Model Checking Reading Group

Qualitative properties of Markov Chains (10.1.2.)

Louis Rustenholz

30 July 2021

Introduction

Where are we ?

Chapter 10: Model checking of Probabilistic Systems

10.1. Markov Chains

- Markov Chains. Examples.

$$M = (S, \mathrm{P}, \iota_{\text{init}}, AP)$$

- Measure theory, probability spaces, cylinder sets.

$$\mathrm{Cyl}(\hat{\pi}) = \{\pi \in \mathrm{Paths}(\mathcal{M}) \mid \hat{\pi} \in \mathrm{pref}(\pi)\}$$

Where are we ?

Chapter 10: Model checking of probabilistic systems

10.1.1. Reachability probabilities

- Reachability, Constrained Reachability (Until), Bounded Until.

$$\Pr(s \models \Diamond B), \Pr(s \models C \, \mathsf{U} \, B), \Pr(s \models C \, \mathsf{U}^{\leq n} B)$$

- Measurability. Computation by infinite sums.
- Linear systems and least fixed-point characterization.

$$x = Ax + b$$

- Unique fixed-point theorem, with a good partition.

$$S = S_{=0} \sqcup S_{?} \sqcup S_{=1}.$$

- Iterations of transition matrix P.

This week

Chapter 10: Model checking of probabilistic systems

10.1.2. Qualitative properties.

- Checking whether $\Pr(s \vDash \varphi) = 0$ or 1.
- Limit behaviour of MCs.
- Graph algorithms, BSCC.
- Linear time algorithms for qualitative properties.
- Polynomial time algorithms for quantitative properties.

- Build on reachability probabilities computed last week.
- Prepare the theory for model-checking of general formulas in the following weeks.

Following weeks

Chapter 10: Model checking of probabilistic systems

10.2. PCTL

- A branching time logic with probabilities. Boolean truth values.
- Measurability.
- PCTL model-checking.
- Comparison between qualitative fragment of PCTL and CTL.

10.3. LTL

- Probabilistic truth values of classical LTL formulas.

Qualitative properties

Qualitative properties

- We want efficient model-checking for *almost sure* events.
- This can be done in *finite* MCs, using graph algorithms.

Examples of properties

In this subsection, measurability of events is checked by hand.
Tools: increasing/decreasing sequences of events, sums of null sets.

- Reachability, Until, Bounded Until.

$$\Diamond B,\ C \,\mathsf{U}\, B,\ C \,\mathsf{U}^{\leq n} B$$

- Repeated reachability. Can this happen infinitely many times ?

$$\Box\Diamond B$$

- Persistence. Is this a constant at infinity ?

$$\Diamond\Box B$$

Fairness of randomness

Limit behaviour of MCs (1)

Theorem (Fairness)

For any MC $\mathcal{M}$, $s, t \in S$,

$$Pr^{\mathcal{M}}(s \models \Box\Diamond t) = Pr_s^{\mathcal{M}}\Big(\bigwedge_{\hat{\pi}\in Paths_{fin}(t)} \Box\Diamond\hat{\pi}\Big).$$

"If t happens infinitely often, anything *finite* that *may* happen after t *does* happen infinitely often."

Proof.

Usual fact in probability theory.
Prove it with monotonous limits and countable unions of null sets. $\square$

Limit behaviour of MCs (1)

Theorem (Fairness)

For any MC $\mathcal{M}$, $s, t \in S$,

$$Pr^{\mathcal{M}}(s \vDash \Box\Diamond t) = Pr_s^{\mathcal{M}}\Big(\bigwedge_{\hat{\pi} \in Paths_{fin}(t)} \Box\Diamond\hat{\pi} \Big).$$

"If t happens infinitely often, anything *finite* that *may* happen after t *does* happen infinitely often."

