $\mathcal{S}$ is said to belong to $\mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$ (denoted $\mathbf{P} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$), if:

$$\forall s, t \in \mathcal{S} \quad \mathbf{P}^-[s,t] \leq \mathbf{P}[s,t] \leq \mathbf{P}^+[s,t]$$

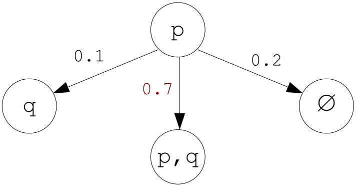
W.l.o.g. we assume that:

$$\mathbf{P}^-[s,t] \geq 1 - \sum_{t' \neq t} \mathbf{P}^+[s,t'] \wedge \mathbf{P}^+[s,t] \leq 1 - \sum_{t' \neq t} \mathbf{P}^-[s,t']$$

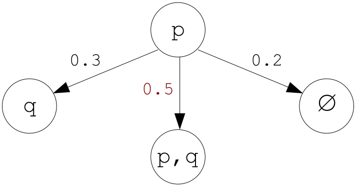
An IMC with two associated DTMCs



Maximizing a probability transition



Minimizing a probability transition



Optimal values for cumulative transition probabilities

Individual transition probabilities

Bounds can always be reached. For every $s, t \in \mathcal{S}$, there is a $\mathbf{P} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$ with $\mathbf{P}[s,t] = \mathbf{P}^+[s,t]$ and a $\mathbf{P} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$ with $\mathbf{P}[s,t] = \mathbf{P}^-[s,t]$.

Let $s \in \mathcal{S}$ and $\mathcal{S}' = \{s_1, \ldots, s_m\} \subset \mathcal{S} = \{s_1, \ldots, s_n\}$

How to maximize $\sum_{t \in \mathcal{S}'} \mathbf{P}[s,t]$ for possible $\mathbf{P}$ in $\mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$?

- Maximize one by one the probability transition taking into account the constraints updated by the previous choices.
- More formally, let $sum = \sum_{j<i} \mathbf{P}[s, s_j]$. Then: $\mathbf{P}[s, s_i] = \min(\mathbf{P}^+[s, s_i], 1 - sum - \sum_{j>i} \mathbf{P}^-[s, s_j]);$

Observations

- There is a similar algorithm for minimization.
- Different subrows $\mathbf{P}[s, -]$ are possible depending on the ordering of $\mathcal{S}'$.

Optimal values for cumulative transition probabilities

Individual transition probabilities

Bounds can always be reached. For every $s, t \in \mathcal{S}$, there is a $\mathbf{P} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$ with $\mathbf{P}[s,t] = \mathbf{P}^+[s,t]$ and a $\mathbf{P} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$ with $\mathbf{P}[s,t] = \mathbf{P}^-[s,t]$.

Let $s \in \mathcal{S}$ and $\mathcal{S}' = \{s_1, \ldots, s_m\} \subset \mathcal{S} = \{s_1, \ldots, s_n\}$

How to maximize $\sum_{t \in \mathcal{S}'} \mathbf{P}[s,t]$ for possible $\mathbf{P}$ in $\mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$?

- Maximize one by one the probability transition taking into account the constraints updated by the previous choices.
- More formally, let $sum = \sum_{j<i} \mathbf{P}[s, s_j]$. Then: $\mathbf{P}[s, s_i] = \min(\mathbf{P}^+[s, s_i], 1 - sum - \sum_{j>i} \mathbf{P}^-[s, s_j]);$

Observations

- There is a similar algorithm for minimization.
- Different subrows $\mathbf{P}[s, -]$ are possible depending on the ordering of $\mathcal{S}'$.

Optimal values for cumulative transition probabilities

Individual transition probabilities

Bounds can always be reached. For every $s, t \in \mathcal{S}$, there is a $\mathbf{P} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$ with $\mathbf{P}[s,t] = \mathbf{P}^+[s,t]$ and a $\mathbf{P} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$ with $\mathbf{P}[s,t] = \mathbf{P}^-[s,t]$.

Let $s \in \mathcal{S}$ and $\mathcal{S}' = \{s_1, \ldots, s_m\} \subset \mathcal{S} = \{s_1, \ldots, s_n\}$

How to maximize $\sum_{t \in \mathcal{S}'} \mathbf{P}[s,t]$ for possible $\mathbf{P}$ in $\mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$?

- Maximize one by one the probability transition taking into account the constraints updated by the previous choices.
- More formally, let $sum = \sum_{j<i} \mathbf{P}[s, s_j]$. Then:
  $\mathbf{P}[s, s_i] = \min(\mathbf{P}^+[s, s_i], 1 - sum - \sum_{j>i} \mathbf{P}^-[s, s_j])$;

Observations

- There is a similar algorithm for minimization.
- Different subrows $\mathbf{P}[s, -]$ are possible depending on the ordering of $\mathcal{S}'$.

Optimal values for cumulative transition probabilities

Individual transition probabilities

Bounds can always be reached. For every $s, t \in \mathcal{S}$, there is a $\mathbf{P} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$ with $\mathbf{P}[s,t] = \mathbf{P}^+[s,t]$ and a $\mathbf{P} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$ with $\mathbf{P}[s,t] = \mathbf{P}^-[s,t]$.

