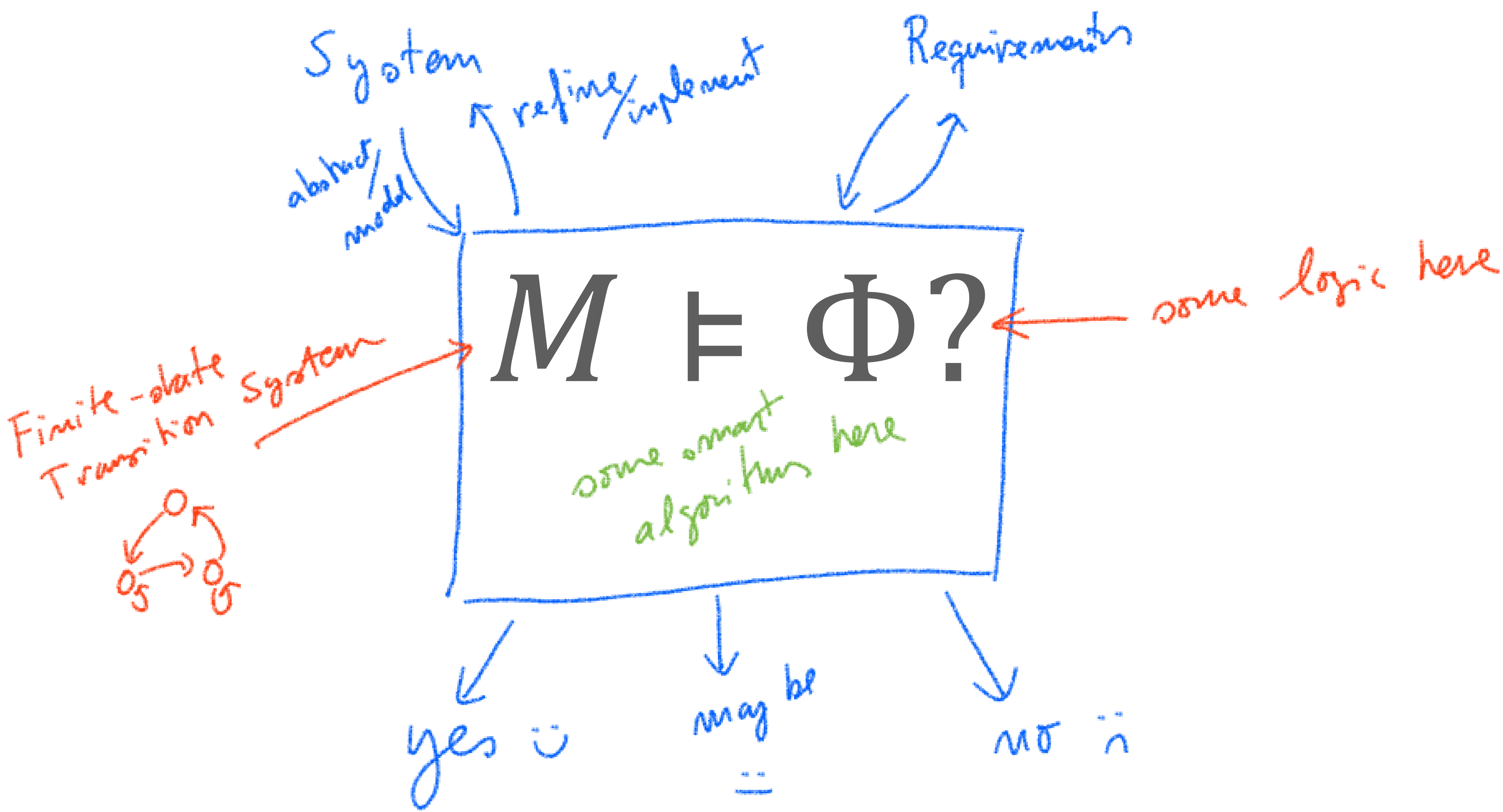
02246 - Model Checking

$$M \models \Phi?$$

Lecture 07 - Probabilistic Temporal Logics

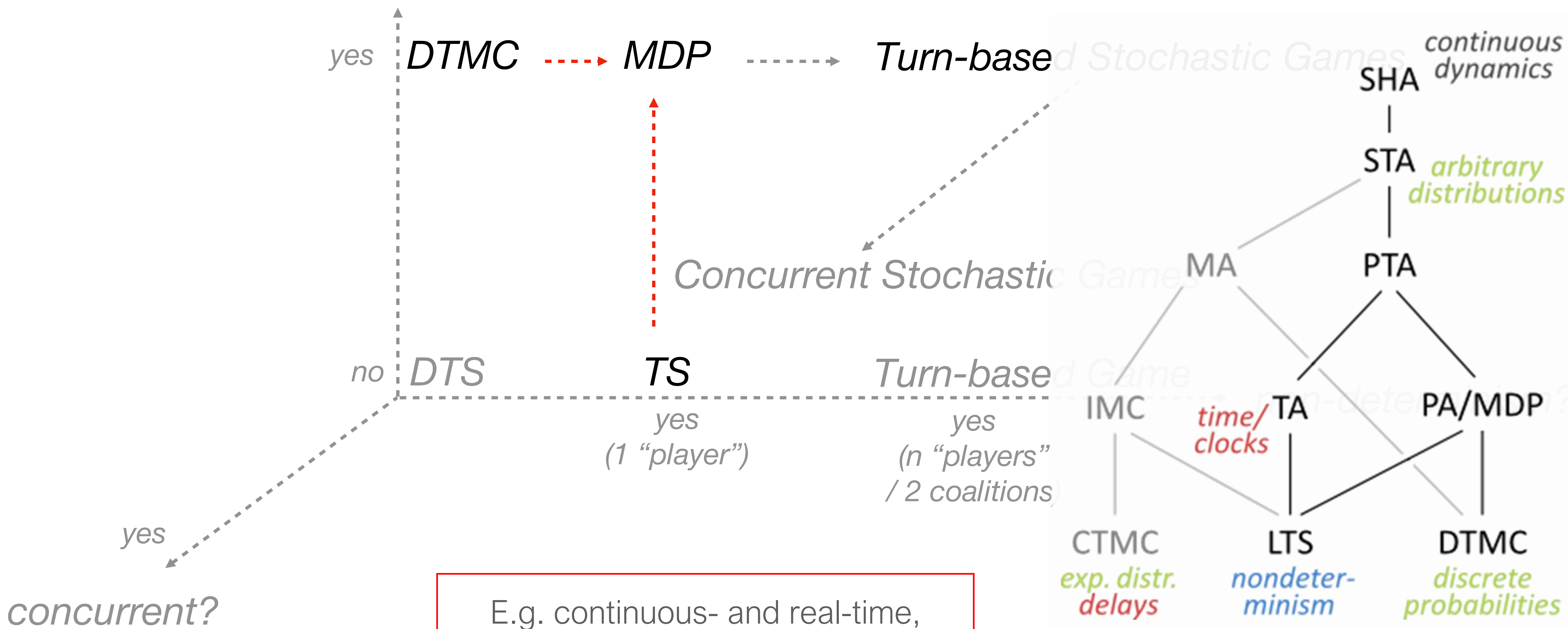
Technical University of Denmark



System
abstract/model
refine/implement
Requirements
M ⊨ Φ?
some smart algorithms here
Finite-state Transition System
some logic here
yes
maybe
no

Some discrete-time models supported by PRISM:

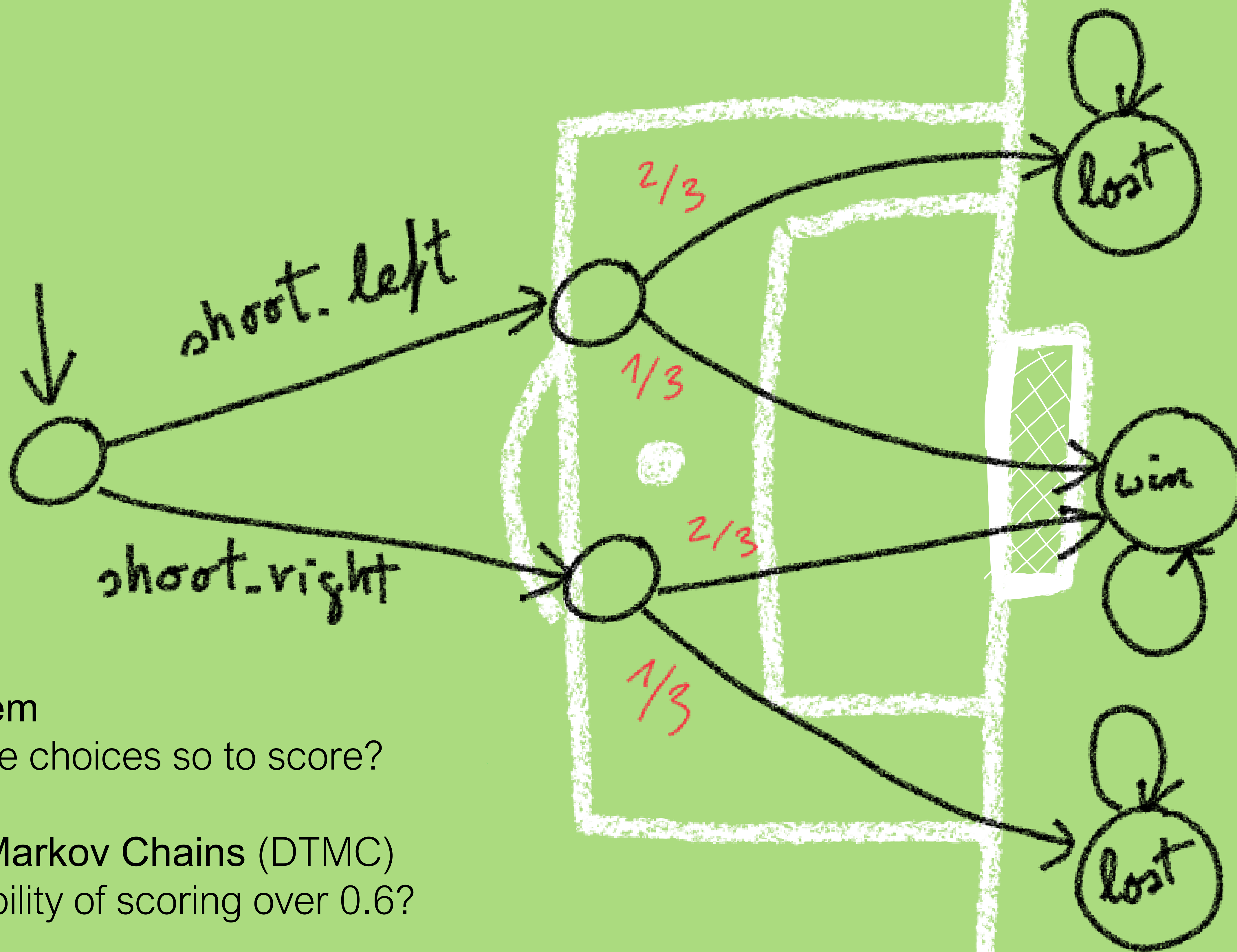
[In the quantitative automata zoo]



