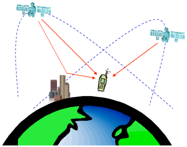
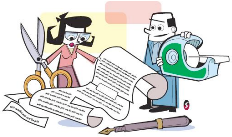
# Probabilistic model checking from finite to parameterized systems

Nathalie Bertrand

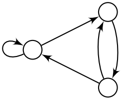
SuMo, Inria Rennes

GT Vérif 17-18 Juin 2013

# What is probabilistic model checking?

Does  satisfy  ?

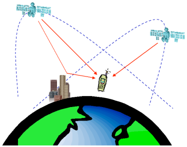
system | specification

 $\models$ $\varphi$ ?

model | formula

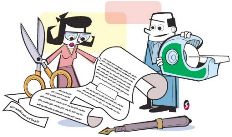
# What is probabilistic model checking?

How much does



system

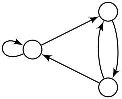
satisfy



specification

?

$\mathbb{P}$ (



model

$\models$

$\varphi$ ) $=$ $p$ ?

formula

1. Finite probabilistic systems
   - Finite Markov chains
   - Finite Markov decision processes

2. Infinite probabilistic systems with a finite attractor
   - Infinite MC with a finite attractor
   - Infinite MDP with a finite attractor
   - Computability of fixpoints

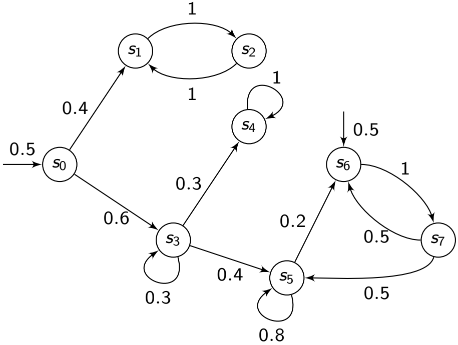
3. Towards parameterized probabilistic systems

1. Finite probabilistic systems
   - Finite Markov chains
   - Finite Markov decision processes

2. Infinite probabilistic systems with a finite attractor
   - Infinite MC with a finite attractor
   - Infinite MDP with a finite attractor
   - Computability of fixpoints

3. Towards parameterized probabilistic systems

# Finite discrete-time Markov chains




## Finite discrete-time MC

$\mathcal{M} = (S, \mathbf{P}, \mu_0)$ where

- $S$ is a finite set of states,
- $\mathbf{P} : S \times S \to [0,1]$ is a probabilistic transition function

$$\forall s \in S, \ \sum_{t \in S} \mathbf{P}(s,t) = 1 \ ,$$

- $\mu_0 : S \to [0,1]$ is the initial distribution: $\sum_{s \in S} \mu_0(s) = 1$.

# Qualitative reachability analysis

Questions

- Is a target set $T$ reachable with positive probability?
- with probability 1?

Solutions: **graph-based algorithms**

- $\mathbb{P}(\Diamond T) > 0$ iff $T$ is reachable from some initial state ($s_0$ s.t. $\mu_0(s_0) > 0$).
- $\mathbb{P}(\Diamond T) = 1$ iff making states in $T$ absorbing, for every initial state, each reachable bottom strongly connected component is a state of $T$.

# Quantitative reachability analysis

## Question

What is the probability of reaching a target set?

Solution: **resolution of linear equation system**

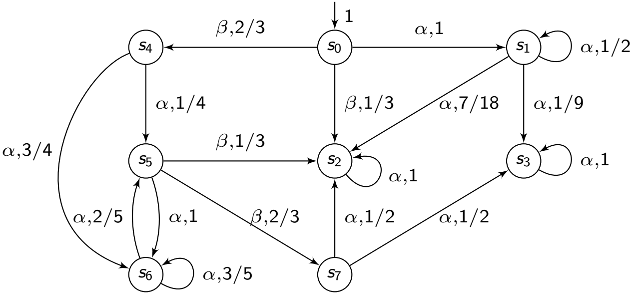
variable $x_s$ represents the probability to reach $T$ from $s$

$$\begin{cases} x_s = 1 \text{ if } s \in T \\ x_s = 0 \text{ if } s \not\xrightarrow{*} T \\ x_s = \sum_{t \in S} \mathbf{P}(s,t)\ x_t \end{cases}$$