Let $s \in \mathcal{S}$ and $\mathcal{S}' = \{s_1, \ldots, s_m\} \subset \mathcal{S} = \{s_1, \ldots, s_n\}$

How to maximize $\sum_{t \in \mathcal{S}'} \mathbf{P}[s,t]$ for possible $\mathbf{P}$ in $\mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)$?

- Maximize one by one the probability transition taking into account the constraints updated by the previous choices.
- More formally, let $sum = \sum_{j<i} \mathbf{P}[s, s_j]$. Then: $\mathbf{P}[s, s_i] = \min(\mathbf{P}^+[s, s_i], 1 - sum - \sum_{j>i} \mathbf{P}^-[s, s_j])$;

Observations

- There is a similar algorithm for minimization.
- Different subrows $\mathbf{P}[s, -]$ are possible depending on the ordering of $\mathcal{S}'$.

IMC for sub-stochastic matrices

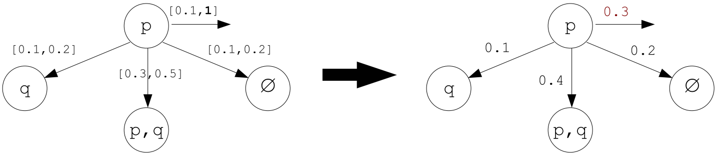
When model checking MCs, one produces MCs with an absorbing state or equivalently sub-stochastic matrices. So:

An IMC $\mathcal{M}(\mathbf{P}^-, \mathbf{P}^+, \mathbf{out})$ for sub-stochastic matrices is enlarged with a vector $\mathbf{out}$ over states such that $\mathbf{P}^-, \mathbf{P}^+, \mathbf{out}$ fulfill for all $s, t \in \mathcal{S}$:

- $0 \leq \mathbf{P}^-[s,t] \leq \mathbf{P}^+[s,t] \wedge \sum_{t' \in \mathcal{S}} \mathbf{P}^-[s,t'] + \mathbf{out}[s] \leq 1$
- $\mathbf{P}^+[s,t] \leq 1 - \sum_{t' \neq t} \mathbf{P}^-[s,t'] - \mathbf{out}[s]$

A sub-stochastic matrix $\mathbf{P}$ over $\mathcal{S}$ belongs to $\mathcal{M}(\mathbf{P}^-, \mathbf{P}^+, \mathbf{out})$ if:

$$\forall s, t \in \mathcal{S} \quad \mathbf{P}^-[s,t] \leq \mathbf{P}[s,t] \leq \mathbf{P}^+[s,t] \wedge \sum_{t' \neq t} \mathbf{P}[s,t'] \leq 1 - \mathbf{out}[s]$$



Stochastic bounds

The survival toolkit: definitions

- Let X, Y be two defective distributions over $\mathcal{S} = \{s_1, \ldots, s_n\}$ defined by $p_X(i) = prob(X = s_i)$ and $p_Y(i) = prob(Y = s_i)$. Then:
$$X \leq_{st} Y \text{ if } \forall i \ \ \sum_{k=1}^{i} p_X(k) \geq \sum_{k=1}^{i} p_Y(k)$$
- Let $\mathbf{P}, \mathbf{P}'$ be two sub-stochastic matrices over $\mathcal{S}$. Then:
$$\mathbf{P} \leq_{st} \mathbf{P}' \text{ if } \forall i \ \ \mathbf{P}[s_i, -] \leq_{st} \mathbf{P}'[s_i, -]$$
- Let $\mathbf{P}$ be a sub-stochastic matrix over $\mathcal{S}$. Then:
$$\mathbf{P} \text{ is } st\text{-monotone if } \forall i < n \ \ \mathbf{P}[s_i, -] \leq_{st} \mathbf{P}[s_{i+1}, -]$$

The survival toolkit: some results

- Let X, Y be two defective distributions over $\mathcal{S}$ such that $X \leq_{st} Y$ and r be a decreasing mapping over $\mathcal{S}$. Then: $E(r(X)) \geq E(r(Y))$
- Let $\mathbf{P} \leq_{st} \mathbf{P}'$ be two sub-stochastic matrices over $\mathcal{S}$ such that either $\mathbf{P}$ or $\mathbf{P}'$ is st-monotone. Then:
  1. The inequality holds for every power of matrices: $\forall k \in \mathbb{N}\ \mathbf{P}^k \leq_{st} \mathbf{P}'^k$
  2. (as a corollary) the mean leaving time of $\mathbf{P}$ is greater than the one of $\mathbf{P}'$:
$$(\sum_{k \in \mathbb{N}} \mathbf{P}^k)\mathbf{1}_n \geq_{el} (\sum_{k \in \mathbb{N}} \mathbf{P}'^k)\mathbf{1}_n$$

Stochastic bounds

The survival toolkit: definitions

- Let X, Y be two defective distributions over $\mathcal{S} = \{s_1, \ldots, s_n\}$ defined by $p_X(i) = prob(X = s_i)$ and $p_Y(i) = prob(Y = s_i)$. Then:
$$X \leq_{st} Y \text{ if } \forall i \;\; \sum_{k=1}^{i} p_X(k) \geq \sum_{k=1}^{i} p_Y(k)$$
- Let $\mathbf{P}, \mathbf{P}'$ be two sub-stochastic matrices over $\mathcal{S}$. Then:
$$\mathbf{P} \leq_{st} \mathbf{P}' \text{ if } \forall i \;\; \mathbf{P}[s_i, -] \leq_{st} \mathbf{P}'[s_i, -]$$
- Let $\mathbf{P}$ be a sub-stochastic matrix over $\mathcal{S}$. Then:
$$\mathbf{P} \text{ is } st\text{-monotone if } \forall i < n \;\; \mathbf{P}[s_i, -] \leq_{st} \mathbf{P}[s_{i+1}, -]$$

