
MUSEE
La Magie des Automates
OUVERT 7/7

Recall:

What we have

Transition systems.

A (set of) natural and expressive composition operator(s).

A natural congruence notion, bisimulation.

What we also have:

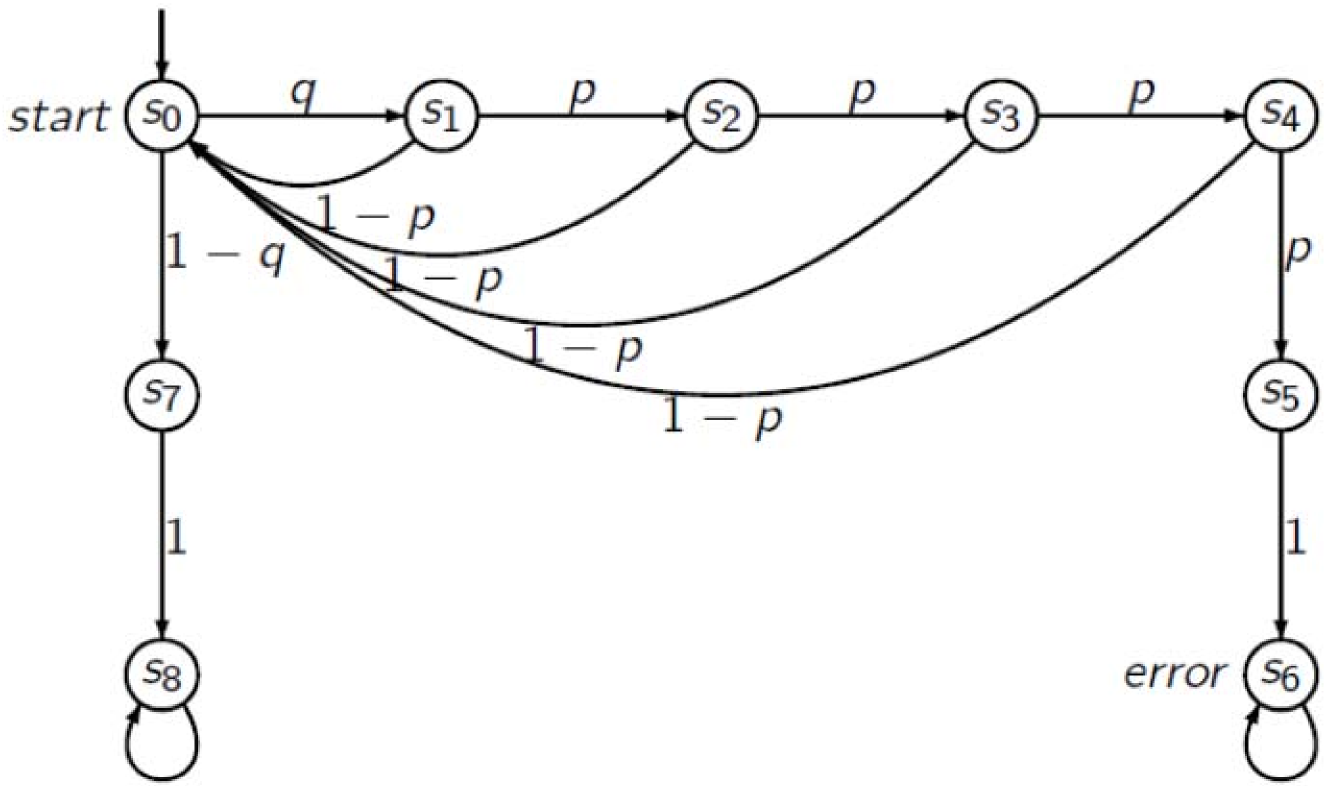
An abstraction operator (hiding).

Efficient minimisation algorithms for bisimulation.

Matching logics (CTL, sugared a-f mu-calculus).

Recall:

Zeroconf as a Markov chain



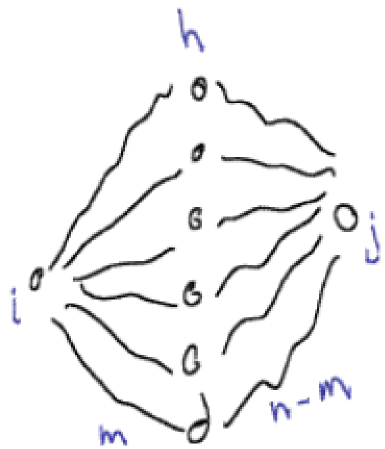
Probabilities for n-steps

- $\mathbf{P}(s, s')$ is the one-step transition probability from s to s'.
- Let $\mathbf{P}^{(n)}$ denote the n-step transition matrix

$$p_{ij}^{(n)} := P(X_n = j \mid X_0 = i) = P(X_{k+n} = j \mid X_k = i).$$

- Note: $\mathbf{P}^{(1)} = \mathbf{P}$
- Applying the law of total probability
  we get the Chapman-Kolmogorov equation:

$$p_{ij}^{(n)} = \sum_{h \in S} p_{ih}^{(m)} p_{hj}^{(n-m)}$$



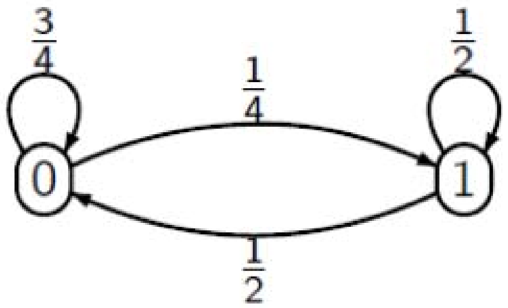
  for all $0 < m < n$
- It then follows that: $\mathbf{P}^{(n)} \; = \; \mathbf{P}\,\mathbf{P}^{(n-1)} \; = \; \mathbf{P}^n$

The transient state probability distribution at time n is defined by:

- $\pi(n) := \; \pi(0)\,\mathbf{P}^n \; = \; \pi(n-1)\,\mathbf{P}$

Example

A simple DTMC



$$\mathbf{P} = \begin{pmatrix} 0.75 & 0.25 \\ 0.5 & 0.5 \end{pmatrix} \qquad \mathbf{P}^2 = \begin{pmatrix} 0.6875 & 0.3125 \\ 0.625 & 0.375 \end{pmatrix}$$

- With initial distribution $\pi(0) = (0, 1)$, we get:

$$\pi(2) = \pi(0)\,\mathbf{P}^2 = (0,1)\,\mathbf{P}^2 = (0.625, 0.375)$$

- With $\pi(0) = (\frac{2}{3}, \frac{1}{3})$, we have:

$$\pi(2) = \pi(0)\,\mathbf{P}^2 = \left(\frac{2}{3}, \frac{1}{3}\right)\mathbf{P}^2 = \left(\frac{2}{3}, \frac{1}{3}\right)$$

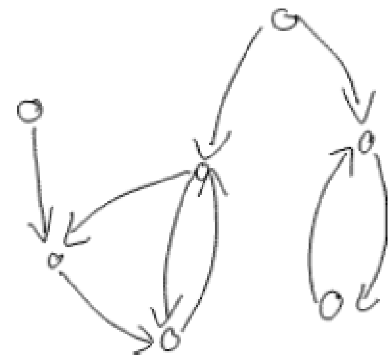
Actually: $\pi(n) \;=\; (\frac{2}{3}, \frac{1}{3}) \quad \forall n \in \mathcal{T}$

On the long run . . .