Solution vector: $(p_s)_{s \in S}$

$\mathbb{P}(\Diamond T) = \sum_{s \in S} \mu_0(s) \cdot p_s$

# Discrete-time Markov decision processes



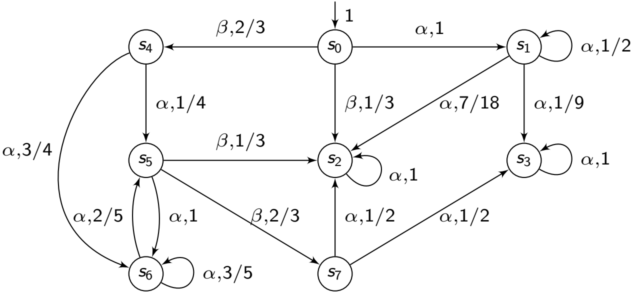

## Finite discrete-time MDP

$\mathcal{P} = (S, \mathbf{P}, Act, \mu_0)$ where

- $Act$ is a finite set of actions
- $\mathbf{P} : S \times Act \times S \to [0,1]$ is a **partial** probabilistic transition function

$$\forall s \in S,\ \forall \alpha \in Act,\ \sum_{t \in S} \mathbf{P}(s, \alpha, t) \in \{0, 1\} \ .$$

# Scheduler




Starting in $s_0$, what is the probability to eventually reach $s_4$? It depends!

## Scheduler

A scheduler $\sigma : S^+ \to Act$ resolves the nondeterminism among actions based on the history of states visited so far.

▷ $\sigma(s_0) = \beta$, $\sigma(*s_4s_5) = \alpha$, $\sigma(*s_6s_5) = \beta$ etc.

# Qualitative reachability analysis

Questions

- Is the max (resp. min) reachability probability positive?
- equal to 1?

Solutions: **(more involved) graph-based algorithms**

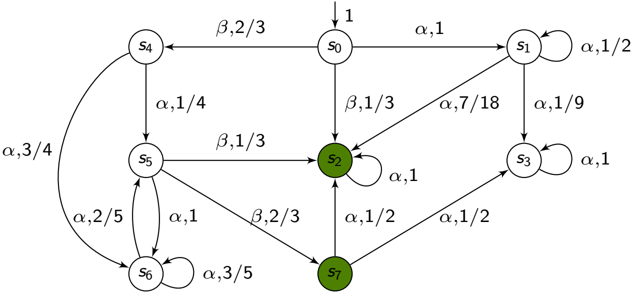
To compute the set of states from which $\max_\sigma \mathbb{P}_\sigma(\Diamond T) = 1$: Iteratively

- remove bad states = states that cannot reach the target $T$
- remove actions leading to bad states with positive probability

# Qualitative reachability analysis: example

To compute the set of states from which $\max_\sigma \mathbb{P}_\sigma(\Diamond T) = 1$: Iteratively

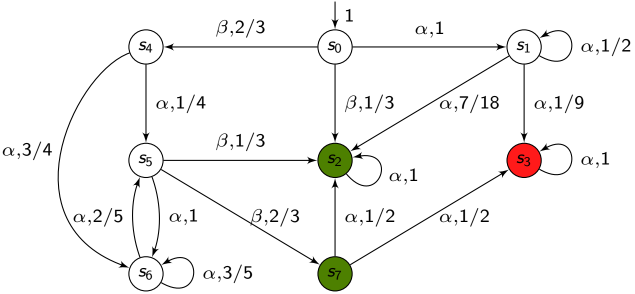
- remove bad states = states that cannot reach the target $T$
- remove actions leading to bad states with positive probability



# Qualitative reachability analysis: example

To compute the set of states from which $\max_\sigma \mathbb{P}_\sigma(\Diamond T) = 1$: Iteratively

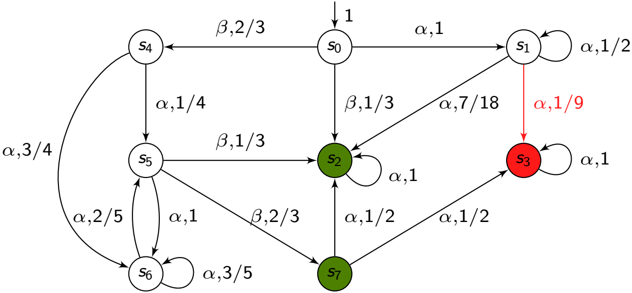
- remove bad states = states that cannot reach the target $T$
- remove actions leading to bad states with positive probability