Corollary

$$Pr\Big(s \vDash \bigwedge_{t \in S} \bigwedge_{u \in Post^*(t)} (\Box\Diamond t \to \Box\Diamond u)\Big) = 1.$$

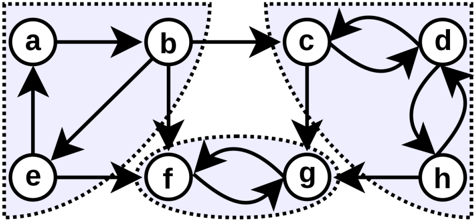
NB: in a *finite* Markov Chain, $Pr\big(s \vDash \bigvee_{t \in S} \Box\Diamond t\big) = 1$!

BSCC

Graph notations for MCs

Consider $\mathcal{M} = (S, \mathrm{P}, \iota_{\text{init}}, AP)$ a MC.

- Underlying digraph (forget probabilities). $1_{>0} : [0,1] \to \{\perp, \top\}$.
- *Strongly connected subset*. $T \subset S, \forall t \in T,\ T \subset Post^*(t)$.
- Strongly connected *component* (SCC) if it is maximal.
- *Bottom strongly connected component* (BSCC),
  if we stay there almost surely, i.e. $\forall t \in T$, $\mathrm{P}(t, T) = 1$.



Limit behaviour of MCs (2)

Theorem

For any finite MC $\mathcal{M}$ and $s \in \mathcal{M}$,

$$Pr_s^{\mathcal{M}}\{\pi \in Paths(s) \,|\, \inf(\pi) \in BSCC(\mathcal{M})\} = 1.$$

Proof.

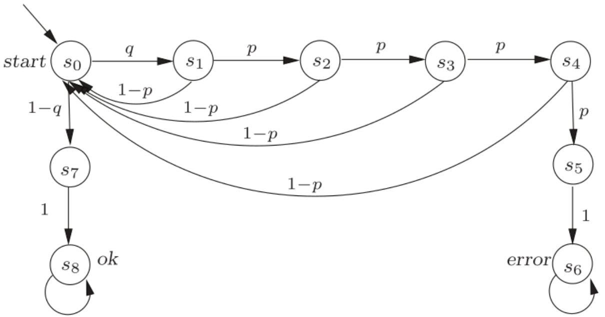
Corollary of fairness theorem. □

"*Almost surely*, any run ends up in a BSCC and visits all of its states infinitely often."

- BSCC decomposition can be computed efficiently.
- This allows for fast verification with graph analysis.

Examples of BSCC decomposition

Zeroconf protocol

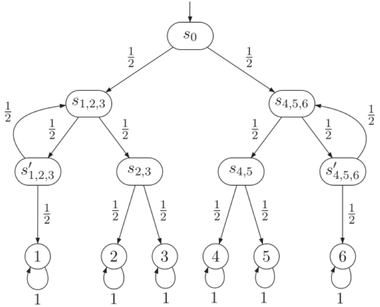


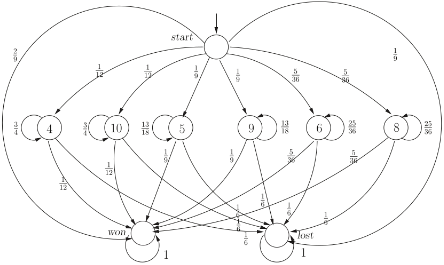
$$BSCC(\mathcal{M}) = \{\{s_6\}, \{s_8\}\}$$

An operator *almost never* asks infinitely many times for a new address.

Examples of BSCC decomposition

Similarly, absorbing states are reached almost surely for Knuth and Yao's die and in craps game.

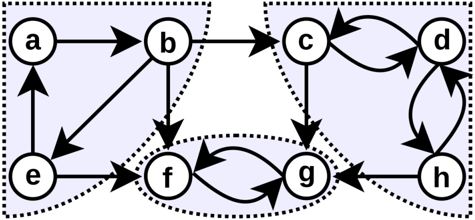


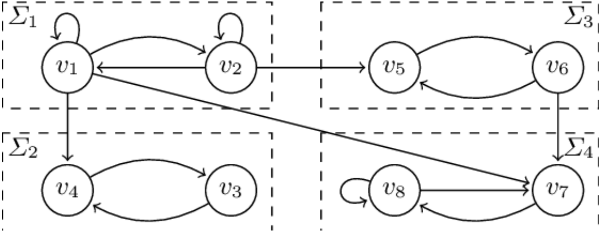


Notice that there are SCC which are not BSCC !