The survival toolkit: some results

- Let X, Y be two defective distributions over $\mathcal{S}$ such that $X \leq_{st} Y$ and r be a decreasing mapping over $\mathcal{S}$. Then: $E(r(X)) \geq E(r(Y))$
- Let $\mathbf{P} \leq_{st} \mathbf{P}'$ be two sub-stochastic matrices over $\mathcal{S}$ such that either $\mathbf{P}$ or $\mathbf{P}'$ is st-monotone. Then:
  1. The inequality holds for every power of matrices: $\forall k \in \mathbb{N} \; \mathbf{P}^k \leq_{st} \mathbf{P}'^k$
  2. (as a corollary) the mean leaving time of $\mathbf{P}$ is greater than the one of $\mathbf{P}'$:
$$(\sum_{k \in \mathbb{N}} \mathbf{P}^k)\mathbf{1}_n \geq_{el} (\sum_{k \in \mathbb{N}} \mathbf{P}'^k)\mathbf{1}_n$$

Stochastic bounds and IMCs

Motivation

How to compute (accurate) bounds for leaving time $\mathbf{m}[s]$ and $\mathbf{M}[s]$?

$$\mathbf{m}[s] \leq \min_{\mathbf{P}\in\mathcal{M}(\mathbf{P}^-,\mathbf{P}^+,\mathbf{out})}\{(\sum_{k\in\mathbb{N}}\mathbf{P}^k)\mathbf{1}_n)[s]\}$$

$$\max_{\mathbf{P}\in\mathcal{M}(\mathbf{P}^-,\mathbf{P}^+,\mathbf{out})}\{(\sum_{k\in\mathbb{N}}\mathbf{P}^k)\mathbf{1}_n)[s]\} \leq \mathbf{M}[s]$$

Computing the best $\mathbf{m}[s]$ is straightforward.

$$\min_{\mathbf{P}\in\mathcal{M}(\mathbf{P}^-,\mathbf{P}^+,\mathbf{out})}\{(\sum_{k\in\mathbb{N}}\mathbf{P}^k)\mathbf{1}_n)[s]\} = (\sum_{k\in\mathbb{N}}(\mathbf{P}^-)^k)\mathbf{1}_n)[s]$$

Computing a bound $\mathbf{M}[s]$ via stochastic order *(Haddad, Moreaux EJOR 2007)*

- There is a unique greatest lower bound $\mathbf{P}^\bullet$ w.r.t. $\leq_{st}$ for $\mathcal{M}(\mathbf{P}^-,\mathbf{P}^+,\mathbf{out})$
- which admits a unique greatest *monotone* lower bounding matrix $\mathbf{P}^\star \leq_{st} \mathbf{P}^\bullet$.
- $\mathbf{M}[s] = (\sum_{k\in\mathbb{N}}(\mathbf{P}^\star)^k)\mathbf{1}_n)[s]$
  (different bounds are possible depending on the ordering of states)
- Furthermore a priori detecting states s for which $\mathbf{M}[s] = \infty$ can be performed in very efficient way without computing the strongly connected components of the underlying graph *(this paper)*.

Stochastic bounds and IMCs

Motivation

How to compute (accurate) bounds for leaving time $\mathbf{m}[s]$ and $\mathbf{M}[s]$?

$$\mathbf{m}[s] \leq \min_{\mathbf{P} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+, \mathbf{out})} \{(\sum_{k \in \mathbb{N}} \mathbf{P}^k) \mathbf{1}_n)[s]\}$$

$$\max_{\mathbf{P} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+, \mathbf{out})} \{(\sum_{k \in \mathbb{N}} \mathbf{P}^k) \mathbf{1}_n)[s]\} \leq \mathbf{M}[s]$$

Computing the best $\mathbf{m}[s]$ is straightforward.

$$\min_{\mathbf{P} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+, \mathbf{out})} \{(\sum_{k \in \mathbb{N}} \mathbf{P}^k) \mathbf{1}_n)[s]\} = (\sum_{k \in \mathbb{N}} (\mathbf{P}^-)^k) \mathbf{1}_n)[s]$$

Computing a bound $\mathbf{M}[s]$ via stochastic order *(Haddad, Moreaux EJOR 2007)*

- There is a unique greatest lower bound $\mathbf{P}^\bullet$ w.r.t. $\leq_{st}$ for $\mathcal{M}(\mathbf{P}^-, \mathbf{P}^+, \mathbf{out})$
- which admits a unique greatest *monotone* lower bounding matrix $\mathbf{P}^\star \leq_{st} \mathbf{P}^\bullet$.
- $\mathbf{M}[s] = (\sum_{k \in \mathbb{N}} (\mathbf{P}^\star)^k) \mathbf{1}_n)[s]$
  (different bounds are possible depending on the ordering of states)
- Furthermore a priori detecting states s for which $\mathbf{M}[s] = \infty$ can be performed in very efficient way without computing the strongly connected components of the underlying graph *(this paper)*.