E.g. continuous- and real-time, cost/rewards, multi-objective optimisation, partial observability…

NB: there are many other aspects and models supported by PRISM, and other tools and theories

https://www.modestchecker.net/



Transition System

- Can we make choices so to score?

Discrete-Time Markov Chains (DTMC)

- Is the probability of scoring over 0.6?

Markov Decision Process (MDP)

- Can we make choices so that the probability of scoring over 0.6?

Key points of this lecture

PCTL as a logical language to express properties of probabilistic transition systems (DTMCs).

Formal semantics of PCTL.

How probabilistic (bounded/unbounded) reachability is formalized with the cylinder set probability measure.

How PCTL relates to transient/steady state distributions.

How PCTL relates to CTL.

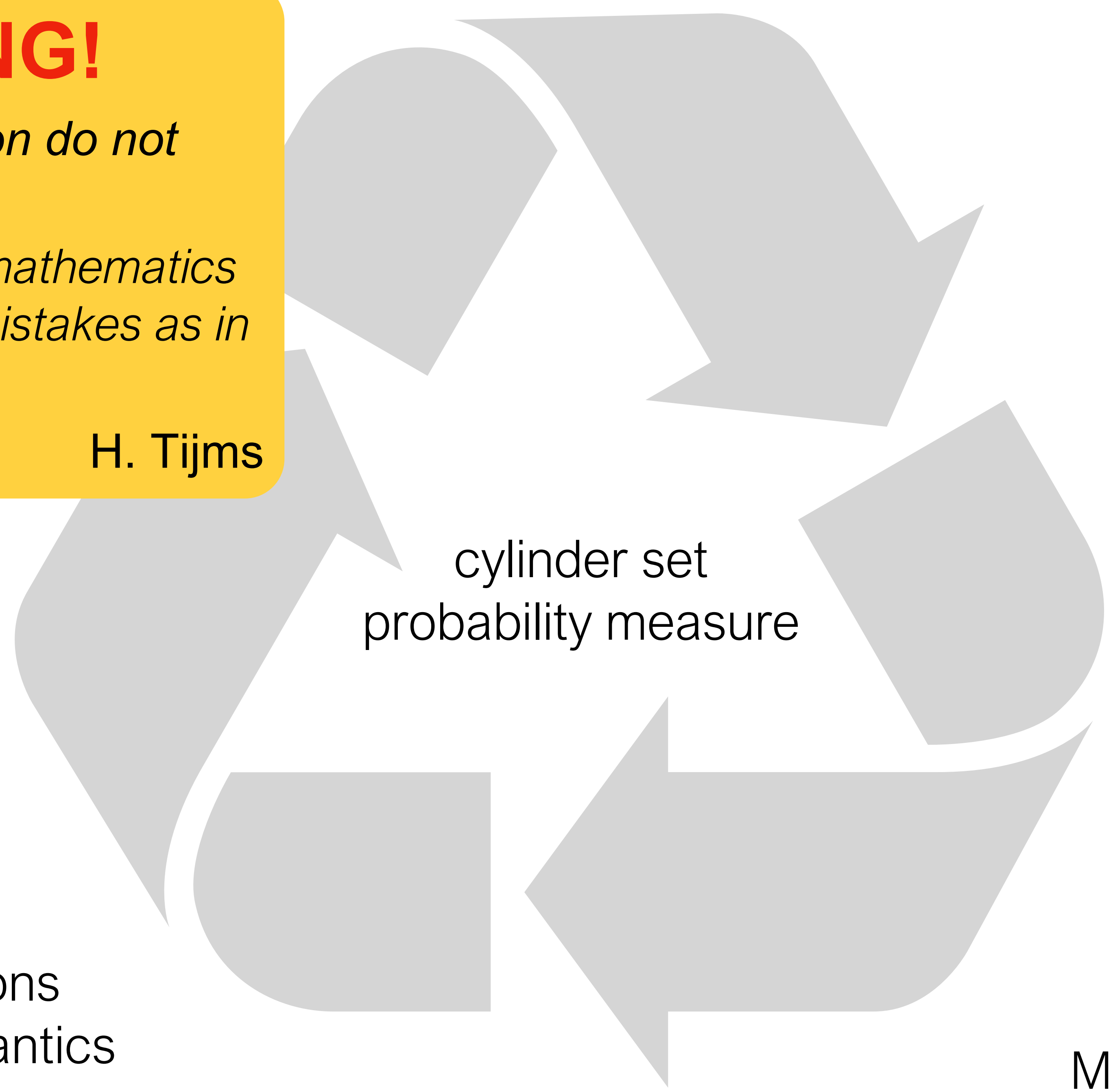
How to check probabilistic properties?

WARNING!

Probability and intuition do not always agree.

In no other branch of mathematics is it so easy to make mistakes as in probability theory.

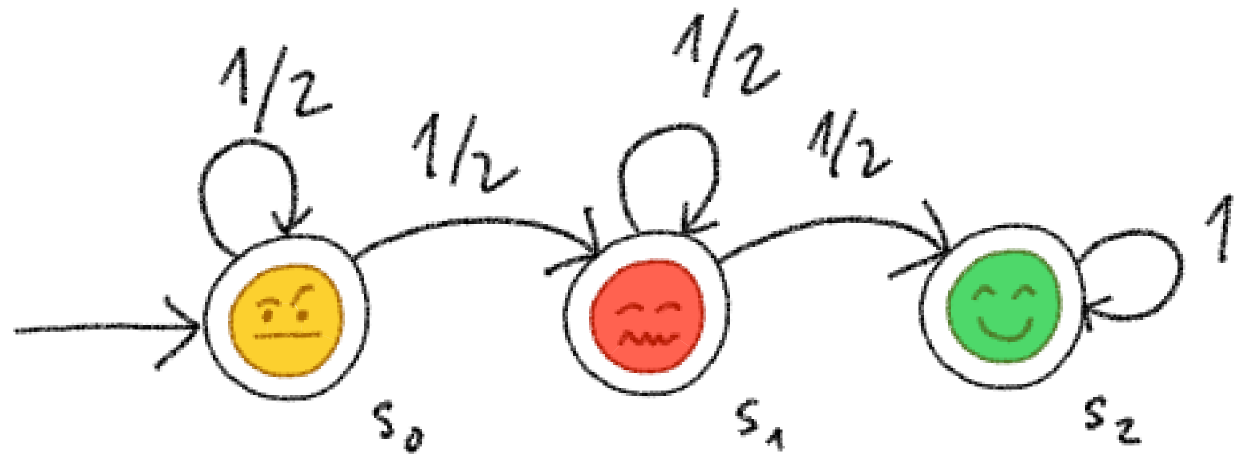
H. Tijms



Probabilistic CTL

- Simple reachability probabilities
- PCTL Syntax
- PCTL Semantics
- Probabilistic Bounded Reachability
- Probabilistic Unbounded Reachability
- PCTL vs other Properties
- Exercises & Homework

Warming up on probabilistic reasoning



Assume transitions model days.

What is the probability of getting infected for the first time in exactly n days?

$n=0 \rightarrow 0$ $\quad n=1 \rightarrow 1/2$ $\quad n=2 \rightarrow 1/4$

What is the probability of getting infected in n days or less?

$n=0 \rightarrow 0$ $\quad n=1 \rightarrow 1/2$ $\quad n=2 \rightarrow 1/2 + 1/4 = 3/4$

What is the probability of getting infected in 0 or more days?

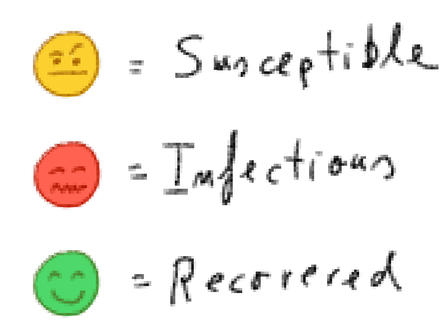
$0 + 1/2 + 1/4 + 1/8 + \dots \rightarrow 1$

What is the probability of eventually getting infected?

1

What is the probability of eventually getting recovered?