Steady state limit

$$\tilde{\pi} := \lim_{n \to \infty} \pi(n) = \lim_{n \to \infty} \pi(0)\, \mathbf{P}^n = \pi(0) \lim_{n \to \infty} \mathbf{P}^n$$

- The limit $\tilde{\pi}$ may not exist.
- The limit $\tilde{\pi}$ may depend on $\pi(0)$.
- If existing, we call $\tilde{\pi}$ the steady state probability distribution.
- $\tilde{\pi}$ is in balance, it satisfies: $\pi = \pi\, \mathbf{P}$.



Cesàro limit

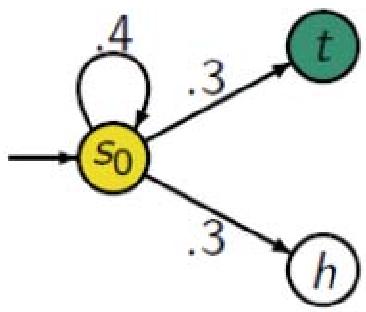
If existing, the limit $\tilde{\pi}$ agrees with the Cesàro limit:

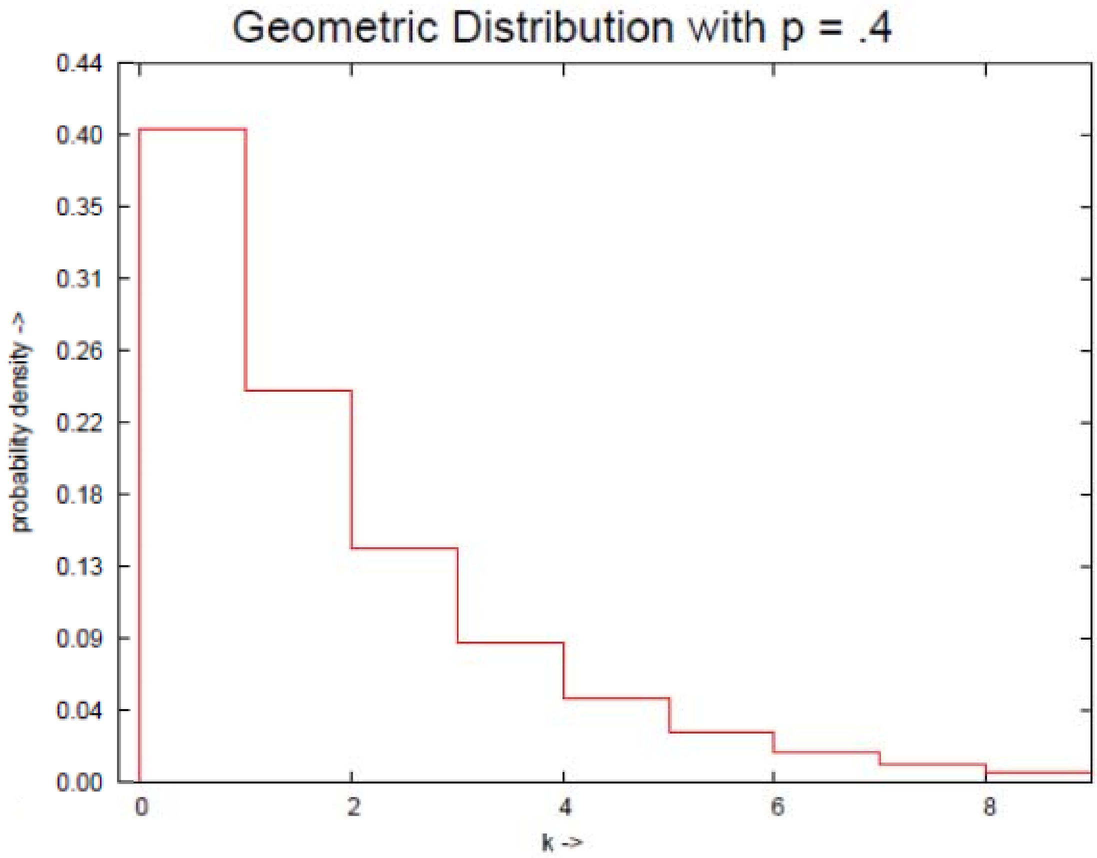
$$\tilde{\pi}_s = \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n} \pi_s(i).$$

The Cesàro limit always exists, it corresponds to
the long run fraction of being in state s, it is also denoted $lrf(s)$.

DTMC: What to remember

- Finite – homogeneous – discrete-time Markov chains.
- Transient behaviour: $\pi(n) \;=\; \pi(0)\,\mathbf{P}^n$.
- Stationary behaviour: $\tilde{\pi} \;=\; \tilde{\pi}\,\mathbf{P}$.
- Sojourn time is geometrically distributed: $P(SJ = k) \;=\; p\,(1-p)^k$.





What comes next

We are going to discuss

Model Construction, and

Model Checking

for DTMCs

DTMC with labels

We equip states of a DTMC with labels to identify state properties:

- AP denotes the set of atomic propositions
- a DTMC is a tuple $\mathcal{D} = (S, \mathbf{P}, \pi(0), AP, L)$ where $L : S \rightarrow 2^{AP}$.

$L(s)$ specifies the properties holding in state s.

Probabilistic Computation Tree Logic: PCTL

Syntax

State formulas:

$$\Phi := \mathit{true} \mid a \mid \Phi_1 \wedge \Phi_2 \mid \neg\Phi \mid \exists\phi \mid \forall\phi$$

where $a \in AP$.

Path formulas:

$$\phi := \mathcal{X}\Phi \mid \Phi_1 \, \mathcal{U} \, \Phi_2$$

Probabilistic Computation Tree Logic: PCTL

Syntax

State formulas:

$$\Phi := \mathit{true} \mid a \mid \Phi_1 \wedge \Phi_2 \mid \neg\Phi \mid \mathbb{P}_J(\phi) \mid \mathbb{L}_J(\Phi)$$

where $a \in AP$, $J \subseteq [0,1]$ is an interval with rational bounds.