Stochastic bounds and IMCs

Motivation

How to compute (accurate) bounds for leaving time $\mathbf{m}[s]$ and $\mathbf{M}[s]$?

$$\mathbf{m}[s] \leq \min_{\mathbf{P}\in\mathcal{M}(\mathbf{P}^-,\mathbf{P}^+,\mathbf{out})}\{(\sum_{k\in\mathbb{N}}\mathbf{P}^k)\mathbf{1}_n)[s]\}$$

$$\max_{\mathbf{P}\in\mathcal{M}(\mathbf{P}^-,\mathbf{P}^+,\mathbf{out})}\{(\sum_{k\in\mathbb{N}}\mathbf{P}^k)\mathbf{1}_n)[s]\} \leq \mathbf{M}[s]$$

Computing the best $\mathbf{m}[s]$ is straightforward.

$$\min_{\mathbf{P}\in\mathcal{M}(\mathbf{P}^-,\mathbf{P}^+,\mathbf{out})}\{(\sum_{k\in\mathbb{N}}\mathbf{P}^k)\mathbf{1}_n)[s]\} = (\sum_{k\in\mathbb{N}}(\mathbf{P}^-)^k)\mathbf{1}_n)[s]$$

Computing a bound $\mathbf{M}[s]$ via stochastic order *(Haddad, Moreaux EJOR 2007)*

- There is a unique greatest lower bound $\mathbf{P}^\bullet$ w.r.t. $\leq_{st}$ for $\mathcal{M}(\mathbf{P}^-,\mathbf{P}^+,\mathbf{out})$
- which admits a unique greatest *monotone* lower bounding matrix $\mathbf{P}^\star \leq_{st} \mathbf{P}^\bullet$.
- $\mathbf{M}[s] = (\sum_{k\in\mathbb{N}}(\mathbf{P}^\star)^k)\mathbf{1}_n)[s]$
  (different bounds are possible depending on the ordering of states)
- Furthermore a priori detecting states s for which $\mathbf{M}[s] = \infty$ can be performed in very efficient way without computing the strongly connected components of the underlying graph *(this paper)*.

Outline

IMC model

2 PCTL

Efficient Model Checking PCTL for IMCs

Conclusion and perspectives

PCTL for MCs

Syntax

$\phi ::= true \mid a \mid \phi \wedge \phi \mid \neg\phi \mid \mathcal{P}_{\lhd p}(\mathcal{X}\phi) \mid \mathcal{P}_{\lhd p}(\phi_1\ \mathcal{U}^{[\alpha,\beta]}\phi_2) \mid \mathcal{D}_{\lhd r}(\phi)$

Semantic: path formulas

A path $\sigma \equiv s_0, s_1, \ldots$ is an infinite sequence of states of the Markov chain.

- $\sigma \models \mathcal{X}\phi$ iff $s_1 \models \phi$
- $\sigma \models \phi_1 \mathcal{U} \phi_2$ iff there exists i such that $s_i \models \phi_2$ and $\forall j < i\ s_j \models \phi_1$

Semantic: state formulas

- Threshold formulas
  based on $Prob^{\mathcal{M}}(s, \varphi)$ *the probability that a random path in* $\mathcal{M}$ *starting from* s *satisfies* φ

  $$s \models \mathcal{P}_{\lhd p}(\varphi) \text{ iff } Prob^{\mathcal{M}}(s, \varphi) \lhd p$$

- Duration formulas
  based on $\mathrm{E}^{\mathcal{M}}(FTime(s, \phi))$ *the mean of the first time that a random path in* $\mathcal{M}$ *starting from* s *satisfies* ϕ

  $$s \models \mathcal{D}_{\lhd r}(\phi) \text{ iff } \mathrm{E}^{\mathcal{M}}(FTime(s, \phi)) \lhd r$$

PCTL for MCs

Syntax

$\phi ::= true \mid a \mid \phi \wedge \phi \mid \neg\phi \mid \mathcal{P}_{\lhd p}(\mathcal{X}\phi) \mid \mathcal{P}_{\lhd p}(\phi_1\ \mathcal{U}^{[\alpha,\beta]}\phi_2) \mid \mathcal{D}_{\lhd r}(\phi)$

Semantic: path formulas

A path $\sigma \equiv s_0, s_1, \ldots$ is an infinite sequence of states of the Markov chain.

- $\sigma \models \mathcal{X}\phi$ iff $s_1 \models \phi$
- $\sigma \models \phi_1 \mathcal{U} \phi_2$ iff there exists i such that $s_i \models \phi_2$ and $\forall j < i\ s_j \models \phi_1$

Semantic: state formulas

- Threshold formulas
  based on $Prob^{\mathcal{M}}(s, \varphi)$ *the probability that a random path in* $\mathcal{M}$ *starting from* s *satisfies* φ

$$s \models \mathcal{P}_{\lhd p}(\varphi) \text{ iff } Prob^{\mathcal{M}}(s, \varphi) \lhd p$$

- Duration formulas
  based on $\mathrm{E}^{\mathcal{M}}(FTime(s, \phi))$ *the mean of the first time that a random path in* $\mathcal{M}$ *starting from* s *satisfies* ϕ

$$s \models \mathcal{D}_{\lhd r}(\phi) \text{ iff } \mathrm{E}^{\mathcal{M}}(FTime(s, \phi)) \lhd r$$

PCTL for MCs

Syntax

$\phi ::= true \mid a \mid \phi \wedge \phi \mid \neg\phi \mid \mathcal{P}_{\lhd p}(\mathcal{X}\phi) \mid \mathcal{P}_{\lhd p}(\phi_1\ \mathcal{U}^{[\alpha,\beta]}\phi_2) \mid \mathcal{D}_{\lhd r}(\phi)$

Semantic: path formulas

A path $\sigma \equiv s_0, s_1, \ldots$ is an infinite sequence of states of the Markov chain.