1

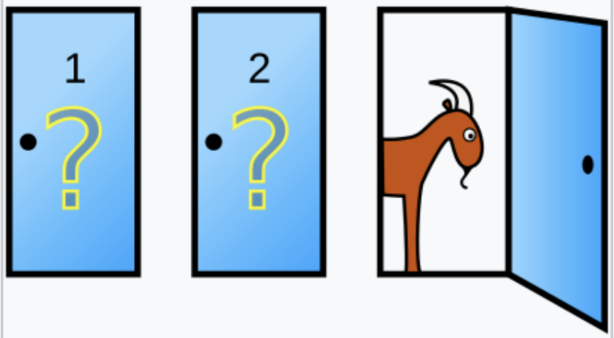


Monty Hall problem

From Wikipedia, the free encyclopedia

The **Monty Hall problem** is a brain teaser, in the form of a probability puzzle, based nominally on the American television game show *Let's Make a Deal* and named after its original host, Monty Hall. The problem was originally posed (and solved) in a letter by Steve Selvin to the *American Statistician* in 1975.[1][2] It became famous as a question from reader Craig F. Whitaker's letter quoted in Marilyn vos Savant's "Ask Marilyn" column in *Parade* magazine in 1990:[3]

> Suppose you're on a game show, and you're given the choice of three doors: Behind one door is a car; behind the others, goats. You pick a door, say No. 1, and the host, who knows what's behind the doors, opens another door, say No. 3, which has a goat. He then says to you, "Do you want to pick door No. 2?" Is it to your advantage to switch your choice?



In search of a new car, the player chooses a door, say *1*. The game host then opens one of the other doors, say *3*, to reveal a goat and offers to let the player switch from door *1* to door *2*.

Probabilistic CTL

- Simple reachability probabilities
- PCTL Syntax
- PCTL Semantics
- Probabilistic Bounded Reachability
- Probabilistic Unbounded Reachability
- PCTL vs other Properties
- Exercises & Homework

PCTL Syntax

The syntax for PCTL state formulas is:

$$\phi \ ::= \ true \ \mid \ p \ \mid \ \neg\phi \ \mid \ \phi_1 \wedge \phi_2 \ \mid \mathbb{P}_J\,(\psi)$$

where p is an atomic proposition, e.g. “infected”,
and $J \subseteq [0,1]$ is an interval, e.g. $J = [0.6, 1.0]$.

$\mathbb{P}_J\,(\psi)$ reads “*the probability to satisfy* ψ *lays in the interval* J”

The syntax for PCTL path formulas is:

$$\psi \ ::= \ \bigcirc\phi \ \mid \ \phi_1 \,\mathsf{U}\, \phi_2 \ \mid \ \phi_1 \,\mathsf{U}^{\leq n}\, \phi_2$$

where $n \in N$ is some natural number.

PCTL in English

"Almost surely …"

$$\mathbb{P}_{\geq 1}(\ldots)$$

"Almost never …"

$$\mathbb{P}_{\leq 0}(\ldots)$$

Derived Operators

syntactic sugar

We have different ways of writing the intervals:

$$\mathbb{P}_{\leq 0.5}(\psi) \equiv \mathbb{P}_{[0.0,\,0.5]}(\psi)$$

We can write formulæ about the “probability of *state* formulæ”:

$$\mathbb{P}_J(\phi) \equiv \mathbb{P}_J(true\ \mathsf{U}^{\leq 0}\ \phi)$$

We can use the “eventually” (diamond) operator as usual:

$$\Diamond\phi \equiv true\ \mathsf{U}\ \phi$$

$$\Diamond^{\leq n}\phi \equiv true\ \mathsf{U}^{\leq n}\ \phi$$

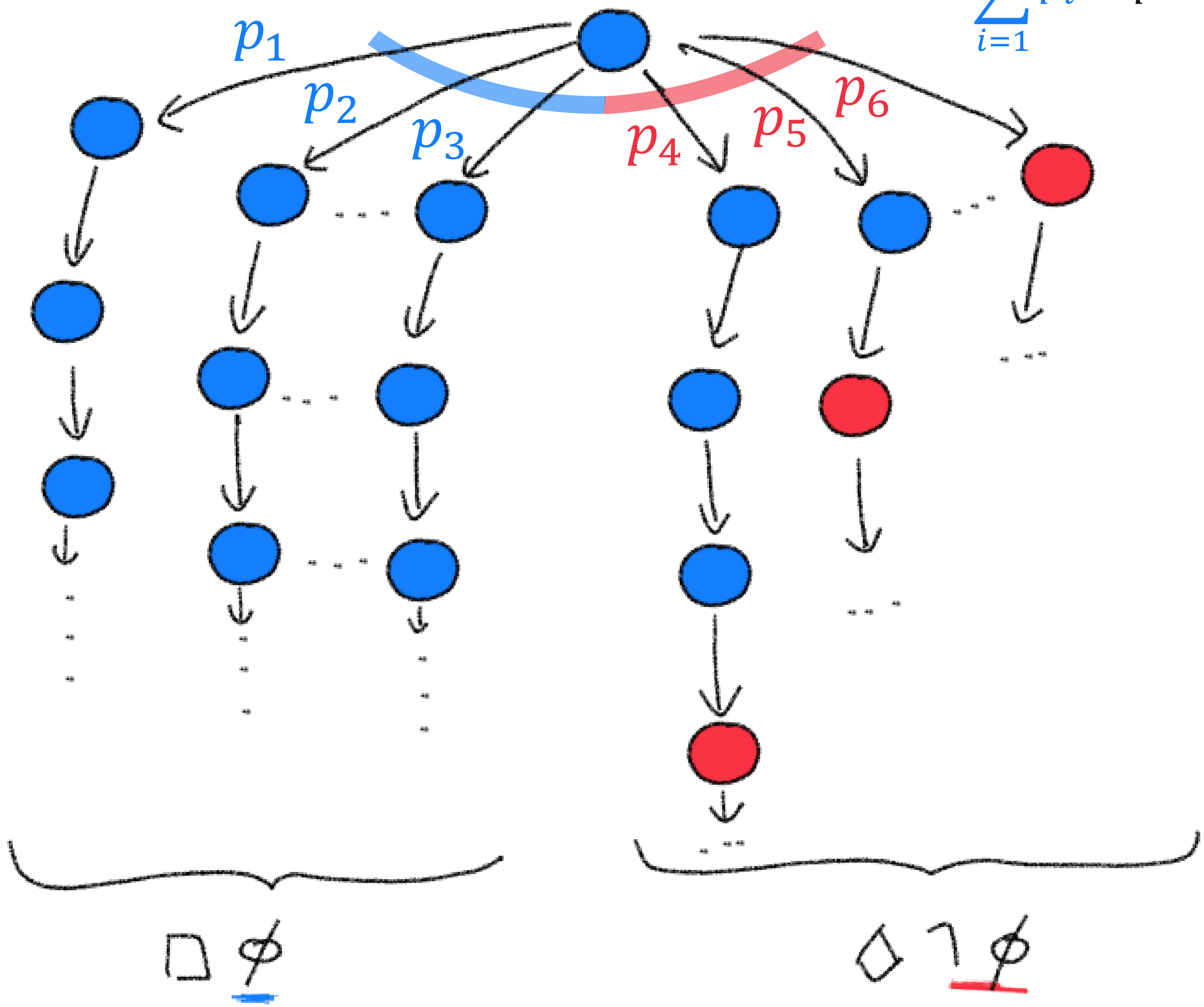
We can also use the “globally” (box) operator, though with care:

$$\mathbb{P}_{\leq p}(\Box\phi) \equiv \mathbb{P}_{\geq 1-p}(\Diamond\neg\phi)$$

B□x / Diam◇nd duality

Intuition of $\mathbb{P}_{\leq p}(\square\phi) \equiv \mathbb{P}_{\geq 1-p}(\diamond\neg\phi)$:

$$\sum_{i=1}^{3} p_i \leq p \;\equiv\; \sum_{j=4}^{6} p_j \geq 1-p$$

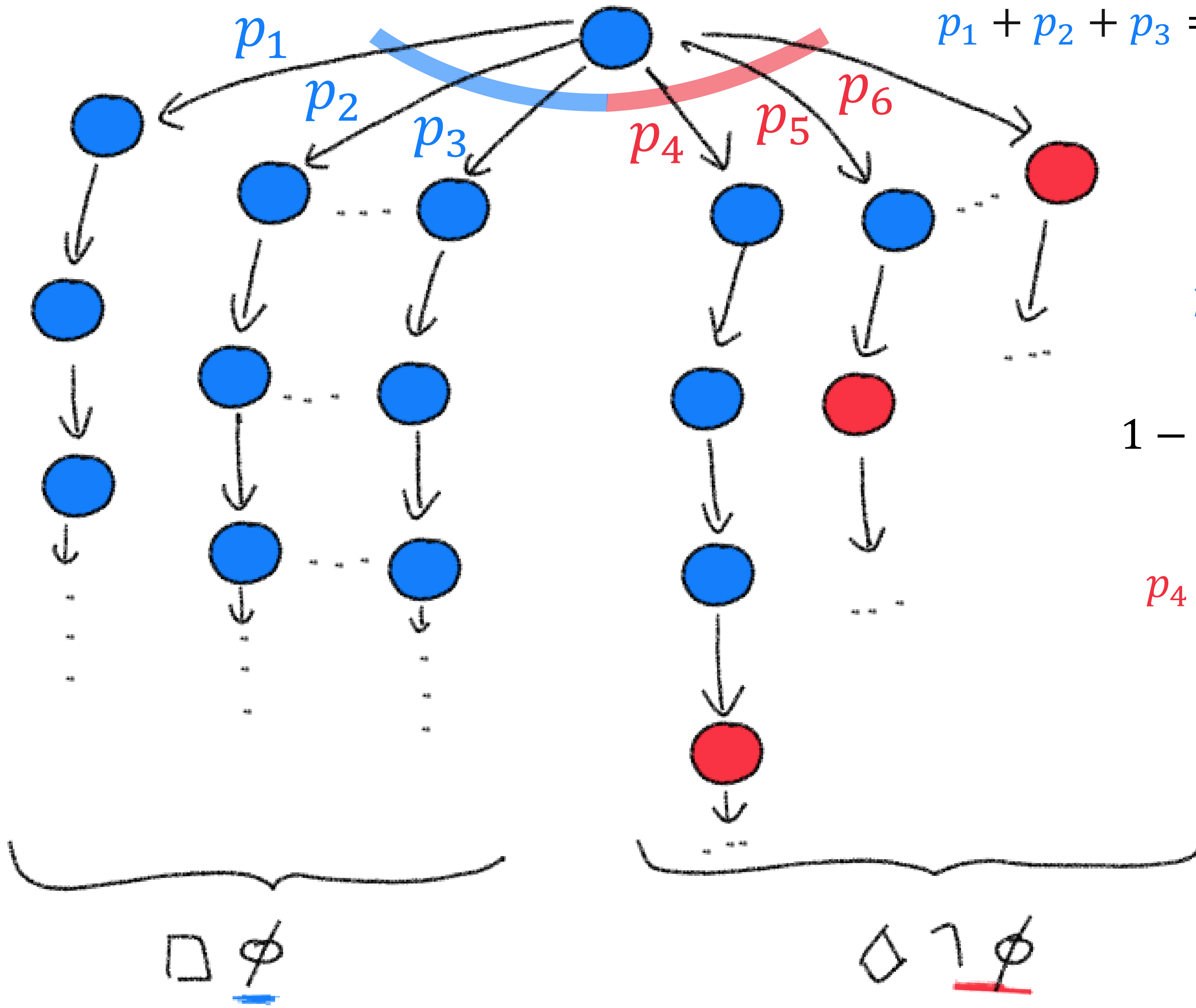


B□x / Diam◇nd duality

Intuition of $\mathbb{P}_{\leq p}(\Box\phi) \equiv \mathbb{P}_{\geq 1-p}(\Diamond\neg\phi)$:

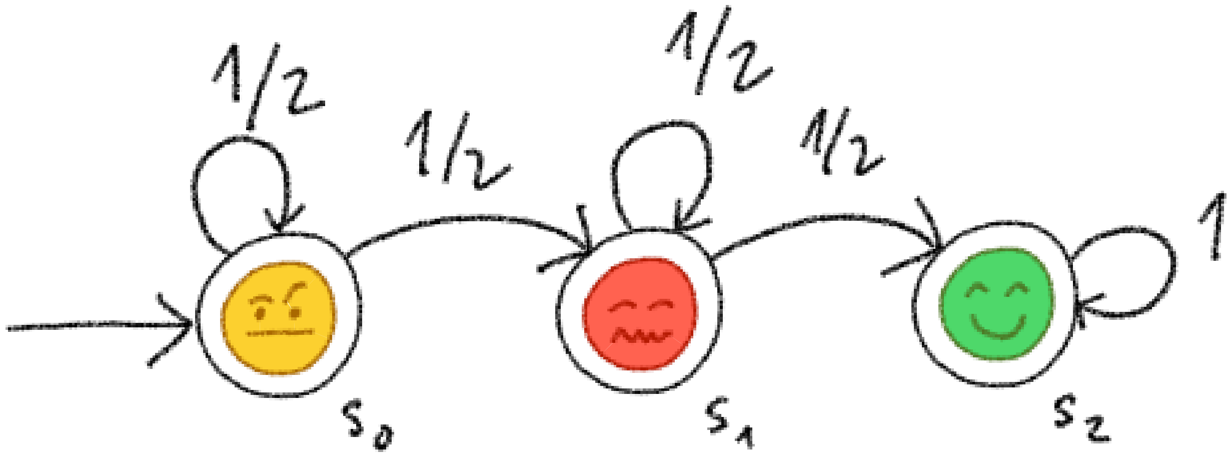
$+ \quad = 1$

$p_1 + p_2 + p_3 = 1 - p_4 - p_5 - p_6$



$$\mathbb{P}_{\leq p}(\Box\phi)$$
$$\Updownarrow$$
$$p_1 + p_2 + p_3 \leq p$$
$$\Updownarrow$$
$$1 - p_4 - p_5 - p_6 \leq p$$
$$\Updownarrow$$
$$p_4 + p_5 + p_6 \geq 1 - p$$
$$\Updownarrow$$
$$\mathbb{P}_{\geq 1-p}(\Diamond\neg\phi)$$

Examples of PCTL formulas



$$\phi ::= true \mid p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \mathbb{P}_J(\psi)$$

$$\psi ::= \bigcirc\phi \mid \phi_1 \,\mathsf{U}\, \phi_2 \mid \phi_1 \,\mathsf{U}^{\le n}\, \phi_2$$

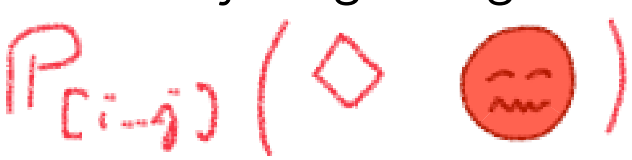
$$\Diamond\phi \equiv true \,\mathsf{U}\, \phi$$

$$\Diamond^{\le n}\phi \equiv true \,\mathsf{U}^{\le n}\, \phi$$

Can we write these properties in PCTL?

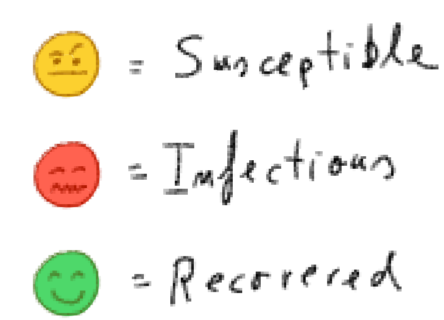
The probability of getting infected in n days or less is in the interval [i..j]?

The probability of getting infected in 0 or more days is in the interval [i..j]?

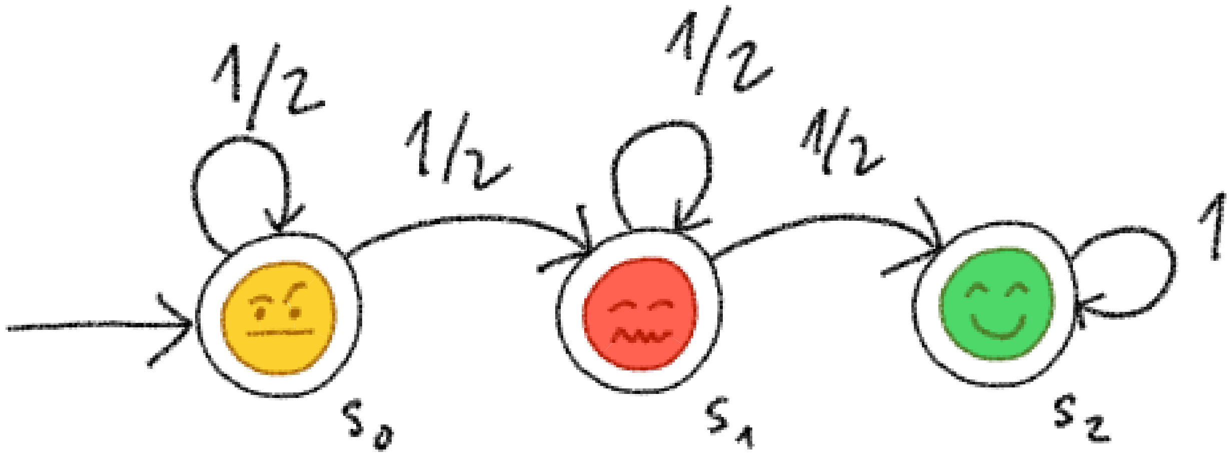


The probability of eventually getting infected is in the interval [i..j]?

The probability of eventually getting recovered is in the interval [i..j]?



Examples of PCTL formulas



ϕ ::= $true$ | p | $\neg\phi$ | $\phi_1 \wedge \phi_2$ | $\mathbb{P}_J(\psi)$

ψ ::= $\bigcirc\phi$ | $\phi_1 \,\mathsf{U}\, \phi_2$ | $\phi_1 \,\mathsf{U}^{\le n}\, \phi_2$

$\Diamond\phi \equiv true \,\mathsf{U}\, \phi$

$\Diamond^{\le n}\phi \equiv true \,\mathsf{U}^{\le n}\, \phi$

Can we write these properties in PCTL?

The probability of getting infected in n days or less is in the interval [i..j]?

$\mathbb{P}_{[i..j]}(\Diamond^{\le n}$  $)$

```
P=? [ F<=n (state=INF) ]
```

```
P=[i..j] [ F<=n (state=INF) ]
```

PRISM's property syntax has no built-in support for this query

The probability of getting infected in 0 or more days is in the interval [i..j]?

$\mathbb{P}_{[i..j]}(\Diamond$  $)$

```
P>=i [ F<=n (state=INF) ]
P<=j [ F<=n (state=INF) ]
```

The probability of eventually getting infected is in the interval [i..j]?

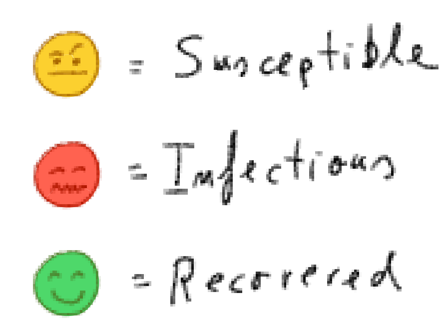
$\mathbb{P}_{[i..j]}(\Diamond$  $)$

```
P>=i [ F (state=INF) ]
P<=j [ F (state=INF) ]
```

The probability of eventually getting recovered is in the interval [i..j]?