Path formulas:

$$\phi := \mathcal{X}\Phi \mid \Phi_1\, \mathcal{U}\, \Phi_2 \mid \Phi_1\, \mathcal{U}^{\leq n}\, \Phi_2$$

Notations

Derived notations

- $\mathbb{P}_{\leq 0.5}(\phi) := \mathbb{P}_{[0,0.5]}(\phi)$
- $\mathbb{P}_{=1}(\phi) := \mathbb{P}_{[1,1]}(\phi)$
- $\neg(\neg\Phi_1 \wedge \neg\Phi_2) := \Phi_1 \vee \Phi_2$
- $\Diamond\Phi := \mathit{true}\ \mathcal{U}\ \Phi$
- $\Box\Phi := \neg(\Diamond\neg\Phi)$ but this is not in PCTL!
- $\Diamond^{\leq n}\Phi := \mathit{true}\ \mathcal{U}^{\leq n}\ \Phi$
- $\mathbb{P}_{<p}(\Box\Phi) := \mathbb{P}_{\geq 1-p}(\Diamond\neg\Phi)$

For the last one: observe $\Box\Phi$ is "the negation" of $\Diamond\neg\Phi$!

Specifying properties using PCTL

- the outcomes of a fair die should occur with equal probability

$$\bigwedge_{i=1,\ldots,6} \mathbb{P}_{=\frac{1}{6}}(\Diamond i)$$

- craps game: the probability of winning is strictly less than 0.5

$$\mathbb{P}_{<0.5}(\Diamond win)$$

- craps game: the probability of winning without ever rolling $8, 9$ or 10 is at least 0.32

$$\mathbb{P}_{\geq 0.32}((\neg 8 \wedge \neg 9 \wedge \neg 10)\ \mathcal{U}\ win)$$

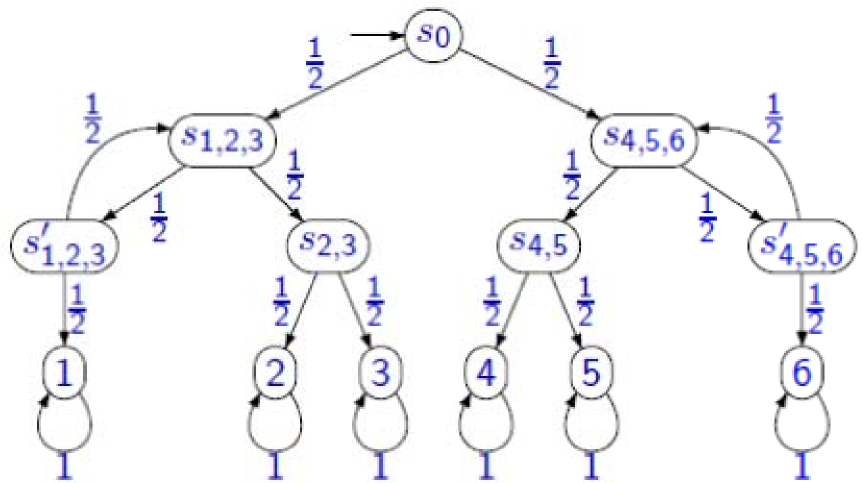


Table 1. Availability measures and their logical specification.

long-run	$\mathbb{L}_{\trianglelefteq p}(up)$
instantaneous	$\mathbb{P}_{\trianglelefteq p}(\Diamond^{[t,t]} up)$
conditional instantaneous	$\mathbb{P}_{\trianglelefteq p}(\Phi \mathcal{U}^{[t,t]} up)$
interval	$\mathbb{P}_{\trianglelefteq p}(\Box^{[t,t']} up)$
long-run interval	$\mathbb{L}_{\trianglelefteq p}(\mathbb{P}_{\trianglelefteq q}(\Box^{[t,t']} up))$
conditional interval long-run	$\mathbb{P}_{\trianglelefteq p}(\Phi \mathcal{U}^{[t,t']}\, \mathbb{L}_{\trianglelefteq q}(up))$

Some Notations

For a given DTMC $\mathcal{D} = (S, \mathbf{P}, \pi(0), AP, L)$,

- denote by **Pr** the induced probability measure,
- denote by $\mathbf{Pr}_s$ the induced probability measure with initial state s,

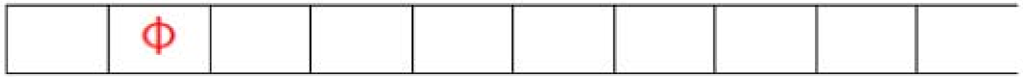
- For a path $\sigma = s_0 s_1 s_2 \ldots$, for $i \geq 0$, $\sigma[i] := s_i$ denotes the $i+1$-th state.

Semantics

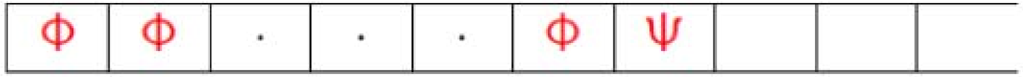
Satisfaction relation for PCTL path formulas

For a path σ through DTMC $\mathcal{D}$, the satisfaction relation $\models$ is defined by:

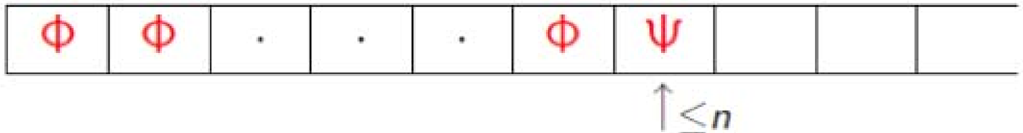
- $\sigma \models \mathcal{X}\Phi$ iff $\sigma[1] \models \Phi$,



- $\sigma \models \Phi \, \mathcal{U} \, \Psi$ iff there exists $0 \leq i$ with $\sigma[i] \models \Psi$ and for all $j < i$, $\sigma[j] \models \Phi$



- $\sigma \models \Phi \, \mathcal{U}^{\leq n} \, \Psi$ iff there exists $0 \leq i$ and $i \leq n$
  with $\sigma[i] \models \Psi$ and for all $j < i$, $\sigma[j] \models \Phi$



Measurability of PCTL events

For DTMC $\mathcal{D} = (S, \mathbf{P}, \pi(0), AP, L)$, state $s \in S$ and any PCTL path formula ϕ, the set $\{\sigma \in Paths(s) \mid \sigma \models \phi\}$ is measurable.