# Qualitative reachability analysis: example

To compute the set of states from which $\max_\sigma \mathbb{P}_\sigma(\Diamond T) = 1$: Iteratively

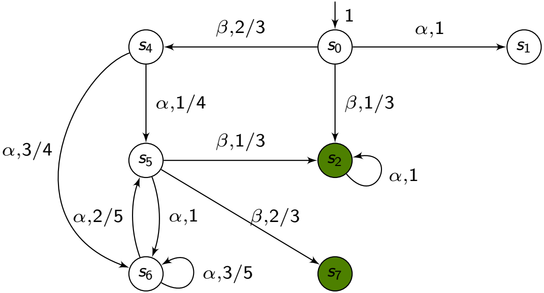
- remove bad states = states that cannot reach the target $T$
- remove actions leading to bad states with positive probability



# Qualitative reachability analysis: example

To compute the set of states from which $\max_\sigma \mathbb{P}_\sigma(\diamond T) = 1$: Iteratively

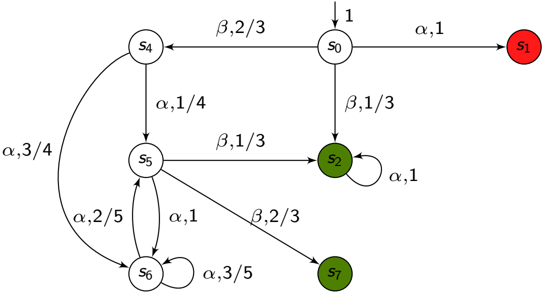
- remove bad states = states that cannot reach the target $T$
- remove actions leading to bad states with positive probability



# Qualitative reachability analysis: example

To compute the set of states from which $\max_\sigma \mathbb{P}_\sigma(\Diamond T) = 1$: Iteratively

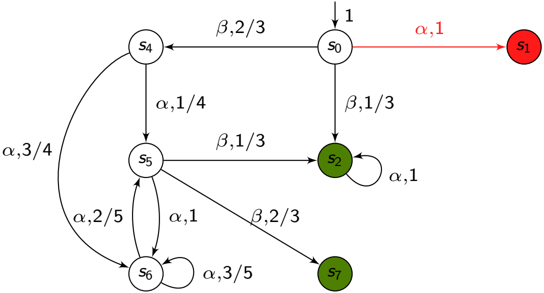
- remove bad states = states that cannot reach the target $T$
- remove actions leading to bad states with positive probability



# Qualitative reachability analysis: example

To compute the set of states from which $\max_\sigma \mathbb{P}_\sigma(\Diamond T) = 1$: Iteratively

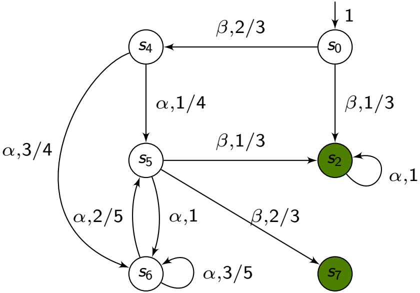
- remove bad states = states that cannot reach the target $T$
- remove actions leading to bad states with positive probability



# Qualitative reachability analysis: example

To compute the set of states from which $\max_\sigma \mathbb{P}_\sigma(\Diamond T) = 1$: Iteratively

- remove bad states = states that cannot reach the target $T$
- remove actions leading to bad states with positive probability



# Quantitative reachability analysis

Question

What is the max (resp. min) reachability probability?