$\mathbb{P}_{[i..j]}(\Diamond$  $)$

```
P>=i [ F (state=REC) ]
P<=j [ F (state=REC) ]
```



Probabilistic CTL

- Simple reachability probabilities
- PCTL Syntax
- PCTL Semantics
- Probabilistic Bounded Reachability
- Probabilistic Unbounded Reachability
- PCTL vs other Properties
- Exercises & Homework

PCTL - formal semantics

We define the formal semantics of PCTL as 2 relations.

A relation between states and **state formulas**:

$$s \models true \qquad \text{(holds always)}$$

$$s \models p \qquad \textit{iff} \;\; p \in L(s)$$

$$s \models \neg\phi \qquad \textit{iff} \;\; s \not\models \phi$$

$$s \models \phi_1 \wedge \phi_2 \qquad \textit{iff} \;\; s \models \phi_1 \textit{ and } s \models \phi_2$$

$$s \models \mathbb{P}_J(\psi) \qquad \textit{iff} \;\; Pr(\{\pi \in Paths(s) \mid \pi \models \psi\}) \in J$$

and a relation between paths and path formulas (next slide)

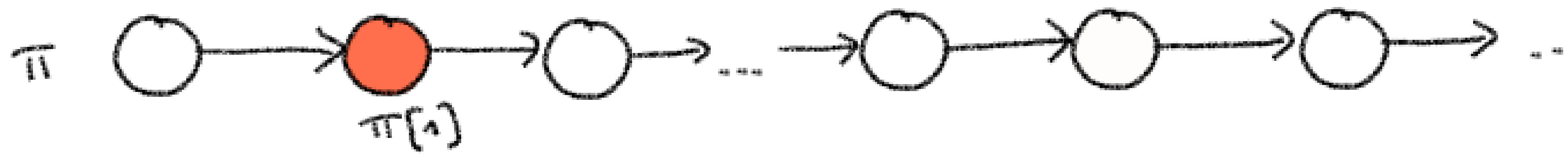
$$\pi \models \psi \qquad \textit{iff} \;\; \ldots$$

$$Pr_s(\psi) = Pr(\{\pi \in Paths(s) \mid \pi \models \psi\})$$

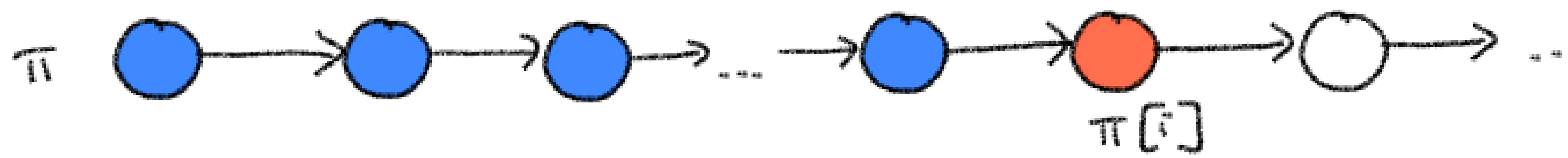
Semantics of path formulas

Here is the formal semantics of **path formulas**:

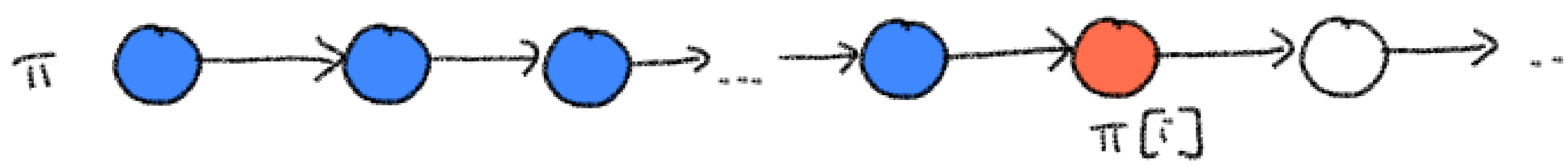
$\pi \vDash \bigcirc\, \phi$ $\quad$ *iff* $\pi[1] \vDash \phi$



$\pi \vDash \phi_1 \,\mathsf{U}\, \phi_2$ $\quad$ *iff* $\exists i \in \mathbb{N}.\, \pi[i] \vDash \phi_2 \wedge \forall 0 \leq j < i.\, \pi[j] \vDash \phi_1$



$\pi \vDash \phi_1 \,\mathsf{U}^{\leq n}\, \phi_2$ $\quad$ *iff* $\exists i \in \mathbb{N}.\, i \leq n \wedge \pi[i] \vDash \phi_2 \wedge \forall 0 \leq j < i.\, \pi[j] \vDash \phi_1$



where *i* and *j* are natural numbers

PCTL - formal semantics

The main new aspect is how to measure probabilities

$$s \vDash \mathbb{P}_J(\psi) \quad iff \quad Pr(\{\pi \in Paths(s) \mid \pi \vDash \psi\}) \in J$$

we may write Pr_s for an implicit "at state s"

We need to use the probability measure based on cylinder sets!

RECALL

Cylinder set probability measure: single paths as outcomes, sets of paths as events.

A finite path and all its possible (maximal) continuations in a Markov chain M define a set of paths called **cylinder set**:

$$cyl(s_0, .., s_n) = \{s_0, .., s_n\sigma \mid s_0, .., s_n\sigma \in Paths(M)\}.$$

Cylinder sets are the basis of the probability measure for sets of paths:

$$Pr(cyl(s_0, .., s_n)) = \iota(s_0) \prod_{0 \le i < n} P(s_i, s_{i+1})$$

One can prove that Pr is a probability measure:

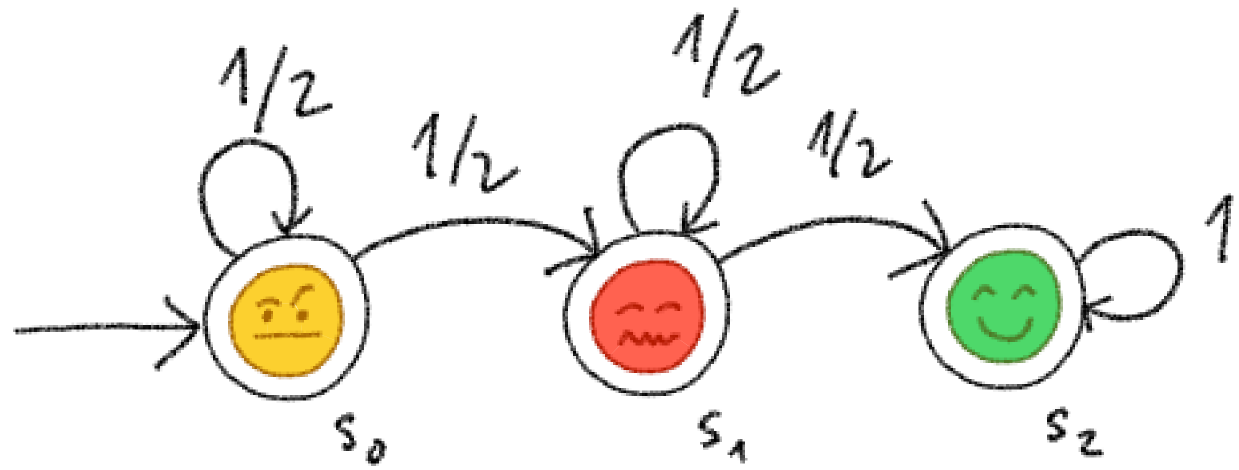
$$Pr(C \cup C') = Pr(C) + Pr(C') \qquad Pr(Paths(M) \setminus C) = 1 - Pr(C)$$

$$Pr(\bigcup_{i \geq 0} C_i) = \sum_{i=1}^{\infty} Pr(C_i) \qquad Pr(Paths(M)) = 1$$

$$Pr(\emptyset) = 0$$

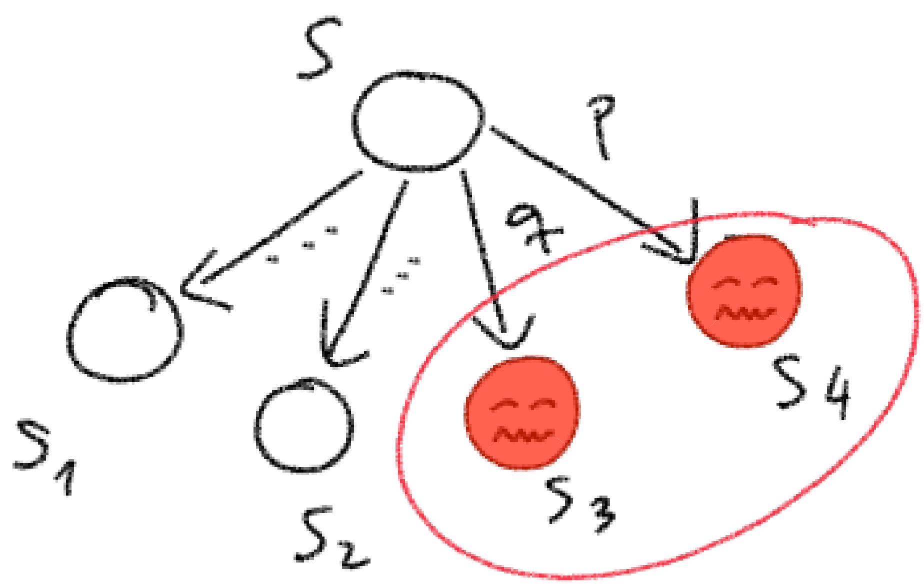
(for disjoint sets C, C' resp. C_i)

Next-Step probability in our example



What is the probability of getting infected tomorrow?

$$Pr_{s_0}(\bigcirc\ \ ) = 1/2$$



p + q

Computation tree (aka "path unrolling")

Next-Step probability in general

What is the probability of reaching a set B in one transition?

$$Pr_s(\bigcirc B) = \sum_{s' \in B} P(s, s')$$

We need to express the set of paths, that start from s and satisfy $\bigcirc B$, using operations on cylinder sets.