Semantics

Satisfaction relation for PCTL state formulas

Given a DTMC $\mathcal{D}$, state $s \in S$, the satisfaction relation $\models$ is defined by:

- $s \models a$ iff $a \in L(s)$,
- $s \models \neg\Phi$ iff $s \not\models \Phi$,
- $s \models \Phi \wedge \Psi$ iff $s \models \Phi$ and $s \models \Psi$,
- $s \models \mathbb{P}_J(\phi)$ iff $\mathbf{Pr}_s(\phi) \in J$,
- $s \models \mathbb{L}_J(\Phi)$ iff $\sum_{s' \models \Phi} lrf_s(s') \in J$,

Model checking

Problem (Model checking)

Let $\mathcal{D}$ be a DTMC and Φ a PCTL state formula. The model checking problem determines whether $s \models \Phi$ for each $s \in S$.

Characterisation of the set *Sat*

- $Sat(true) = S$,
- $Sat(a) = \{s \mid a \in L(s)\}$,
- $Sat(\Phi \wedge \Psi) = Sat(\Phi) \cap Sat(\Psi)$,
- $Sat(\neg\Phi) = S \setminus Sat(\Phi)$,
- $Sat(\mathbb{P}_J(\phi)) = \{s \mid \mathbf{Pr}_s(\phi) \in J\}$
- $Sat(\mathbb{L}_J(\phi)) = \{s \mid \sum_{s' \in Sat(\Phi)} lrf_s(s') \in J\}$

How to check the probabilistic formulae

Consider the formula $\mathbb{P}_J(\phi)$

To compute the set $Sat(\mathbb{P}_J(\phi))$, it is sufficient to compute the probability $\mathbf{Pr}_s(\phi)$ for all s.

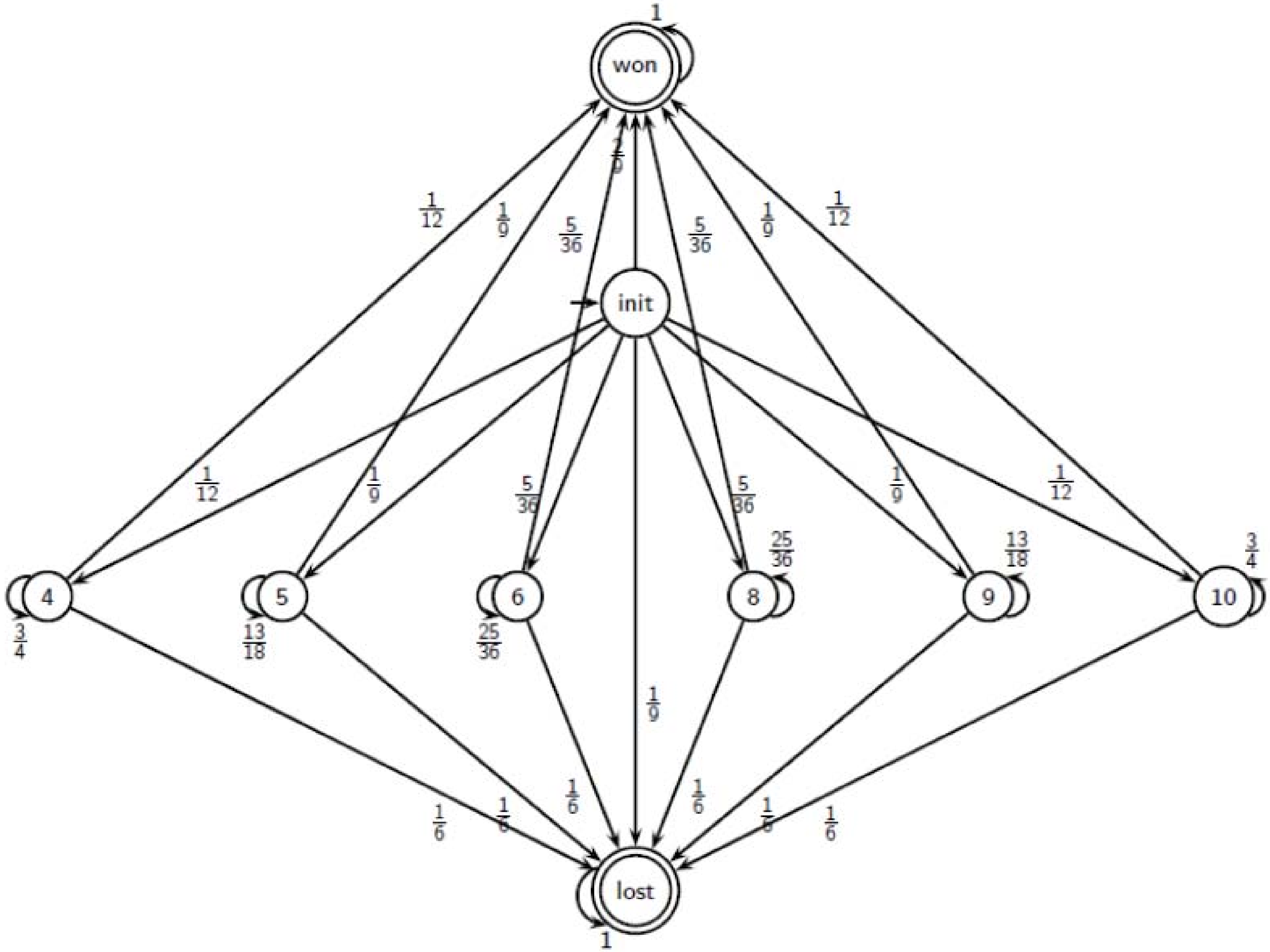
(In practice, we compute this number up to a given accuracy ϵ.)