- $\sigma \models \mathcal{X}\phi$ iff $s_1 \models \phi$
- $\sigma \models \phi_1 \mathcal{U} \phi_2$ iff there exists i such that $s_i \models \phi_2$ and $\forall j < i\ s_j \models \phi_1$

Semantic: state formulas

- Threshold formulas
  based on $Prob^{\mathcal{M}}(s,\varphi)$ the probability that a random path in $\mathcal{M}$ starting from s satisfies φ
  $$s \models \mathcal{P}_{\lhd p}(\varphi) \text{ iff } Prob^{\mathcal{M}}(s,\varphi) \lhd p$$
- Duration formulas
  based on $\mathtt{E}^{\mathcal{M}}(FTime(s,\phi))$ the mean of the first time that a random path in $\mathcal{M}$ starting from s satisfies ϕ
  $$s \models \mathcal{D}_{\lhd r}(\phi) \text{ iff } \mathtt{E}^{\mathcal{M}}(FTime(s,\phi)) \lhd r$$

PCTL for IMCs

Exact semantic

1. $\forall \mathcal{M} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)\ \mathcal{M}, s \models \phi$ *(always satisfied)*
2. $\forall \mathcal{M} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)\ \mathcal{M}, s \models \neg\phi$ *(never satisfied)*
3. $\exists \mathcal{M}, \mathcal{M}' \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)\ \mathcal{M}, s \models \phi \wedge \mathcal{M}', s \models \neg\phi$ *(sometimes satisfied and sometimes not)*

Approximate semantic induced by a semi-decisional procedure

Six possible alternative information labels for s w.r.t. ϕ

- $s.\phi = \forall^+$ when it is known that case 1 holds.
- $s.\phi = \forall^-$ when it is known that case 2 holds.
- $s.\phi = \exists^{+-}$ when it is known that case 3 holds.
- $s.\phi = \exists^+$ when it is known that cases 1 or 3 hold.
- $s.\phi = \exists^-$ when it is known that cases 2 or 3 hold.
- $s.\phi = ?$ when no information has been obtained.

PCTL for IMCs

Exact semantic

1. $\forall \mathcal{M} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)\ \mathcal{M}, s \models \phi$ *(always satisfied)*
2. $\forall \mathcal{M} \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)\ \mathcal{M}, s \models \neg\phi$ *(never satisfied)*
3. $\exists \mathcal{M}, \mathcal{M}' \in \mathcal{M}(\mathbf{P}^-, \mathbf{P}^+)\ \mathcal{M}, s \models \phi \wedge \mathcal{M}', s \models \neg\phi$
   (sometimes satisfied and sometimes not)

Approximate semantic induced by a semi-decisional procedure

Six possible alternative information labels for s w.r.t. ϕ

- $s.\phi = \forall^+$ when it is known that case 1 holds.
- $s.\phi = \forall^-$ when it is known that case 2 holds.
- $s.\phi = \exists^{+-}$ when it is known that case 3 holds.
- $s.\phi = \exists^+$ when it is known that cases 1 or 3 hold.
- $s.\phi = \exists^-$ when it is known that cases 2 or 3 hold.
- $s.\phi = ?$ when no information has been obtained.

Outline

IMC model

PCTL

3. Efficient Model Checking PCTL for IMCs

Conclusion and perspectives

General principles

First step. Split the set of states depending on:

- the current label $(\forall^{+}, \ldots)$ to be assigned to states;
- the labels of states w.r.t. the sub-formulas occurring in the formula;
- the external path operator of the formula;
- the kind of comparison $\leq, \geq$.

Second step. Build one or more sub-stochastic matrices

- by (appropriately) ordering the states inside the subsets;
- and applying an algorithm for IMC to compute the coefficients (maximizing cumulative probabilities, st-monotone glb matrix, etc.).

Third step. Perform a standard computation for Markov chains.

General principles

First step. Split the set of states depending on:

- the current label $(\forall^+, \ldots)$ to be assigned to states;
- the labels of states w.r.t. the sub-formulas occurring in the formula;
- the external path operator of the formula;
- the kind of comparison $\leq, \geq$.

Second step. Build one or more sub-stochastic matrices

- by (appropriately) ordering the states inside the subsets;
- and applying an algorithm for IMC to compute the coefficients (maximizing cumulative probabilities, st-monotone glb matrix, etc.).

Third step. Perform a standard computation for Markov chains.

General principles

First step. Split the set of states depending on:

- the current label ($\forall^+, \ldots$) to be assigned to states;
- the labels of states w.r.t. the sub-formulas occurring in the formula;
- the external path operator of the formula;
- the kind of comparison $\leq, \geq$.

Second step. Build one or more sub-stochastic matrices

- by (appropriately) ordering the states inside the subsets;
- and applying an algorithm for IMC to compute the coefficients (maximizing cumulative probabilities, st-monotone glb matrix, etc.).

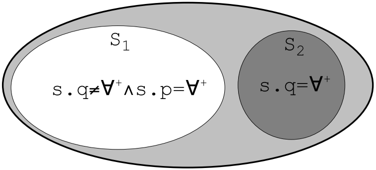
Third step. Perform a standard computation for Markov chains.