Can we express the set $\bigcirc B$ as a ***disjoint union*** of cylinder sets?

NOTE: abusing notation—as in the book—we write sets of states such as 'B' directly in the formulæ.

Next-Step probability in general

What is the probability of reaching a set B in one transition?

$$Pr_s(\bigcirc B) =$$

$$Pr_s(\{\pi \in Paths(s) \mid \pi[1] \in B\}) =$$

$$Pr_s\left(\bigcup_{s' \in Post(s)} \{\pi \in Path(s) \mid \pi[1] = s' \wedge \pi[1] \in B\}\right) =$$

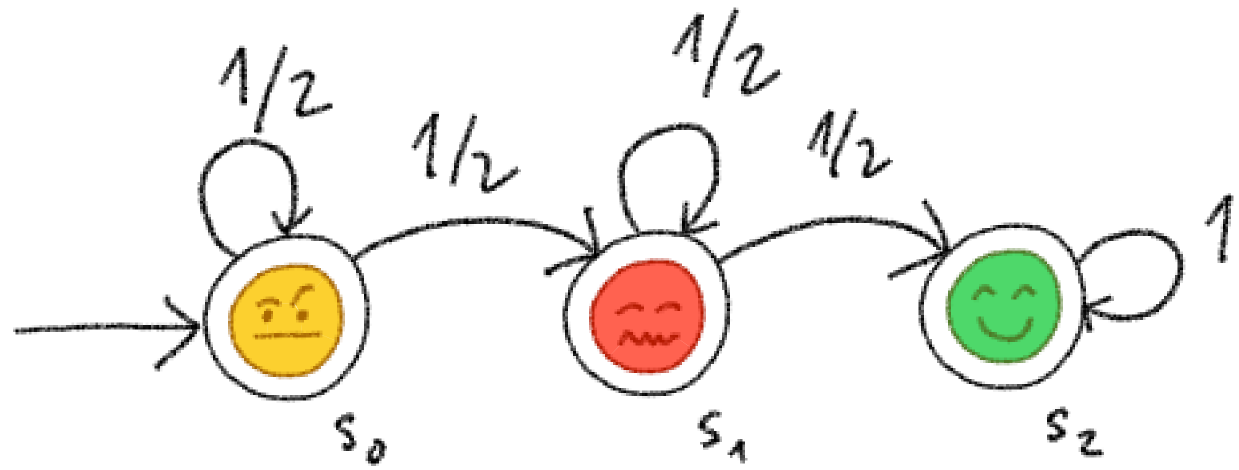
$$Pr_s\left(\bigcup_{s' \in B} cyl(s\, s')\right) =$$

$$\sum_{s' \in B} Pr_s(cyl(s, s')) = \sum_{s' \in B} P(s, s')$$

Probabilistic CTL

- Simple reachability probabilities
- PCTL Syntax
- PCTL Semantics
- Probabilistic Bounded Reachability
- Probabilistic Unbounded Reachability
- PCTL vs other Properties
- Exercises & Homework

Probabilistic Bounded Reachability in our example



What is the probability of getting infected in n days or less?

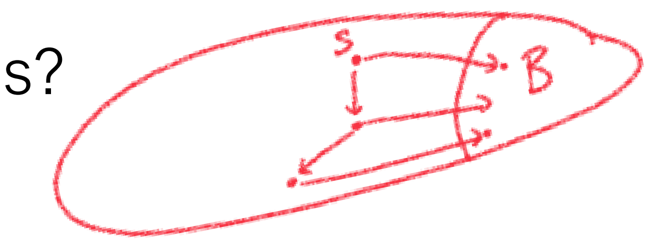
$$Pr_{s_0}(\Diamond^{\leq n} \;) = \ldots$$

	$Pr_{s_0}(\ldots)$
$\{\pi \in Paths(s_0) \mid \pi \models \Diamond^{\leq 0} \; \} = \emptyset$	0
$\{\pi \in Paths(s_0) \mid \pi \models \Diamond^{\leq 1} \; \} = cyl(s_0 s_1)$	$1/2$
$\{\pi \in Paths(s_0) \mid \pi \models \Diamond^{\leq 2} \; \} = cyl(s_0 s_1) \cup cyl(s_0 s_0 s_1)$	$1/2 + 1/4 = 3/4$

(bounded) path unrolling

Probabilistic Bounded Reachability in general

What is the probability of reaching a set $B \subseteq S$ in n or less transitions?



$$Pr_s(\Diamond^{\leq n} B) = \sum_{i=0}^{m} Pr(C_i)$$

We need to express the set of paths, that start from s and satisfy $\Diamond^{\leq n} B$, using operations on cylinder sets.

Can we express the set $\Diamond^{\leq n} B$ as a ***disjoint union*** of cylinder sets?

C_i

$$Pr(\{\pi \in Paths(s) \,/\, \pi \models \Diamond^{\leq m} B\})$$

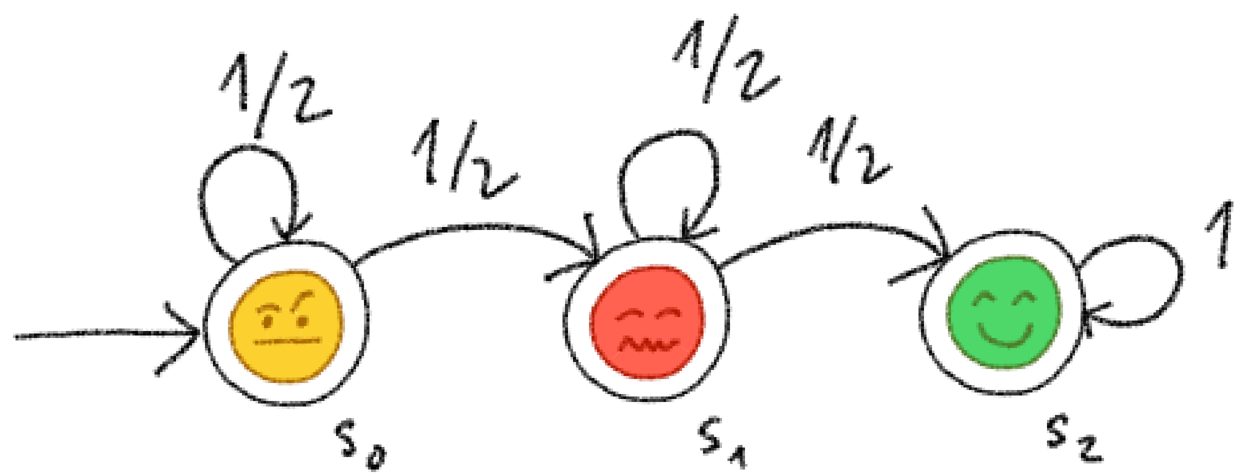
$$= Pr\Big(\bigcup_{0 \leq i \leq m} \{\pi \in Path(s) \,/\, \pi = \underbrace{s_0 s_1 s_2 \dots s_{i-1}}_{\notin B} \underbrace{s_i}_{\in B} \dots\}\Big)$$

S^B

$$= Pr\Big(\dot{\bigcup_{0 \leq i \leq m}} cyl(s_0 s_1 s_2 \dots s_{i-1} s_i)\Big)$$

$$= \sum_{0 \leq i \leq m} Pr(cyl(s_0 s_1 \dots s_i)) = \sum_{0 \leq i \leq m} \prod_{0 \leq j < i} P(s_j, s_{j+1})$$

Let's try with another example



What is the probability of getting recovered in 4 days or less?

$$Pr_{s_0}(\Diamond^{\leq 4}\ ) = \sum_{i=0}^{4} P_r(R_i) = \frac{11}{16}$$

$R_0 = \emptyset \longrightarrow 0$

$R_1 = \emptyset \longrightarrow 0$

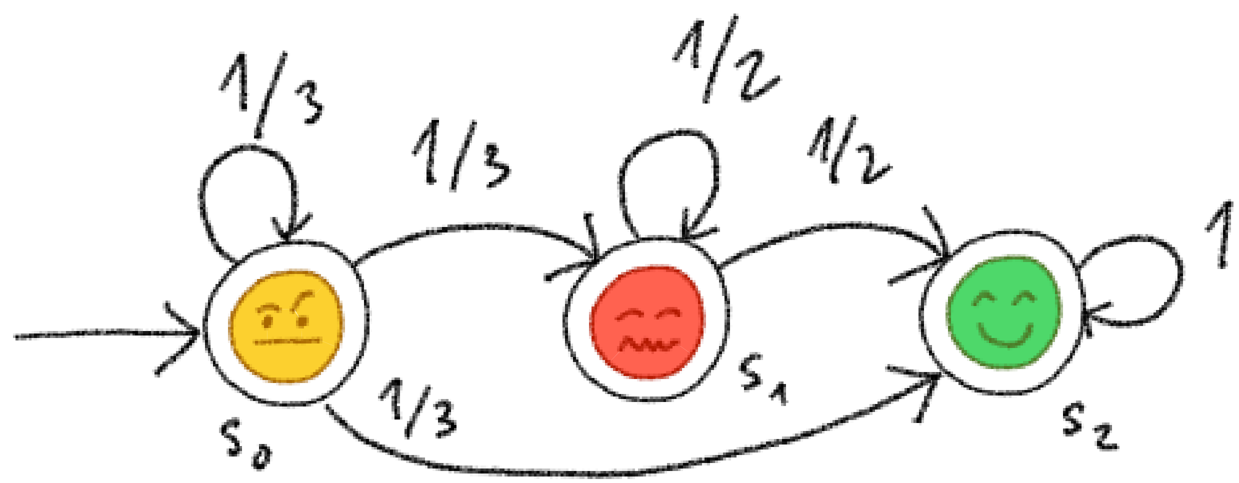
$R_2 = \{s_0\, s_1\, s_2 \dots\} = cyl(s_0 \overset{1/2}{\curvearrowright} s_1 \overset{1/2}{\curvearrowright} s_2) \rightarrow 1/4$

$R_3 = \{s_0\, s_0\, s_1\, s_2 \dots\} \cup \{s_0 \overset{1/2}{\frown} s_1 \overset{1/2}{\frown} s_1 \overset{1/2}{\frown} s_2 \dots\} \rightarrow 1/8 + 1/8 = 1/4$

$R_4 = \{s_0\, s_0\, s_0\, s_1\, s_2 \dots\} \cup \{s_0\, s_1\, s_1\, s_1\, s_2 \dots\} \cup \{s_0\, s_0\, s_1\, s_1\, s_2 \dots\} \rightarrow 3/16$

bounded path unrolling

What about until in general?