Examples of BSCC decomposition

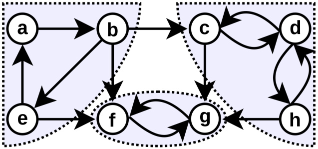
Of course, BSCCs may be larger than single absorbing states.





Computing (B)SCC decompositions

Computing a decomposition in SCCs can be done in $O(|\mathcal{M}|)$, with two DFS, one in the graph G and one in G^{op} (Kosaraju's algorithm).
Eliminating SCCs that are not BSCCs is also easy.



Many other algorithms exist. Optimizing this (optimizing the constant, for parallelism, ...) is a vast subject.
(Note that $|\mathcal{M}| = E + V$.)

Applications

Application: Almost Sure Reachability

Theorem

Let $\mathcal{M}$ be a finite MC with state space S, $s \in S$ and $B \subset S$ a set of absorbing states.

$$Pr(s \vDash \Diamond B) = 1 \iff s \in S \setminus Pre^*(S \setminus Pre^*(B)).$$

Proof.

$\Rightarrow$ is easy. $\Leftarrow$ comes from looking at BSCCs. □

$$\{s \in S \mid Pr(s \vDash \Diamond B) = 1\}$$

can thus be computed in $O(|\mathcal{M}|)$ in the following way.

- Turn $\mathcal{M}$ into a new $\mathcal{M}_B$ where all $s \in B$ are absorbing.
- Do two backward searches in the underlying digraph of $\mathcal{M}_B$.

Application: Qualitative Constrained Reachability

Let $\mathcal{M}$ be a finite MC with state space S, $B, C \subset S$. The sets

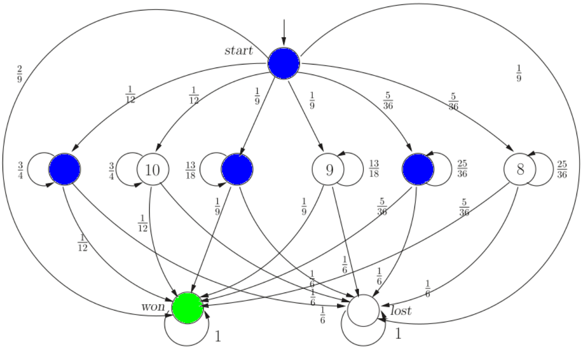
$$S_{=0} = \{s \in S \mid Pr(s \vDash C \,\mathrm{U}\, B) = 0\},\ S_{=1} = \{s \in S \mid Pr(s \vDash C \,\mathrm{U}\, B) = 1\}$$

can be computed in $O(|\mathcal{M}|)$.

- States *almost never* reached are (really) *never* reached. Compute (the complement of) $S_{=0}$ by a backward analysis starting from B-states.
- For $S_{=1}$, turn $\mathcal{M}$ into a new $\mathcal{M}'$ where all $s \in B \cup S \setminus (C \cup B)$ are absorbing, and compute almost sure reachability.

Example – Qualitative Constrained Reachability

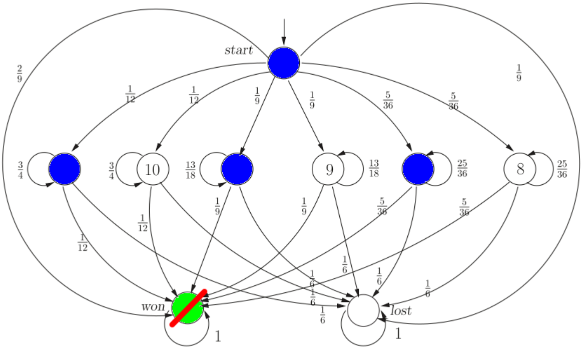
Consider the case of craps game, $B = \{\text{won}\}$, $C = \{\text{start}, 4, 5, 6\}$.