Solution: **resolution of a linear program**

variable $x_s$ represents the maximum probability to reach $T$ from $s$

$$\begin{cases} x_s = 1 \text{ if } s \in T \\ x_s = 0 \text{ if } s \not\xrightarrow{*} T \\ x_s = \max_{\alpha \in Act} \sum_{t \in S} \mathbf{P}(s, \alpha, t)\ x_t \end{cases}$$

Solution vector: $(p_s)_{s \in S}$

$\max_\sigma \mathbb{P}_\sigma(\Diamond T) = \sum_{s \in S} \mu_0(s) \cdot p_s$

1. Finite probabilistic systems
   - Finite Markov chains
   - Finite Markov decision processes

2. Infinite probabilistic systems with a finite attractor
   - Infinite MC with a finite attractor
   - Infinite MDP with a finite attractor
   - Computability of fixpoints

3. Towards parameterized probabilistic systems

# Attractors in Markov chains

## Attractor

An attractor in a Markov Chain $\mathcal{M}$ is a set $W \subseteq S$ of states that is visited almost surely from any starting state:

$$\forall s_0,\ \mathbb{P}(s_0 \models \Diamond W) = 1 \ .$$

Examples of MC admitting **finite** attractors

- Finite Markov chains
- Random walk on $\mathbb{N}$ with $p_{\text{left}} > \frac{1}{2}$
- Markov chain induced by probabilistic lossy channel systems

## Property

If $W$ is an attractor, then $\forall s_0,\ \mathbb{P}(s_0 \models \Box\Diamond W) = 1 \ .$

- The states composing an attractor need not be recurrent.
- The attractor need not be absorbing.

# Qualitative reachability analysis

Hypothesis: $\mathcal{M}$ Markov chain with a finite attractor

## Questions

- Is a target set reachable with positive probability?
- with probability 1?

**Solutions: graph-based algorithms**

- $\mathbb{P}(s \models \Diamond T) > 0 \quad \text{iff} \quad s \xrightarrow{*} T$
- $\mathbb{P}(s \models \Diamond T) = 1 \quad \text{iff} \quad s \in \nu X.\ \mu Y.\ T \cup \big(Pre(Y) \cap \widetilde{Pre}(X)\big)$

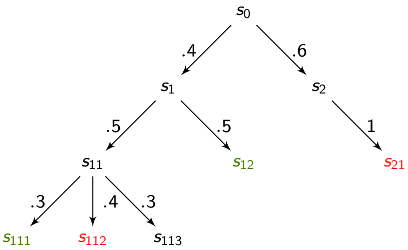
  Greatest set $X$ of states from which
  - $T$ can be reached with positive probability
  - while being sure to stay in $X$

issue: decidability of $s \xrightarrow{*} T$? computability of $\text{Pre}^*(T)$?
computability of fixpoint terms?

# Quantitative reachability analysis

**Question**
What is the probability of reaching a target set?

Solution: **approximation algorithm**




unfolding $\mathcal{M}$ from $s_0$

- ▷ $\mathbb{P}^k_\top$ probability to reach $T$ within $k$ steps
- ▷ $\mathbb{P}^k_\bot$ probability to reach $S \setminus \mathsf{Pre}^*(T)$ within $k$ steps
- ▷ $\mathbb{P}^k_\top \leq \mathbb{P}(s_0 \models \Diamond T) \leq 1 - \mathbb{P}^k_\bot$

Consequence of finite attractor property: $\lim_{k\to\infty} \mathbb{P}^k_\top = \lim_{k\to\infty} \mathbb{P}^k_\bot$

# Attractors in MDP

## Finite attractor

$W \subseteq S$ is a **finite attractor** for the MDP $\mathcal{P}$ if $W$ is finite and for every policy $\sigma$, $W$ is an attractor in the Markov chain $\mathcal{P}_\sigma$.

Examples of MDP admitting **finite** attractors

- Finite Markov decision processes
- Markov decision process induced by nondeterministic lossy channel systems with probabilistic losses

## Property

If $W$ is an attractor, then $\forall\sigma,\ \forall s_0,\ \mathbb{P}_\sigma(s_0 \models \Box\Diamond W) = 1$ .

# Qualitative reachability analysis

**Questions**

How does max (resp. min) reachability probability compare to 0 and 1?

**Examples**

- $\max_\sigma \ \mathbb{P}_\sigma(\Diamond T) = 1$?
- $\min_\sigma \ \mathbb{P}_\sigma(\Diamond T) = 0$?