What is the probability of getting recovered in 3 or less days without getting infected?

$Pr_{s_0}(\neg$  $U^{\leq 3}$  $) = \frac{13}{27}$

$A_0 = \emptyset$

$A_1 = \{ s_0 s_2 \dots \} \longrightarrow 1/3$

$A_2 = \{ s_0 s_0 s_2 \dots \} \longrightarrow 1/9$

$A_3 = \{ s_0 s_0 s_0 s_2 \dots \} \rightarrow 1/3^3 = 1/27$

bounded path unrolling

Probabilistic Bounded Until in general

What is the probability of reaching a set $B \subseteq S$ in zero or more transitions, traversing only states in $C \subseteq S$ before reaching B ?

$$Pr_s(C \, \mathsf{U}^{\leq n} \, B) = \sum_{i=0}^{n} Pr(A_i)$$

We need to express the set of paths, that start from s and satisfy $C \, \mathsf{U} \, B$, using operations on cylinder sets.

Can we express the set $C \, \mathsf{U}^{\leq n} \, B$ as a ***disjoint union*** of cylinder sets?

$$A_i = \{ \pi \in Paths(s) \mid \pi = \underbrace{s_0 \, s_1 \, s_2 \dots s_{i-1}}_{\notin B, \ \boxed{\in C}} \, s_i \dots \}$$

$s_0 = s$, $s_i \in B$, $\boxed{i \leq n}$

Probabilistic CTL

- Simple reachability probabilities
- PCTL Syntax
- PCTL Semantics
- Probabilistic Bounded Reachability
- Probabilistic Unbounded Reachability
- PCTL vs other Properties
- Exercises & Homework

Probabilistic Unbounded Reachability in general

What is the probability of reaching a set $B \subseteq S$ in zero or more transitions?

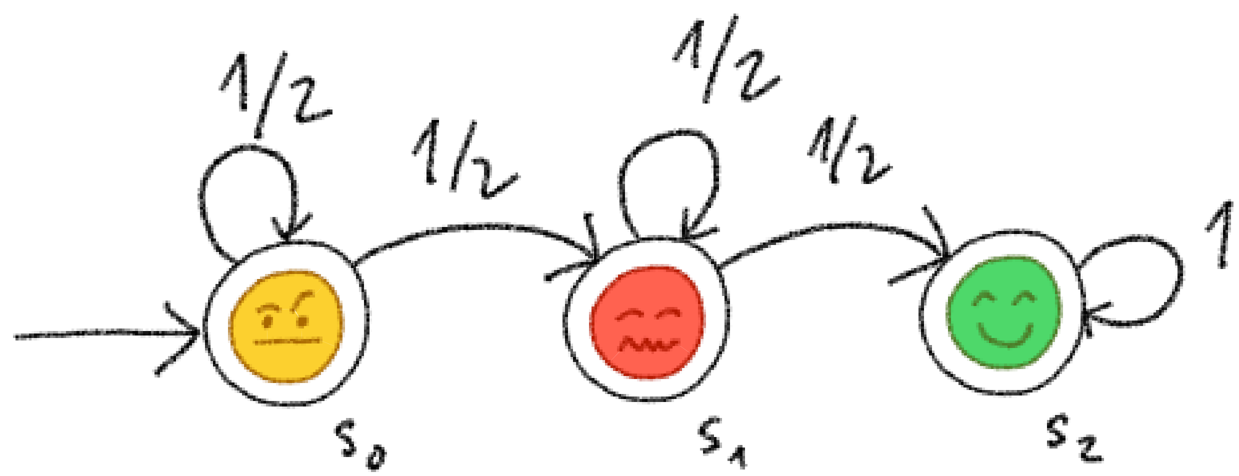
$$Pr_s(\Diamond B) = \sum_{i=0}^{\infty} Pr(C_i)$$

We need to express the set of paths, that start from s and satisfy $\Diamond B$, using operations on cylinder sets.

Can we express the set $\Diamond B$ as a ***disjoint union*** of cylinder sets?

$$C_i = \{ \pi \in Path(s) \,/\, \pi = \underbrace{\overset{s}{\overset{\parallel}{s_0}}\, s_1\, s_2 \,\ldots\, s_{i-1}}_{\notin B}\, \underset{B}{\underset{\cap}{s_i}} \ldots \}$$

Probabilistic <u>Un</u>bounded Reachability in our example



What is the probability of getting infected in 0 or more days?

$Pr_{s_0}(\Diamond$  $) = \sum_{i=0}^{\infty} Pr(I_i) =$

$$= Pr(I_0) + \sum_{i=1}^{\infty} Pr(I_i) = 0 + \sum_{i=1}^{\infty} Pr(I_i) = \sum_{i=1}^{\infty} 1/2^{i} = \sum_{i=0}^{\infty} 1/2^{i} - 1/2^{0}$$

$$= 2 - 1 = 1$$

$I_0 = \emptyset$

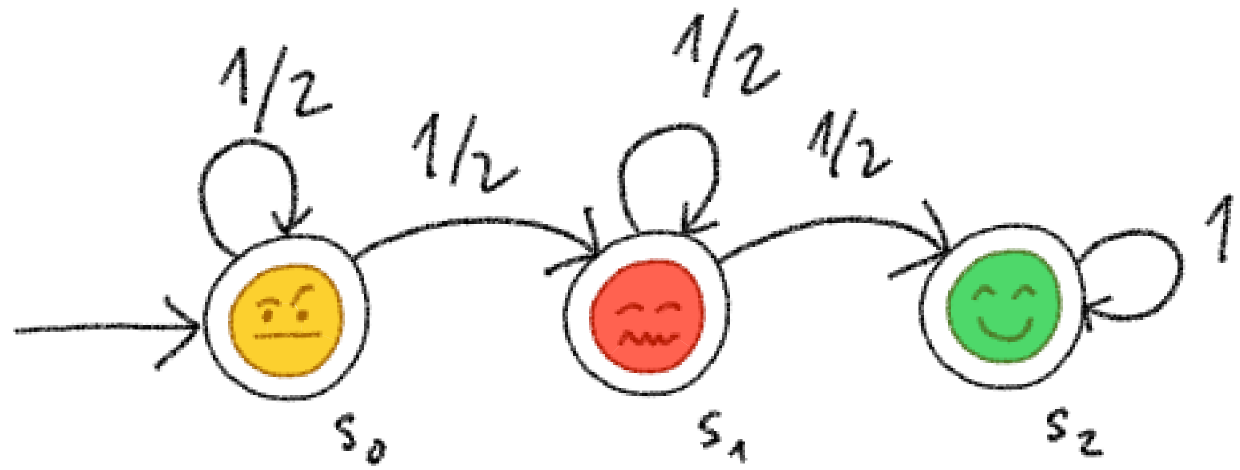
$I_i = \{ s_0^i \, s_1 \ldots \}$ for $i > 0$

$Pr(I_0) = 0$

$Pr(I_i) = 1/2^{i-1} \cdot 1/2$ for $i > 0$

$= 1/2^{i}$

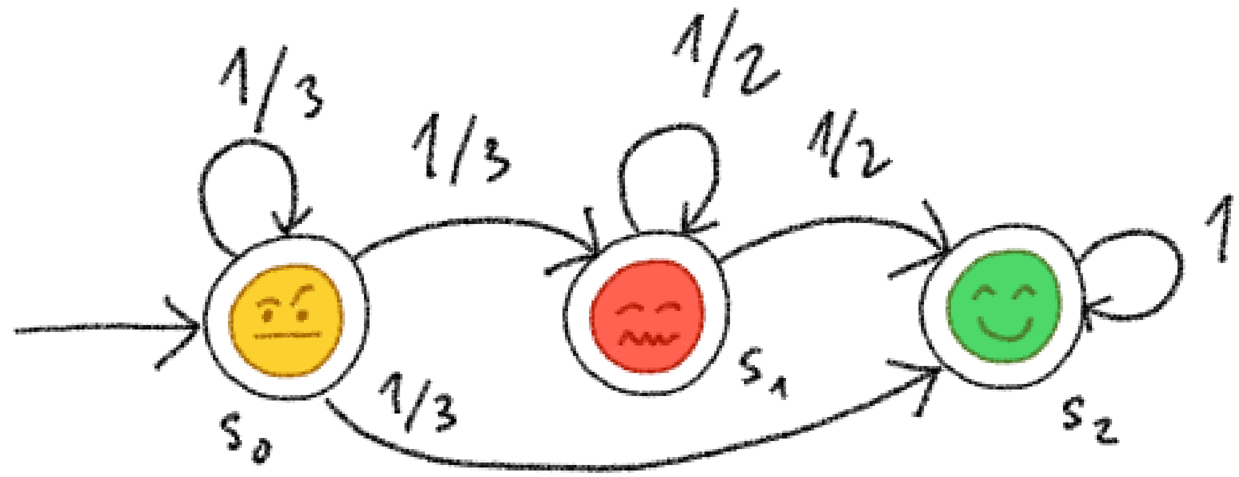
Let's try with another example



What is the probability of getting recovered in 0 or more days?

$$Pr_{s_0}(\Diamond \;\text{[smiley]}\;) = \ldots$$

What about until?