For $(Pr(s \models C \cup B) = 0)_s$, backward analysis in the original graph.
For $(Pr(s \models C \cup B) = 1)_s$, double backward analysis in a modified graph.

Example – Qualitative Constrained Reachability

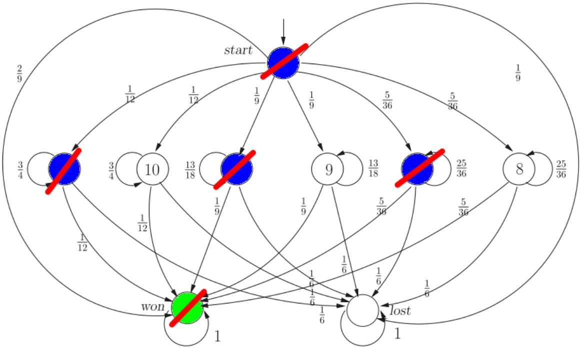
Craps game, $B = \{\text{won}\}$, $C = \{\text{start}, 4, 5, 6\}$.



$$S_{=0} = S \setminus Sat(\exists(C \cup B))$$

Example – Qualitative Constrained Reachability

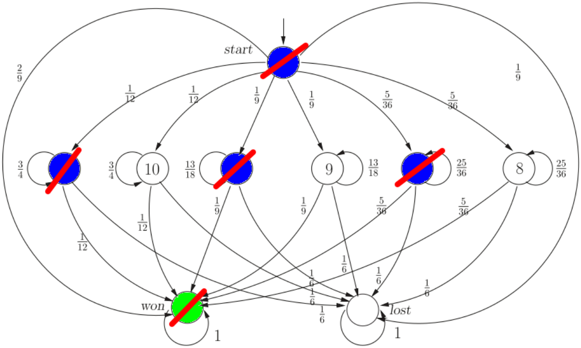
Craps game, $B = \{\mathrm{won}\}$, $C = \{\mathrm{start}, 4, 5, 6\}$.



$$S_{=0} = S \setminus Sat(\exists(C \cup B))$$

Example – Qualitative Constrained Reachability

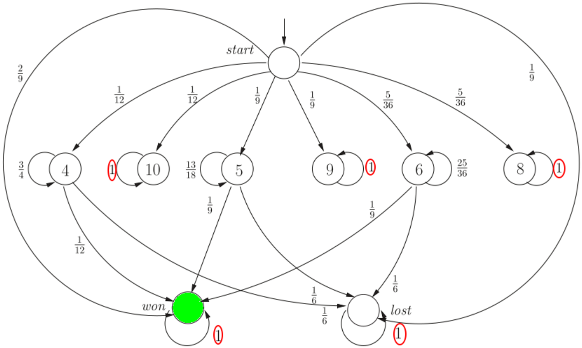
Craps game, $B = \{\text{won}\}$, $C = \{\text{start}, 4, 5, 6\}$.



$$S_{=0} = S \setminus Sat(\exists(C \cup B))$$
$$= \{\text{lost}, 8, 9, 10\}$$

Example – Qualitative Constrained Reachability

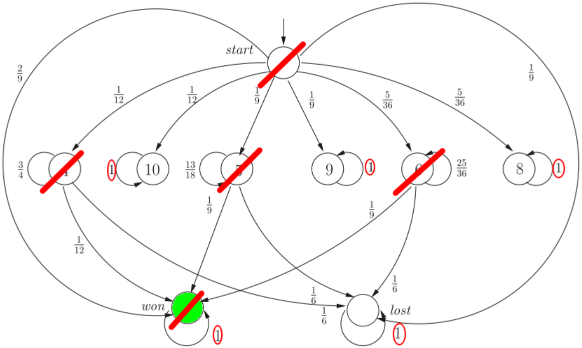
Craps game, $B = \{\mathrm{won}\}$, $C = \{\mathrm{start}, 4, 5, 6\}$.