Solutions: **fixpoint expressions** for "winning sets" of states

- $\nu X.\mu Y.T \cup \left(\bigcup_{\alpha \in Act} Pre[\alpha](Y) \cap \widetilde{Pre}[\alpha](X)\right)$
- $\nu X.(S \setminus T) \cap \left(\bigcup_{\alpha \in Act} \mathrm{Pre}[\alpha](S) \cap \widetilde{\mathrm{Pre}}[\alpha](X)\right)$

further issue: convergence of fixpoint computation

# Well-quasi orderings

## Well-quasi ordering (wqo)

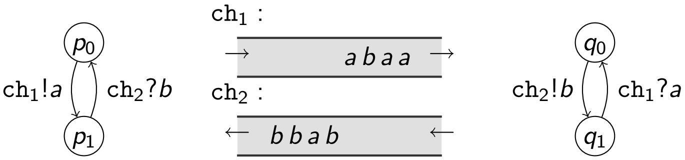
A wqo on $S$ is a reflexive and transitive relation $\preceq \subseteq S \times S$ such that any infinite sequence of elements $s_0, s_1, s_2, \cdots$ from $S$ contains an increasing pair $s_i \preceq s_j$ with $i < j$.

Upward-closure operator: For $T \subseteq S$, $\uparrow T = \{s \in S \mid \exists t \in T \text{ s.t. } t \preceq s\}$.
Upward-closed set: $T \subseteq S$ such that $T = \uparrow T$.

## Property of wqo

Any infinite non-decreasing sequence $T_0 \subseteq T_1 \subseteq T_2 \cdots$ of upward-closed sets converges: $\exists i \; \forall k > 0 \; T_{i+k} = T_i$.

# Wqo in lossy channel systems




quasi ordering $\preceq$ on states of LCS

subword ordering on channel contents + same control states

Illustration of $\preceq$

- $\forall w,\ (p,\varepsilon) \preceq (p,w)$
- $(q, abba) \preceq (q, abracadabra)$

## Higman's lemma

$\preceq$ is a well-quasi ordering.

# $\mu$-calculus

$(2^S, \subseteq)$ is a complete Boolean lattice

## $\mu$-calculus

$\mu$-calculus terms are defined in the following syntax

$$\phi ::= f(\phi_1, \ldots, \phi_n) \mid X \mid \mu X.\phi \mid \nu X.\phi$$

for $f$ monotonic operator.

Examples of monotonic operators

- constants (= sets of states)
- union, intersection
- predecessor
- upward-closure (for given ordering)

# Guarded terms

joint work with Christel Baier and Philippe Schnoebelen

## Guardedness

A term $\phi$ is guarded if

- for all least-fixpoint subterms $\mu X.\phi_1$
  $X$ is under the scope of an upward-closure operator in $\phi_1$
- for all greatest-fixpoint subterms $\nu X.\phi_1$
  $X$ is under the scope of a downward-closure operator in $\phi_1$

### Examples of guarded terms

- $\mu X. T \cup \uparrow Pre(X)$
- $\nu Y.\mu X. \uparrow T \cup \Big( Pre(X) \cap \downarrow \widetilde{Pre}(Y) \Big)$

## Convergence for guarded terms

The iterative computation of fixpoint expressed by guarded $\mu$-calculus terms terminates.

# Probabilistic (nondeterministic) lossy channel systems

## Purely probabilistic LCS

- Markov chain with **finite attractor**
- **computability** of $\mathrm{Pre}^*(T)$
- consequence: decidability of qualitative reachability analysis

## Probabilistic and nondeterministic LCS

1 player controlling actions (sendings, receptions, internal)
probabilistic losses

- MDP with **finite attractor**
- **guarded terms** for winning sets
- consequence: decidability of qualitative reachability problems

1. Finite probabilistic systems
   - Finite Markov chains
   - Finite Markov decision processes

2. Infinite probabilistic systems with a finite attractor
   - Infinite MC with a finite attractor
   - Infinite MDP with a finite attractor
   - Computability of fixpoints

3. Towards parameterized probabilistic systems

# Parameterized verification

Goal: verify several instances of a problem with a parameter taking values in infinite domain

Examples of parameters

- ▷ initial graph in GTS
- ▷ value of a constant (e.g. probability of a transition)
- ▷ **number of processes** in network

Questions

1. $\forall N, S^N \models \varphi$?
2. dually $\exists N,\ S^N \models \varphi$?