The case $\phi = \mathcal{X}\Phi$

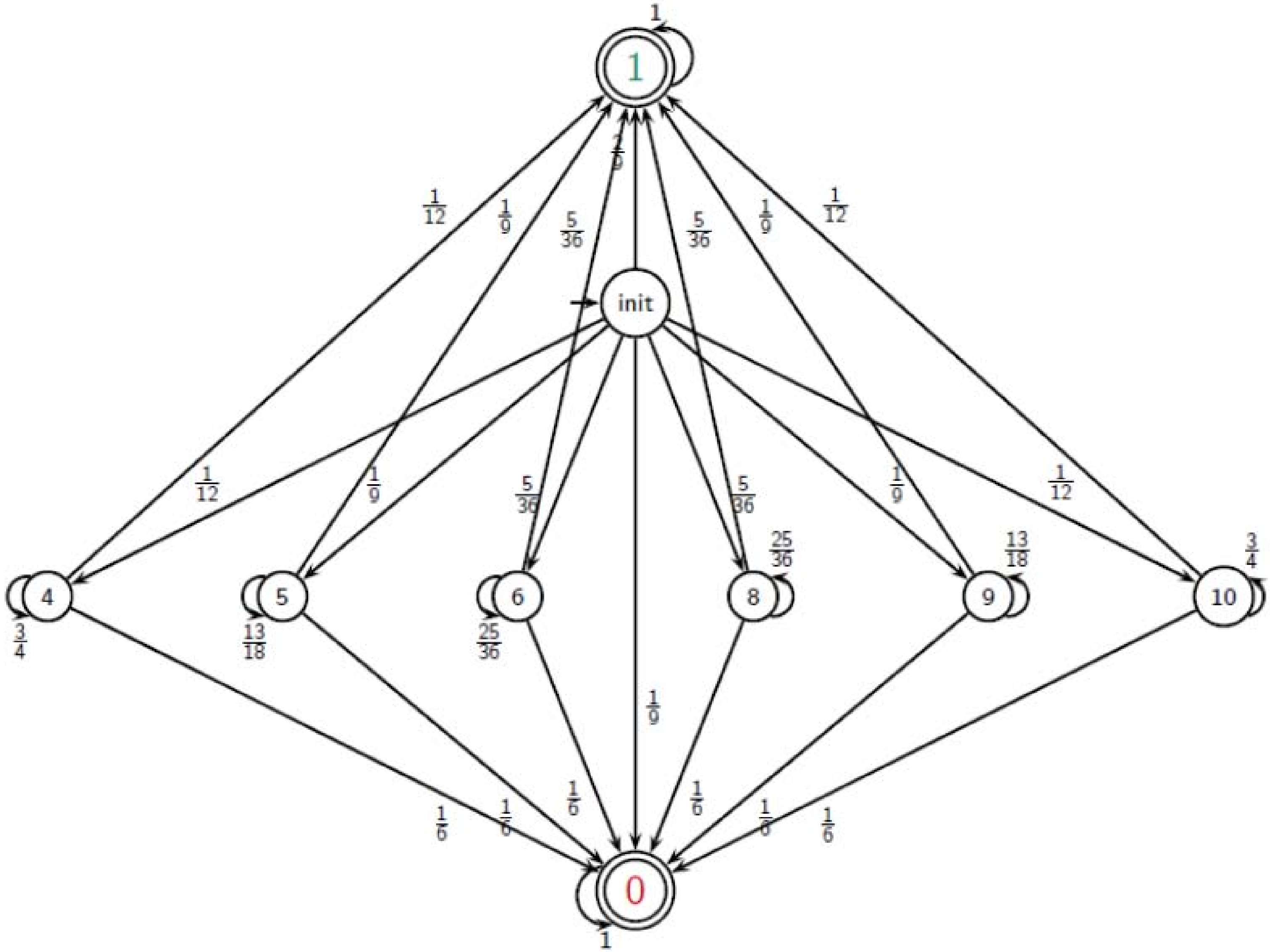
The set $Sat(\Phi)$ is computed recursively. It holds:

$$\mathbf{Pr}_s(\mathcal{X}\Phi) = \sum_{s' \in Sat(\Phi)} \mathbf{P}(s, s')$$

Do you win? $\mathbb{P}_{>0.5}(\Diamond win)$

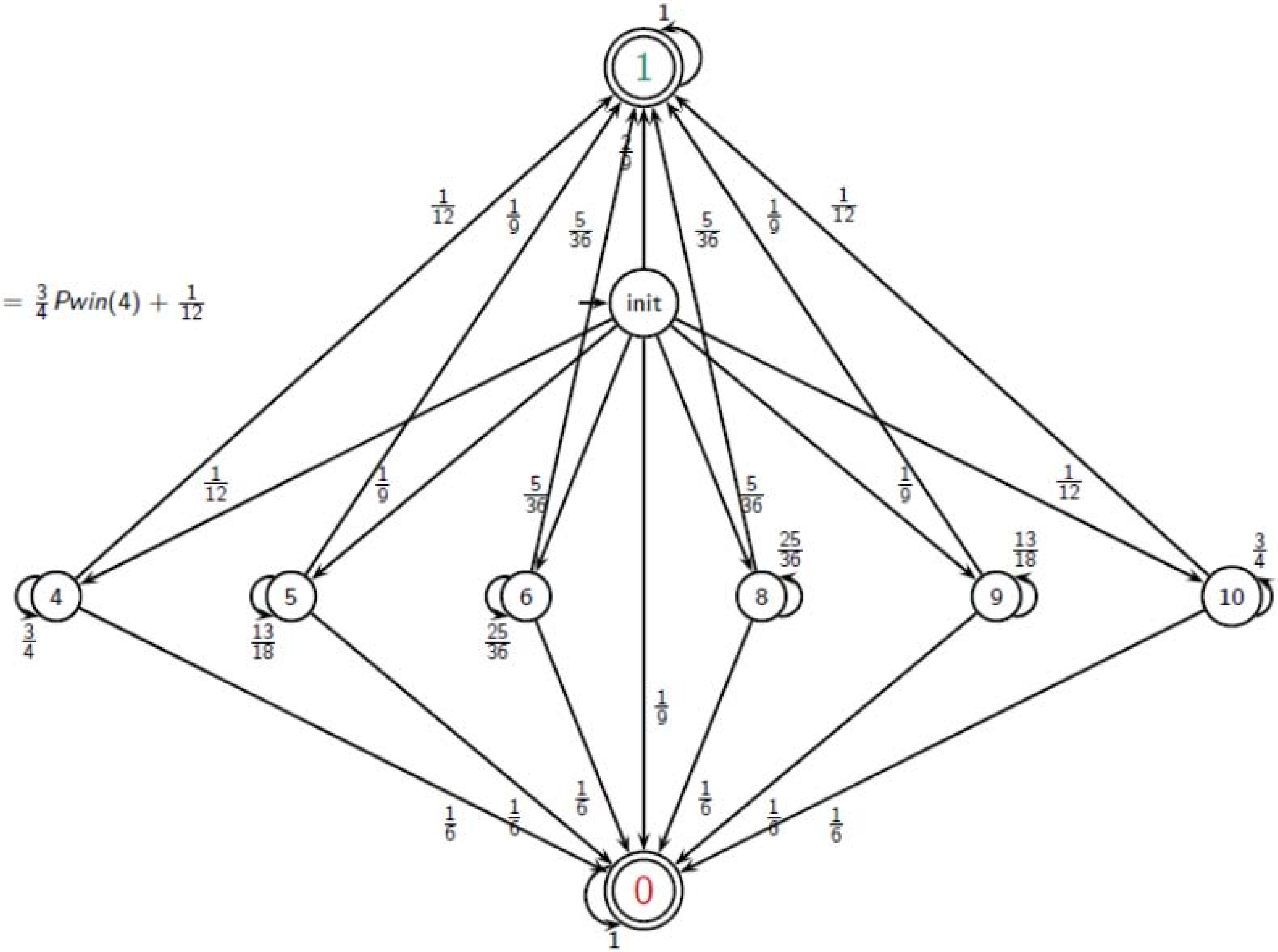


Do you win? $\mathbb{P}_{>0.5}(\Diamond win)$



Do you win? $\mathbb{P}_{>0.5}(\Diamond win)$

$Pwin(4) = \frac{3}{4} Pwin(4) + \frac{1}{12}$

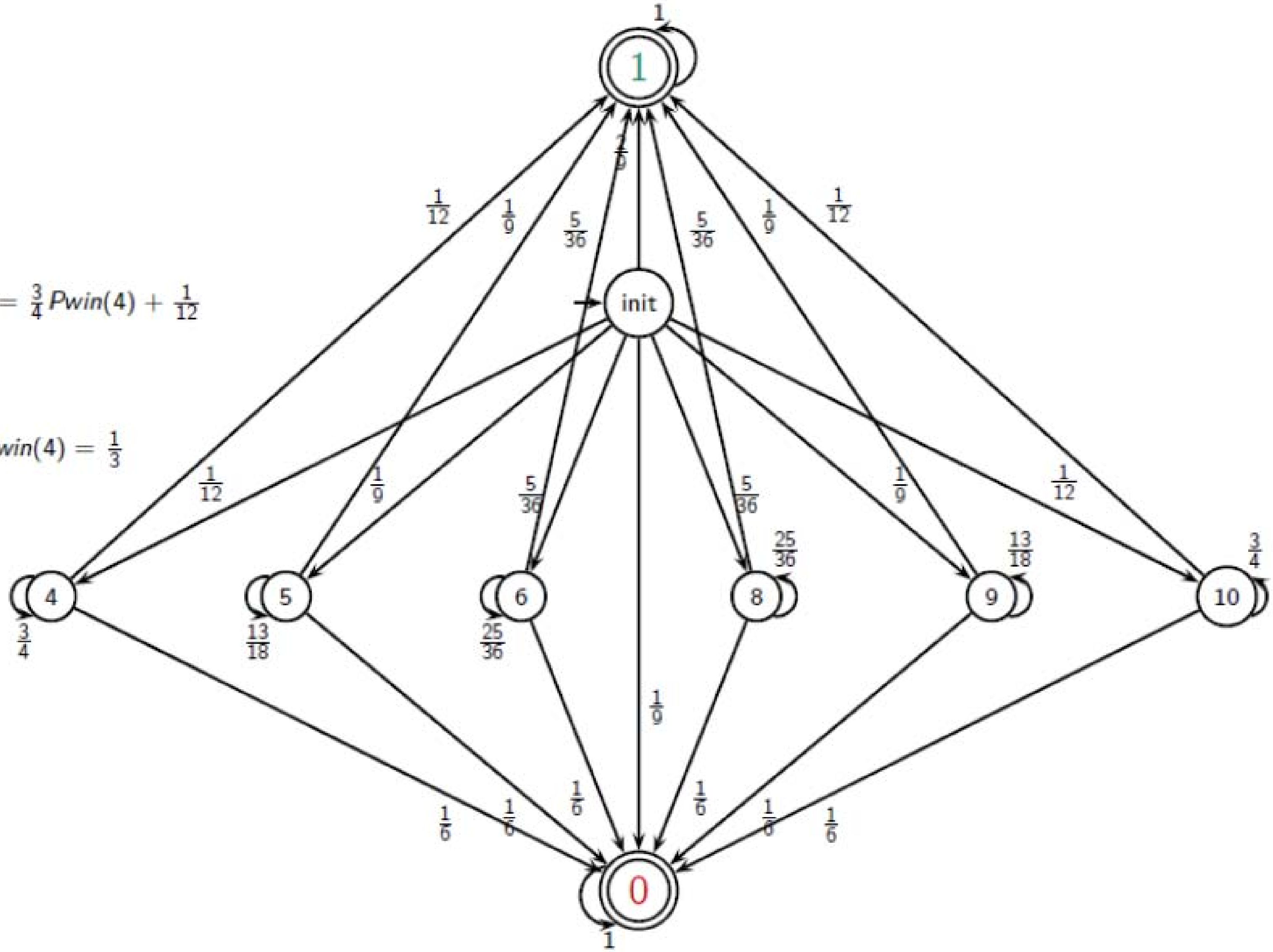


Holger Hermanns

Do you win? $\mathbb{P}_{>0.5}(\Diamond win)$

$Pwin(4) = \frac{3}{4} Pwin(4) + \frac{1}{12}$

$Pwin(4) = \frac{1}{3}$

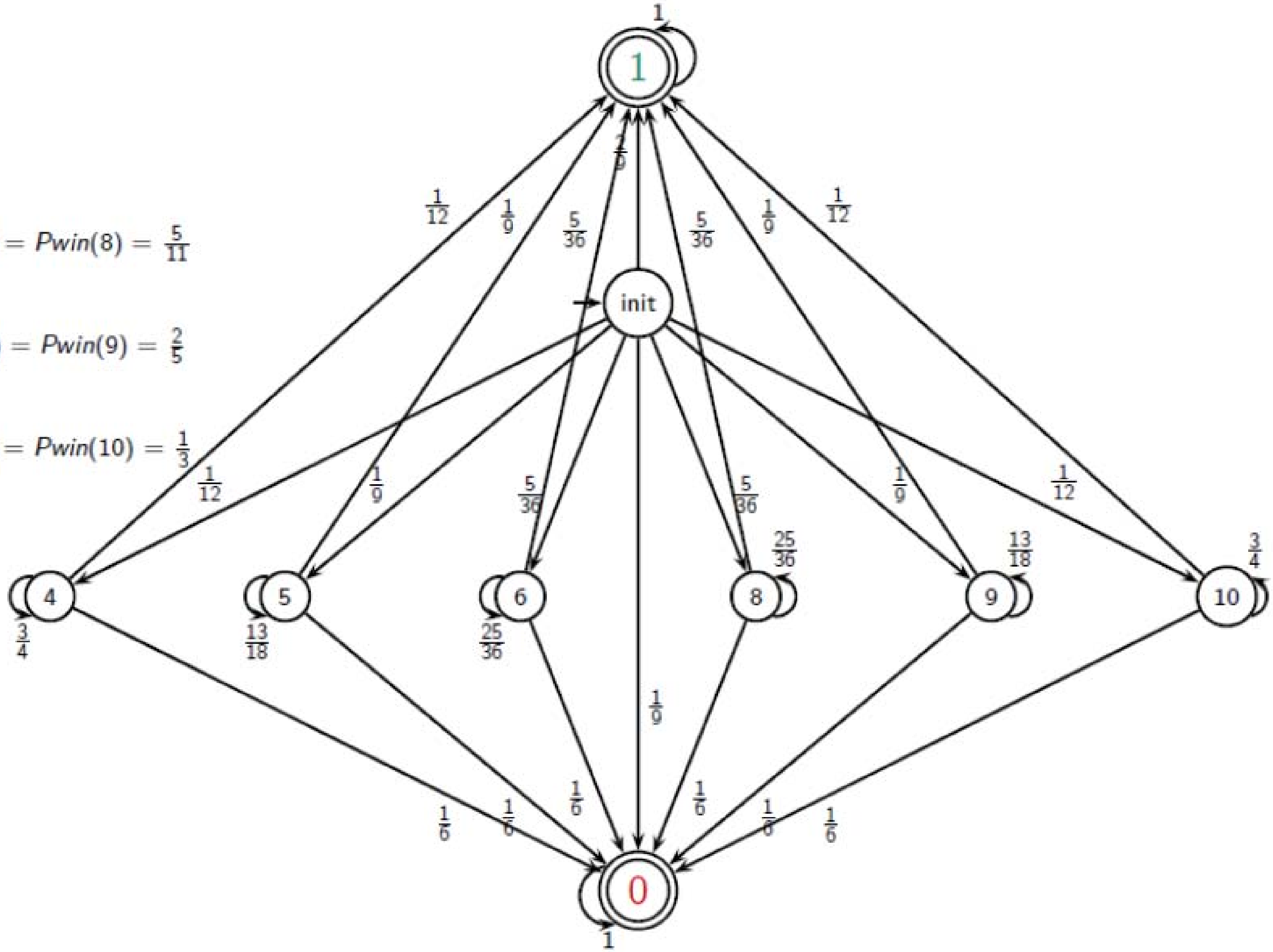