Assigning $\forall^-$ for formula $\mathcal{P}_{\leq p}(p\ \mathcal{U}^{[0,\beta]} q)$

First step.

The semi-decision procedure implies a conservative approach. Thus:

- $\mathcal{S} \setminus (\mathcal{S}_1 \cup \mathcal{S}_2) = \{s \in \mathcal{S} \mid s.p \neq \forall^+ \wedge s.q \neq \forall^+\}$ is the set of states such that one cannot assign $\forall^-$.
  (the probability of satisfaction for the random path could be 0)
- $\mathcal{S}_2 = \{s \in \mathcal{S} \mid s.q = \forall^+\}$ is the set of states such that one can surely assign $\forall^-$.
  (the probability of satisfaction for the random path is 1)
- $\mathcal{S}_1 = \{s \in \mathcal{S} \mid s.p = \forall^+ \wedge s.q \neq \forall^+\}$ is the set of states that requires a (conservative) computation.



Assigning $\forall^-$ for formula $\mathcal{P}_{\leq p}(p\ \mathcal{U}^{[0,\beta]} q)$

Second step.
What is the quantity to lower bound?
The probability to reach $\mathcal{S}_2$ from $\mathcal{S}_1$ without leaving $\mathcal{S}_1$ in at most β steps:

$$\left(\sum_{k=0}^{\beta-1} (\mathbf{P}_{|\mathcal{S}_1 \times \mathcal{S}_1})^k\right) \cdot \mathbf{r}$$

where $\mathbf{r}[s]$ is the probability to immediately reach $\mathcal{S}_2$ from s.

So we perform the following substitutions:

- Matrice $\mathbf{P}^-$ is substituted to $\mathbf{P}$.
- Vector $\mathbf{r}$ is substituted by $\mathbf{r}^- = \max(\sum_{s' \in \mathcal{S}_2} \mathbf{P}^-[s,s'], 1 - \sum_{s' \notin \mathcal{S}_2} \mathbf{P}^+[s,s'])$

Third step. Compute $\boxed{\mathbf{m} = \left(\sum_{k=0}^{\beta-1} (\mathbf{P}^-_{|\mathcal{S}_1 \times \mathcal{S}_1})^k\right) \cdot \mathbf{r}^-}$
and assign $\forall^-$ to s iff $\mathbf{m}[s] > p$.

Assigning $\forall^-$ for formula $\mathcal{P}_{\leq p}(p\ \mathcal{U}^{[0,\beta]} q)$

Second step.
What is the quantity to lower bound?
The probability to reach $\mathcal{S}_2$ from $\mathcal{S}_1$ without leaving $\mathcal{S}_1$ in at most β steps:

$$\left(\sum_{k=0}^{\beta-1} (\mathbf{P}_{|\mathcal{S}_1 \times \mathcal{S}_1})^k\right) \cdot \mathbf{r}$$

where $\mathbf{r}[s]$ is the probability to immediately reach $\mathcal{S}_2$ from s.

So we perform the following substitutions:

- Matrice $\mathbf{P}^-$ is substituted to $\mathbf{P}$.
- Vector $\mathbf{r}$ is substituted by $\mathbf{r}^- = \max(\sum_{s' \in \mathcal{S}_2} \mathbf{P}^-[s, s'], 1 - \sum_{s' \notin \mathcal{S}_2} \mathbf{P}^+[s, s'])$

Third step. Compute $\boxed{\mathbf{m} = \left(\sum_{k=0}^{\beta-1} (\mathbf{P}^-_{|\mathcal{S}_1 \times \mathcal{S}_1})^k\right) \cdot \mathbf{r}^-}$
and assign $\forall^-$ to s iff $\mathbf{m}[s] > p$.

Assigning $\forall^-$ for formula $\mathcal{P}_{\leq p}(p\ \mathcal{U}^{[0,\beta]} q)$

Second step.

What is the quantity to lower bound?

The probability to reach $\mathcal{S}_2$ from $\mathcal{S}_1$ without leaving $\mathcal{S}_1$ in at most β steps:

$$\left(\sum_{k=0}^{\beta-1} (\mathbf{P}_{|\mathcal{S}_1 \times \mathcal{S}_1})^k\right) \cdot \mathbf{r}$$

where $\mathbf{r}[s]$ is the probability to immediately reach $\mathcal{S}_2$ from s.

So we perform the following substitutions:

- Matrice $\mathbf{P}^-$ is substituted to $\mathbf{P}$.
- Vector $\mathbf{r}$ is substituted by $\mathbf{r}^- = \max(\sum_{s' \in \mathcal{S}_2} \mathbf{P}^-[s,s'], 1 - \sum_{s' \notin \mathcal{S}_2} \mathbf{P}^+[s,s'])$

Third step. Compute $\boxed{\mathbf{m} = \left(\sum_{k=0}^{\beta-1} (\mathbf{P}^-_{|\mathcal{S}_1 \times \mathcal{S}_1})^k\right) \cdot \mathbf{r}^-}$

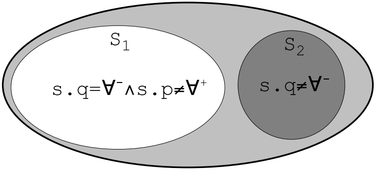
and assign $\forall^-$ to s iff $\mathbf{m}[s] > p$.