$$S_{=1} = S \setminus Pre^*(S \setminus Pre^*(B))$$

Example – Qualitative Constrained Reachability

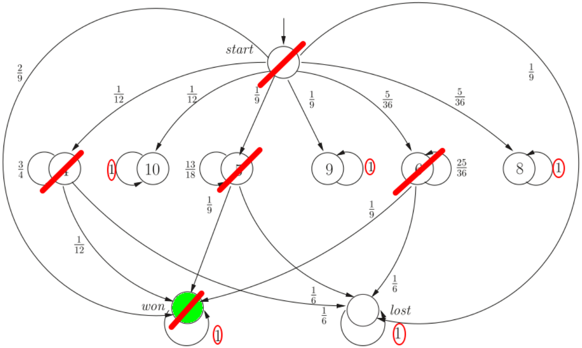
Craps game, $B = \{\text{won}\}$, $C = \{\text{start}, 4, 5, 6\}$.



$$S_{=1} = S \setminus Pre^*(S \setminus Pre^*(B))$$

Example – Qualitative Constrained Reachability

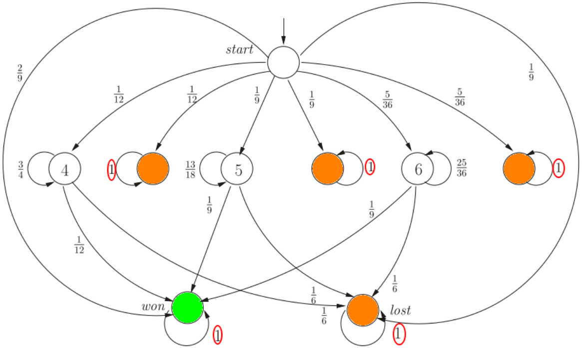
Craps game, $B = \{\text{won}\}$, $C = \{\text{start}, 4, 5, 6\}$.



$$S_{=1} = S \setminus Pre^*(S \setminus Pre^*(B))$$
$$= S \setminus Pre^*\{\text{lost}, 8, 9, 10\}$$

Example – Qualitative Constrained Reachability

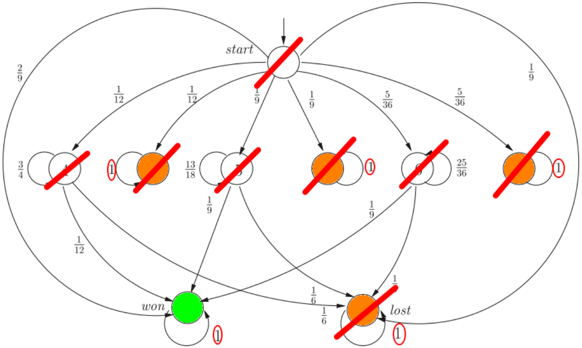
Craps game, $B = \{\mathrm{won}\}$, $C = \{\mathrm{start}, 4, 5, 6\}$.



$$S_{=1} = S \setminus Pre^*(S \setminus Pre^*(B))$$
$$= S \setminus Pre^*\{\mathrm{lost}, 8, 9, 10\}$$

Example – Qualitative Constrained Reachability

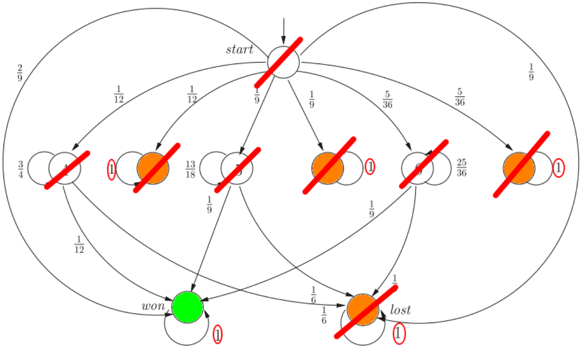
Craps game, $B = \{\mathrm{won}\}$, $C = \{\mathrm{start}, 4, 5, 6\}$.