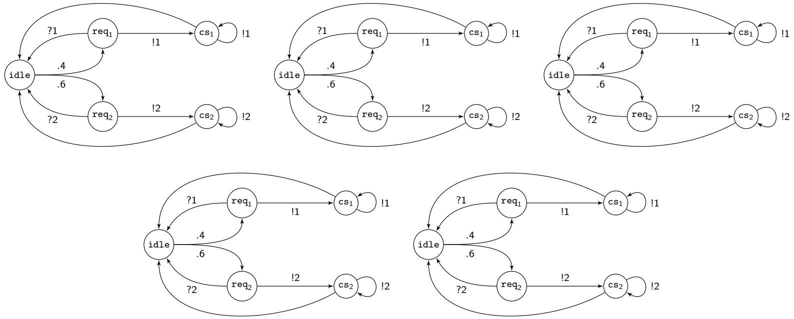
In an MDP context: $\exists N,\ \max_\sigma \mathbb{P}_\sigma(\mathcal{P}^N \models \Diamond T) = 1$?

# Existing work

- undecidable in general — Apt,Kozen [ipl86]
- networks of identical finite automata — Clarke et al. [concur95]
- networks of identical timed automata — Abdulla et al. [tcs03,lics04]
- ad-hoc networks — Sangnier et al. [concur10,formats'11, etc.]