Assigning $\forall^+$ for formula $\mathcal{P}_{\leq p}(p\ \mathcal{U}^{[0,\beta]} q)$

First step.

The semi-decision procedure implies a conservative approach. Thus:

- $\mathcal{S} \setminus (\mathcal{S}_1 \cup \mathcal{S}_2) = \{s \in \mathcal{S} \mid s.p = \forall^- \wedge s.q = \forall^-\}$ is the set of states such that one can surely assign $\forall^+$.
  (the probability of satisfaction for the random path is 0)
- $\mathcal{S}_2 = \{s \in \mathcal{S} \mid s.q \neq \forall^-\}$ is the set of states such that one cannot assign $\forall^+$.
  (the probability of satisfaction for the random path could be 1)
- $\mathcal{S}_1 = \{s \in \mathcal{S} \mid s.p \neq \forall^- \wedge s.q = \forall^-\}$ is the set of states that requires a (conservative) computation.



Assigning $\forall^+$ for formula $\mathcal{P}_{\leq p}(p\ \mathcal{U}^{[0,\beta]} q)$

Second step.
We now upper bound

$$\left(\sum_{k=0}^{\beta-1}(\mathbf{P}_{|\mathcal{S}_1\times\mathcal{S}_1})^k\right)\cdot\mathbf{r}$$

So we define an appropriate $\mathcal{M}(\mathbf{P}^-,\mathbf{P}^+,\mathbf{out})$ over $\mathcal{S}_1$:

- Matrices $\mathbf{P}^+,\mathbf{P}^-$ are the original matrices restricted to $\mathcal{S}_1$.
- Vector $\mathbf{out}$ is defined by:
  $\mathbf{out}[s]=\max(\sum_{s'\notin\mathcal{S}_1}\mathbf{P}^-[s,s'],1-\sum_{s'\in\mathcal{S}_1}\mathbf{P}^+[s,s'])$
- Moreover we upper bound $\mathbf{r}$ by
  $\mathbf{r}^+=\min(\sum_{s'\in\mathcal{S}_2}\mathbf{P}^+[s,s'],1-\sum_{s'\notin\mathcal{S}_2}\mathbf{P}^-[s,s'])$

Warning In order to apply stochastic bound, $\mathbf{r}^+$ must be decreasing. So it implies a re-ordering of states of $\mathcal{S}_1$ before computing $\mathbf{P}^\star$.

Third step. Compute $\boxed{\mathbf{M}=\left(\sum_{k=0}^{\beta-1}(\mathbf{P}^\star)^k\right)\cdot\mathbf{r}^+}$

and assign $\forall^+$ to s iff $\mathbf{M}[s]\leq p$.

Assigning $\forall^+$ for formula $\mathcal{P}_{\leq p}(p\ \mathcal{U}^{[0,\beta]} q)$

Second step.
We now upper bound

$$\left(\sum_{k=0}^{\beta-1} (\mathbf{P}_{|\mathcal{S}_1 \times \mathcal{S}_1})^k\right) \cdot \mathbf{r}$$

So we define an appropriate $\mathcal{M}(\mathbf{P}^-, \mathbf{P}^+, \mathbf{out})$ over $\mathcal{S}_1$:

- Matrices $\mathbf{P}^+, \mathbf{P}^-$ are the original matrices restricted to $\mathcal{S}_1$.
- Vector $\mathbf{out}$ is defined by:
  $\mathbf{out}[s] = \max(\sum_{s' \notin \mathcal{S}_1} \mathbf{P}^-[s,s'], 1 - \sum_{s' \in \mathcal{S}_1} \mathbf{P}^+[s,s'])$
- Moreover we upper bound $\mathbf{r}$ by
  $\mathbf{r}^+ = \min(\sum_{s' \in \mathcal{S}_2} \mathbf{P}^+[s,s'], 1 - \sum_{s' \notin \mathcal{S}_2} \mathbf{P}^-[s,s'])$

Warning In order to apply stochastic bound, $\mathbf{r}^+$ must be decreasing. So it implies a re-ordering of states of $\mathcal{S}_1$ before computing $\mathbf{P}^\star$.

Third step. Compute $\boxed{\mathbf{M} = \left(\sum_{k=0}^{\beta-1} (\mathbf{P}^\star)^k\right) \cdot \mathbf{r}^+}$

and assign $\forall^+$ to s iff $\mathbf{M}[s] \leq p$.

Assigning $\forall^+$ for formula $\mathcal{P}_{\leq p}(p\ \mathcal{U}^{[0,\beta]} q)$

Second step.
We now upper bound

$$\left(\sum_{k=0}^{\beta-1} (\mathbf{P}_{|\mathcal{S}_1 \times \mathcal{S}_1})^k\right) \cdot \mathbf{r}$$

So we define an appropriate $\mathcal{M}(\mathbf{P}^-, \mathbf{P}^+, \mathbf{out})$ over $\mathcal{S}_1$:

- Matrices $\mathbf{P}^+, \mathbf{P}^-$ are the original matrices restricted to $\mathcal{S}_1$.
- Vector $\mathbf{out}$ is defined by:
  $\mathbf{out}[s] = \max(\sum_{s' \notin \mathcal{S}_1} \mathbf{P}^-[s, s'], 1 - \sum_{s' \in \mathcal{S}_1} \mathbf{P}^+[s, s'])$
- Moreover we upper bound $\mathbf{r}$ by
  $\mathbf{r}^+ = \min(\sum_{s' \in \mathcal{S}_2} \mathbf{P}^+[s, s'], 1 - \sum_{s' \notin \mathcal{S}_2} \mathbf{P}^-[s, s'])$

Warning In order to apply stochastic bound, $\mathbf{r}^+$ must be decreasing. So it implies a re-ordering of states of $\mathcal{S}_1$ before computing $\mathbf{P}^\star$.