Do you win? $\mathbb{P}_{>0.5}(\Diamond win)$

$Pwin(6) = Pwin(8) = \frac{5}{11}$

$Pwin(5) = Pwin(9) = \frac{2}{5}$

$Pwin(4) = Pwin(10) = \frac{1}{3}$



Holger Hermanns

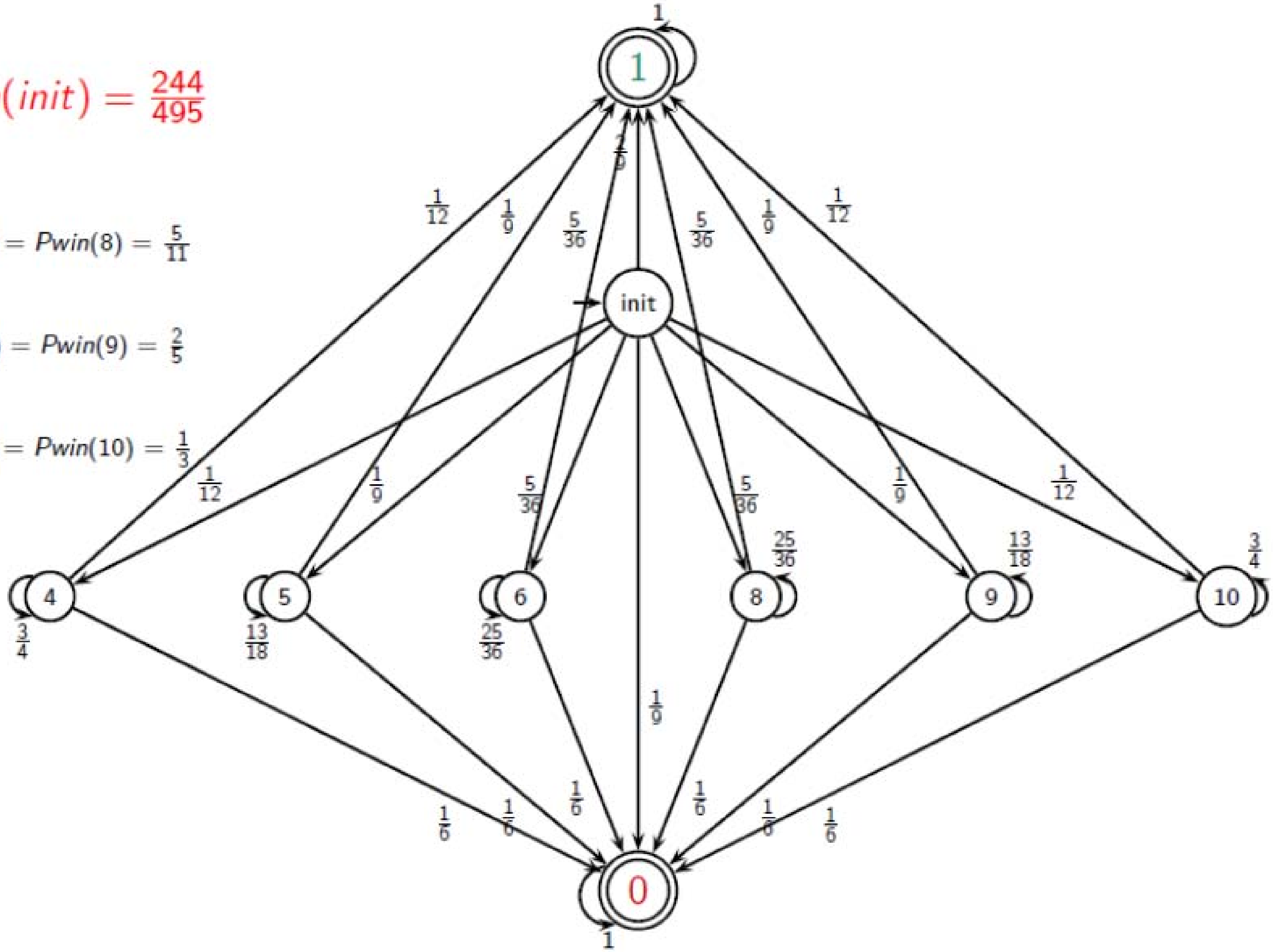
Do you win? $\mathbb{P}_{>0.5}(\Diamond win)$

$Pwin(init) = \frac{244}{495}$

$Pwin(6) = Pwin(8) = \frac{5}{11}$

$Pwin(5) = Pwin(9) = \frac{2}{5}$

$Pwin(4) = Pwin(10) = \frac{1}{3}$



Reachability Probability

Given a DTMC $(S, \mathbf{P}, \pi(0))$, a set of goal state $B \subseteq S$,
what is the probability of reaching B eventually?