$$S_{=1} = S \setminus Pre^*(S \setminus Pre^*(B))$$
$$= S \setminus Pre^*\{\mathrm{lost}, 8, 9, 10\}$$

Example – Qualitative Constrained Reachability

Craps game, $B = \{\text{won}\}$, $C = \{\text{start}, 4, 5, 6\}$.



$$S_{=1} = S \setminus Pre^*(S \setminus Pre^*(B))$$
$$= S \setminus Pre^*\{\text{lost}, 8, 9, 10\} = \{\text{won}\}$$

Application: Qualitative Repeated Reachability

Theorem

Let $\mathcal{M}$ be a finite MC, $s \in S$, $B \subset S$.

$$Pr(s \models \Box\Diamond B) = 1 \iff T \cap B \neq \varnothing \text{ for each BSCC } T \text{ reachable from } s.$$

Proof.

Consequence of our BSCC theorem. $\square$

$$\{s \in S \mid Pr(s \models \Box\Diamond B) = 1\}$$

can thus be computed in $O(|\mathcal{M}|)$ in the following way.

- Compute $BSCC(\mathcal{M})$ in $O(|\mathcal{M}|)$ (while marking all T such that $T \cap B \neq \varnothing$).
- Compute the union U of all $T \in BSCC(\mathcal{M})$ such that $T \cap B \neq \varnothing$.
- Compute $S \setminus Pre^*(S \setminus Pre^*(U))$ by backward analysis.

Application: Quantitative Repeated Reachability

Corollary

Let $\mathcal{M}$ be a finite MC, $s \in S$, $B \subset S$, and U be the union of all $T \in BSCC(\mathcal{M})$ such that $B \cap T \neq \varnothing$.

$$Pr(s \vDash \Box\Diamond B) = Pr(s \vDash \Diamond U)$$

$$s \mapsto Pr(s \vDash \Box\Diamond B)$$

can thus be computed in $O(\mathrm{Pol}(|\mathcal{M}|))$ in the following way.

- Compute $BSCC(\mathcal{M})$ in $O(|\mathcal{M}|)$ (while marking all T such that $T \cap B \neq \varnothing$).
- Compute the union U of $T \in BSCC(\mathcal{M})$ such that $T \cap B \neq \varnothing$.
- Compute $(Pr(s \vDash U))_s$, e.g. by solving a linear system.

Application: Persistence

Theorem

Let $\mathcal{M}$ be a finite MC, $s \in S$, $B \subset S$, and U be the union of all $T \in BSCC(\mathcal{M})$ such that $B \subset T$.

$$Pr(s \models \Box\Diamond B) = 1 \iff Pr(s \models \Diamond U) = 1$$

$$Pr(s \models \Box\Diamond B) = Pr(s \models \Diamond U)$$

This gives a linear time algorithm for qualitative persistence, and a polynomial time algorithm for quantitative persistence.
The same kind of techniques can be used for various other properties.

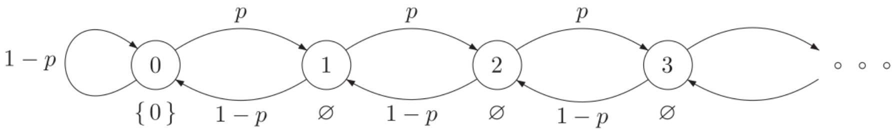
Conclusion

Infinite Markov Chains

Conclusion:

For *finite* Markov Chains, *qualitative properties* *don't* depend on probability transitions !

This is not the case for *infinite* Markov Chains.



Conclusion

For *finite* Markov Chains, *qualitative properties* *don't* depend on probability transitions !

- Anything that *may* happen after something that happens infinitely often *does* happens infinitely often.
- Every run finishes in a *BSCC*.
- $BSCC(\mathcal{M})$ can be computed in $O(|\mathcal{M}|)$.
- Qualitative properties (like reachability, repeated reachability, persistence, ...) can be checked in linear time.
- Quantitative versions can be checked in polynomial time.

More generic solutions will be studied in section 10.2. about PCTL.