Third step. Compute $\boxed{\mathbf{M} = \left(\sum_{k=0}^{\beta-1} (\mathbf{P}^\star)^k\right) \cdot \mathbf{r}^+}$
and assign $\forall^+$ to s iff $\mathbf{M}[s] \leq p$.

Assigning $\exists^+$ for formula $\mathcal{P}_{\leq p}(p\ \mathcal{U}^{[0,\beta]} q)$

First step as in the previous case.

Second step.

Here we guess one (or more) matrix $\mathbf{P}$ with a small value of:

$$\left(\sum_{k=0}^{\beta-1}(\mathbf{P}_{|\mathcal{S}_1\times\mathcal{S}_1})^k\right)\cdot\mathbf{r}$$

- We order the states of $\mathcal{S}$: first $\mathcal{S}_2$ then $\mathcal{S}_1$ and $\mathcal{S}\setminus(\mathcal{S}_1\cup\mathcal{S}_2)$
- Inside S_1, order the states w.r.t. $\mathbf{r}[s]=\max(\sum_{s'\in\mathcal{S}_2}\mathbf{P}^+[s,s'],1-\sum_{s'\notin\mathcal{S}_2}\mathbf{P}^+[s,s'])$
- Build $\mathbf{P}$ by minimizing the transition probabilities following that order.

Warning All the choices above are heuristics and should be tuned by experiments.

Third step. Compute $\boxed{\mathbf{M}=\left(\sum_{k=0}^{\beta-1}(\mathbf{P}_{|\mathcal{S}_1\times\mathcal{S}_1})^k\right)\cdot\mathbf{r}}$

and assign $\exists^+$ to s iff $\mathbf{m}[s]\leq p$.

Assigning $\exists^+$ for formula $\mathcal{P}_{\leq p}(p\ \mathcal{U}^{[0,\beta]} q)$

First step as in the previous case.

Second step.

Here we guess one (or more) matrix $\mathbf{P}$ with a small value of:

$$\left(\sum_{k=0}^{\beta-1}(\mathbf{P}_{|\mathcal{S}_1\times\mathcal{S}_1})^k\right)\cdot\mathbf{r}$$

- We order the states of $\mathcal{S}$: first $\mathcal{S}_2$ then $\mathcal{S}_1$ and $\mathcal{S}\setminus(\mathcal{S}_1\cup\mathcal{S}_2)$
- Inside S_1, order the states w.r.t. $\mathbf{r}[s] = \max(\sum_{s'\in\mathcal{S}_2}\mathbf{P}^+[s,s'], 1-\sum_{s'\notin\mathcal{S}_2}\mathbf{P}^+[s,s'])$
- Build $\mathbf{P}$ by minimizing the transition probabilities following that order.

Warning All the choices above are heuristics and should be tuned by experiments.

Third step. Compute $\boxed{\mathbf{M} = \left(\sum_{k=0}^{\beta-1}(\mathbf{P}_{|\mathcal{S}_1\times\mathcal{S}_1})^k\right)\cdot\mathbf{r}}$

and assign $\exists^+$ to s iff $\mathbf{m}[s]\leq p$.

Assigning $\exists^+$ for formula $\mathcal{P}_{\leq p}(p\ \mathcal{U}^{[0,\beta]} q)$

First step as in the previous case.

Second step.

Here we guess one (or more) matrix $\mathbf{P}$ with a small value of:

$$\left(\sum_{k=0}^{\beta-1}(\mathbf{P}_{|\mathcal{S}_1\times\mathcal{S}_1})^k\right)\cdot\mathbf{r}$$

- We order the states of $\mathcal{S}$: first $\mathcal{S}_2$ then $\mathcal{S}_1$ and $\mathcal{S}\setminus(\mathcal{S}_1\cup\mathcal{S}_2)$
- Inside S_1, order the states w.r.t. $\mathbf{r}[s]=\max(\sum_{s'\in\mathcal{S}_2}\mathbf{P}^+[s,s'],1-\sum_{s'\notin\mathcal{S}_2}\mathbf{P}^+[s,s'])$
- Build $\mathbf{P}$ by minimizing the transition probabilities following that order.

Warning All the choices above are heuristics and should be tuned by experiments.

Third step. Compute $\boxed{\mathbf{M}=\left(\sum_{k=0}^{\beta-1}(\mathbf{P}_{|\mathcal{S}_1\times\mathcal{S}_1})^k\right)\cdot\mathbf{r}}$

and assign $\exists^+$ to s iff $\mathbf{m}[s]\leq p$.

Outline

Conclusion and perspectives

Summary of results

- Efficient semi-decision procedure for model checking IMCs
- Application of stochastic comparisons for model checking PCTL over IMCs
- Handling the interval constrained until and the mean reachability time operators
- Providing partial answers $\exists^+$, $\exists^-$

Perspectives

- Development of a prototype for high level formalisms with IMC as possible semantic
- Accuracy of bounds and impact of heuristics
- One year post-doc position available for this project