# A parameterized and probabilistic model

joint work with Paulin Fournier




## Networks of many identical MDP

- arranged in a clique
- communicating by broadcast

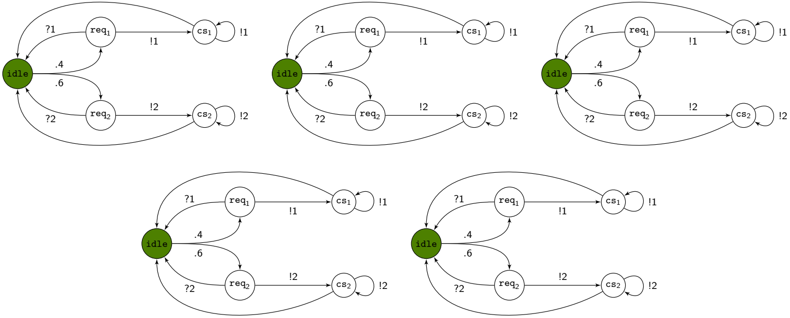
# Semantics

Markov decision process

Configuration $(q_0, q_1, \cdots, q_N)$

Scheduler chooses a process and an action

broadcasts are received by all other processes



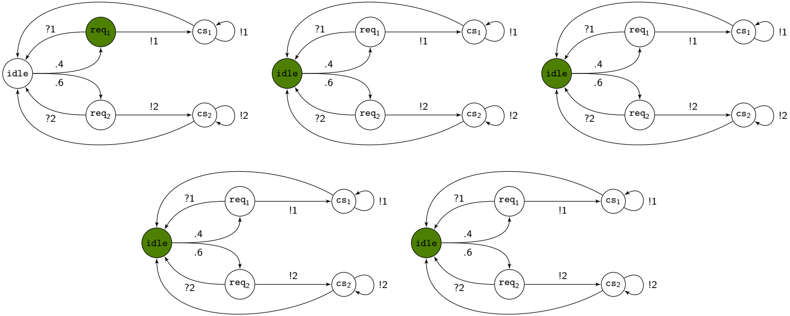
# Semantics

Markov decision process

Configuration $(q_0, q_1, \cdots, q_N)$

Scheduler chooses a process and an action

broadcasts are received by all other processes



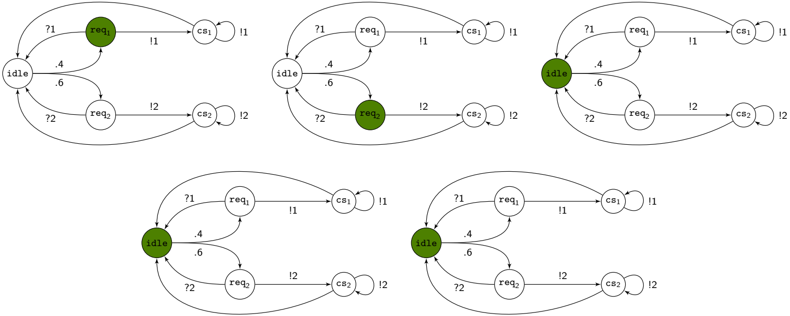
# Semantics

Markov decision process

Configuration $(q_0, q_1, \cdots, q_N)$

Scheduler chooses a process and an action

broadcasts are received by all other processes



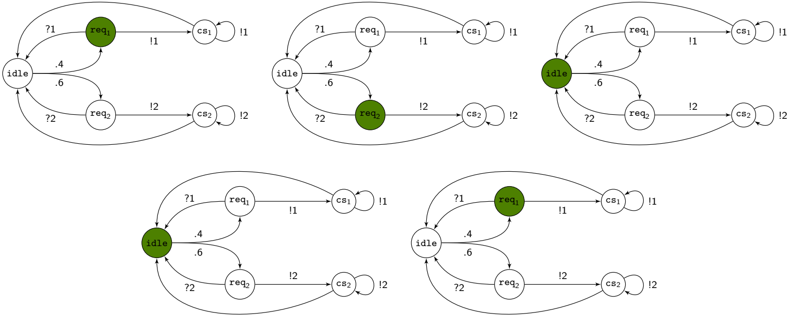
# Semantics

Markov decision process

Configuration $(q_0, q_1, \cdots, q_N)$

Scheduler chooses a process and an action

broadcasts are received by all other processes



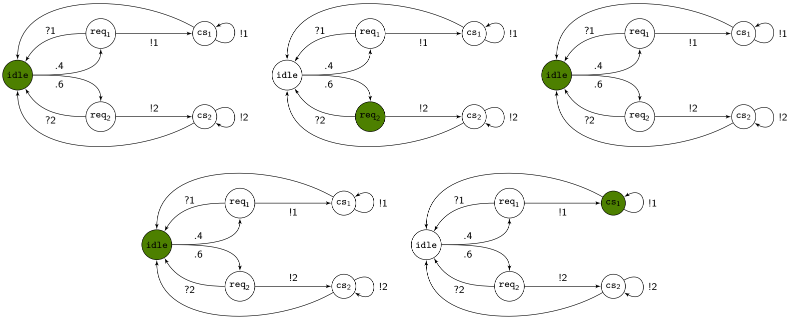
# Semantics

Markov decision process

Configuration $(q_0, q_1, \cdots, q_N)$

Scheduler chooses a process and an action

broadcasts are received by all other processes



# Dynamic networks of communicating MDP

After each action probabilistic deletions and creations of processes

- ▷ fixed individual failure rate $\lambda$
- ▷ insertion probability law: $k$ processes with $\mu^k(1-\mu)$

## Properties of dynamic networks

- **finite attractor** property
- natural **wqo** on configurations
- Pre operator preserves upward closedness
  consequence: winning sets can be written as **guarded terms**

Qualitative reachability problems are decidable
for dynamic networks of communicating MDP

# Summary

Review of model checking techniques for probabilistic systems

- finite Markov chains and Markov decision processes
- infinite MC and MDP with a finite attractor

Parameterized verification of networks of communicating MDP

- unknown initial number of processes
- random process creation and disparition
- decidability of qualitative reachability problems
- more results in Paulin's talk this afternoon

# Perspectives for parameterized verification of MDP

Further investigation of parameterized verification of probabilistic systems

- **refine model** of process deletion/creation
- consider **quantitative** properties
- **synthesize relations** between parameter and performances
- alternative problem: networks of MDP with **dynamic topology** (chosen at each step by the scheduler)
- **distributed schedulers** basing their decisions only on local states

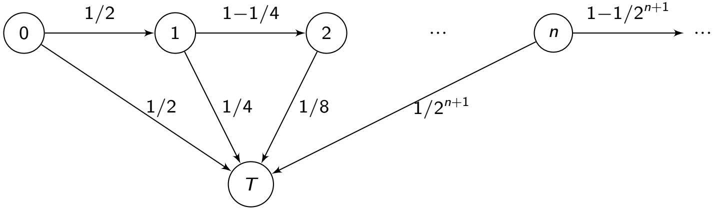
# Counterexample without finite attractor

Correctness of fixpoint relies on **finite attractor** property!

$$\mathbb{P}(s \models \Diamond T) = 1 \quad \text{iff} \quad s \in \nu X.\ \mu Y.\ T \cup \big(Pre(Y) \cap \widetilde{Pre}(X)\big)$$

Greatest set $X$ of states from which

- ▷ $T$ can be reached with positive probability
- ▷ while being sure to stay in $X$




Back to main