- Let x_s denote this probability starting in state s
- for $s \in B$, $x_s = 1$
- for $s \in S \setminus B$, it holds: $$x_s = \sum_{t \in S \setminus B} \mathbf{P}(s,t)x_t + \sum_{u \in B} \mathbf{P}(s,u)$$

  In matrix form: $\mathbf{x} = \mathbf{A}\mathbf{x} + \mathbf{b}$

  where $\mathbf{A} = (\mathbf{P}(s,t))_{s,t \in S \setminus B}$

  $\mathbf{b} = (b_s)_{s \in S \setminus B}$ with $b_s = \mathbf{P}(s, B)$.
- The matrix problem can be reduced by precomputing

  $S_{=0} = \{s \in S \mid \mathbf{Pr}_s(\Diamond B) = 0\}$ and $S_{=1} = \{s \in S \mid \mathbf{Pr}_s(\Diamond B) = 1\}$

  and then restricting to $S_{=?} = S \setminus (S_{=1} \cup S_{=0})$

Reachability Probability

Given a DTMC $(S, \mathbf{P}, \pi(0))$, a set of goal state $B \subseteq S$,
what is the probability of reaching B eventually?

- Let x_s denote this probability starting in state s
- for $s \in S_{=1}$, $x_s = 1$, for $s \in S_{=0}$, $x_s = 0$.
- for $s \in S_{=?}$, it holds: $$x_s = \sum_{t \in S_{=?}} \mathbf{P}(s,t)x_t + \sum_{u \in S_{=1}} \mathbf{P}(s,u)$$

  In matrix form: $\mathbf{x} = \mathbf{A}\mathbf{x} + \mathbf{b}$

  where $\mathbf{A} = (\mathbf{P}(s,t))_{s,t \in S_{=?}}$

  $\mathbf{b} = (b_s)_{s \in S_{=?}}$ with $b_s = \mathbf{P}(s, S_{=1})$.
- The matrix problem can be reduced by precomputing

  $S_{=0} = \{s \in S \mid \mathbf{Pr}_s(\Diamond B) = 0\}$ and $S_{=1} = \{s \in S \mid \mathbf{Pr}_s(\Diamond B) = 1\}$

  and then restricting to $S_{=?} = S \setminus (S_{=1} \cup S_{=0})$

Fixed point characterisation

We need to solve a more general problem: conditional reachability probability for two state sets C and B:

$$\mathbf{Pr}_s(C \; \mathcal{U} \; B) := \mathbf{Pr}_s\{\sigma \mid \exists i. \, \forall j < i. \, \sigma[j] \in C \wedge \sigma[i] \in B\}$$

We define:

- $S_{=1} = \{s \mid \mathbf{Pr}_s(C \; \mathcal{U} \; B) = 1\}$ and $S_{=0} = \{s \mid \mathbf{Pr}_s(C \; \mathcal{U} \; B) = 0\}$, and use this to define $S_?$, $\mathbf{A}$ and $\mathbf{b}$ as before.

Theorem

The vector $(x_s)_{s \in S_?}$ with $x_s = \mathbf{Pr}_s(C \; \mathcal{U} \; B)$ is the unique fixed point of the operator $\nabla : (S_? \to [0,1]) \to (S_? \to [0,1])$ defined by:

$$\nabla(\mathbf{y}) = \mathbf{A} \cdot \mathbf{y} + \mathbf{b}$$

Further, for $\mathbf{x}(0) = \mathbf{0}$ and $\mathbf{x}(n+1) = \nabla(\mathbf{x}(n))$, we get:

- $\mathbf{x}(i)$ *is increasing,*
- $\mathbf{x} = \lim_{n \to \infty} \mathbf{x}(n)$
- $\mathbf{x}_s(n) = \mathbf{Pr}_s(C \; \mathcal{U}^{\leq n} S_{=1})$ *for* $s \in S_?$,

PCTL Semantics

Satisfaction relation for PCTL state formulas

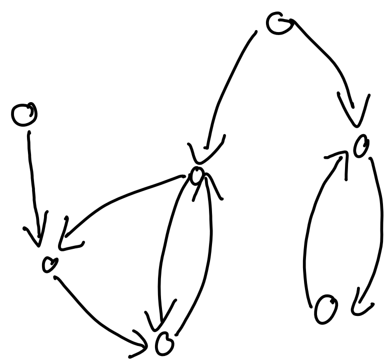
Given a DTMC $\mathcal{D}$, state $s \in S$, the satisfaction relation $\models$ is defined by:

- $s \models a$ iff $a \in L(s)$,
- $s \models \neg\Phi$ iff $s \not\models \Phi$,
- $s \models \Phi \wedge \Psi$ iff $s \models \Phi$ and $s \models \Psi$,
- $s \models \mathbb{P}_J(\phi)$ iff $\mathbf{Pr}_s(\phi) \in J$,
- $s \models \mathbb{L}_J(\Phi)$ iff $\mathit{lrf}_s(\Phi) \in J$,

Model checking steady state operator

Steady state operator $\mathbb{L}_J(\Phi)$:

- Assume Φ is computed recursively.
- Determine the set $\mathbf{B}$ of bottom strongly connected components, BSCCs.
- Compute the probability of reaching each BSCC B.
- For each B compute lrf restricted to B.
- finally, compute $\mathit{lrf}_s(\Phi)$ as follows:



$$\mathit{lrf}_s(\Phi) = \sum_{B \in \mathbf{B}} \left(\mathbf{Pr}_s(\Diamond B) \sum_{s' \in B, s' \models \Phi} \mathit{lrf}^B(s') \right)$$

using that lrf^B is the unique solution of $\pi^B = \pi^B \, \mathbf{P}^B$.

A maybe surprising summary

1. Unbounded until: we can start at the vector $(x_s)_{s \in S_?}$ with $x_s = 0$, and compute $\mathbf{x}(i+1) = \mathbf{A}\mathbf{x}(i) + \mathbf{b}$ until the difference is small.
2. If we stop at iteration k, the above delivers bounded reachability for bound k.
3. Steady-state: we can start at the initial distribution $\pi(0)$, compute $\pi(i+1) = \pi(i)\mathbf{P}$ until the difference is small

All of the three measures can be obtained by transient analysis.
Caution: this might not be the most efficient way!

Complexity

- Solving the equation systems is in polynomial time.
- Matrix vector multiplication is also in polynomial time.
- The computation will be repeated for each state sub-formula.
- Overall complexity:

  polynomial in the size of $\mathcal{D}$,

  linear in the size of Φ,

  linear in the maximal step bound n.