What is the probability of getting recovered in 0 or more days ***without getting*** infected?

$Pr_{s_0}(\neg$  U  $) = \ldots$

$A_i = \{ \pi \in Path(s_0) \mid \pi = s'_0 \, s'_1 \ldots s'_{i-1} \, s'_i \}$

$s'_0 = s_0$, $s'_i = s_2 \in$ 

$\underbrace{s'_0 \ldots s'_{i-1}}$ $\notin$ 

$\in \neg$ 

Probabilistic Unbounded Until in general

What is the probability of reaching a set $B \subseteq S$ in zero or more transitions, traversing only states in $C \subseteq S$ before reaching B ?

$$Pr_s(C \cup B) = \sum_{i=0}^{\infty} Pr(A_i)$$

We need to express the set of paths, that start from s and satisfy $C \cup B$,
using operations on cylinder sets.

Can we express the set $C \cup B$ as a *disjoint union* of cylinder sets?

$$A_i = \{ \pi \in Path(s) \,/\, \pi = \underbrace{\underset{\overset{\shortparallel}{s}}{s_0} \, s_1 \, s_2 \, \ldots \, s_{i-1}}_{\substack{\notin B \\ \in C}} \, \underset{\overset{\cap}{B}}{s_i} \ldots \}$$

Probabilistic CTL

- Simple reachability probabilities
- PCTL Syntax
- PCTL Semantics
- Probabilistic Bounded Reachability
- Probabilistic Unbounded Reachability
- PCTL vs other Properties
- Exercises & Homework

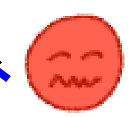
Probabilistic Bounded Reachability via Transient Distribution?

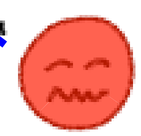
$$Pr_{s_0}(\Diamond^{\leq n} \quad) = \ldots$$

n	$Pr_{s_0}(\Diamond^{\leq n} \quad)$	$\theta_n(\quad)$
0		
1		
2		
3		
4	...	

Probabilistic **Un**bounded Reachability via Transient Distribution?

If only we could compute PCTL using transient distributions, we could skip some lectures!

$Pr_{s_0}(\Diamond^{\cancel{\leq n}}$  $) = \ldots$

n	$Pr_{s_0}(\Diamond^{\cancel{\leq n}}$  $)$	$\theta_n($  $)$
0		
1		
2		
3		
4	...	

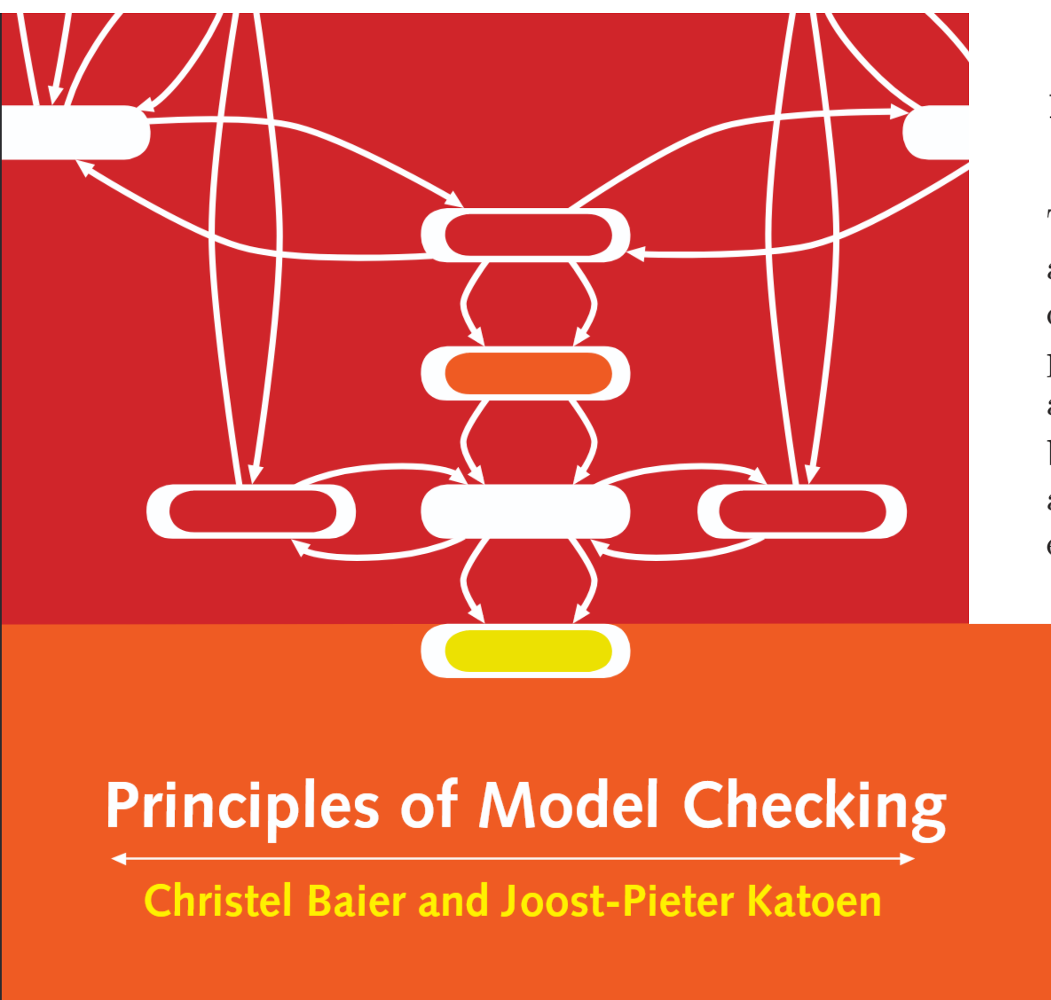
PCTL via CTL?

If only we could encode PCTL into CTL, we could skip the some lessons!

But… do the following statements hold?

$s \vDash \mathbb{P}_{>0}(\Diamond \phi)$ *iff* $s \vDash \exists \Diamond \phi$

$s \vDash \mathbb{P}_{=1}(\Diamond \phi)$ *iff* $s \vDash \forall \Diamond \phi$



10.2.2 The Qualitative Fragment of PCTL

The logic PCTL has been introduced as a variant of CTL where the path quantifiers $\exists$ and $\forall$ are replaced by the probabilistic operator $\mathbb{P}_J$. It is the purpose of this section to compare the expressiveness of CTL and PCTL in more detail. As PCTL provides the possibility to specify lower (or upper) bounds in the likelihood that they differ from zero and 1, as in $\mathbb{P}_{\geqslant \frac{1}{2}}(\varphi)$, it is evident that there exist properties that can be defined in PCTL but not in CTL. It remains to investigate how the *qualitative fragment* of PCTL—only allowing bounds with p=0 or p=1—relates to CTL. As we will see, these logics are not equally expressive, but are incomparable (though their common fragment is large).

Probabilistic CTL

- Simple reachability probabilities
- PCTL Syntax
- PCTL Semantics
- Probabilistic Bounded Reachability
- Probabilistic Unbounded Reachability
- PCTL vs other Properties
- Exercises & Homework

Key points of this lecture

PCTL as a logical language to express properties of probabilistic transition systems (DTMCs).

Formal semantics of PCTL.

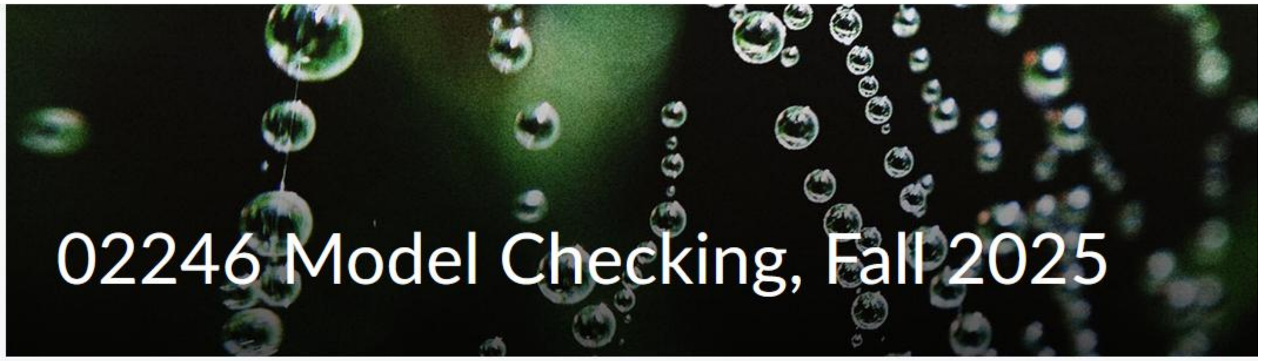
How probabilistic (bounded/unbounded) reachability is formalized with the cylinder set probability measure.

How PCTL relates to transient/steady state distributions.

How PCTL relates to CTL.

Research projects!

02246 Model Checking, Fall 2025



Announcements

What is the plan for the Assignment 05 - Research Project?

Alberto Lluch Lafuente posted on 22 October, 2025 16:39

What is the plan for the Assignment 05 - Research Project?

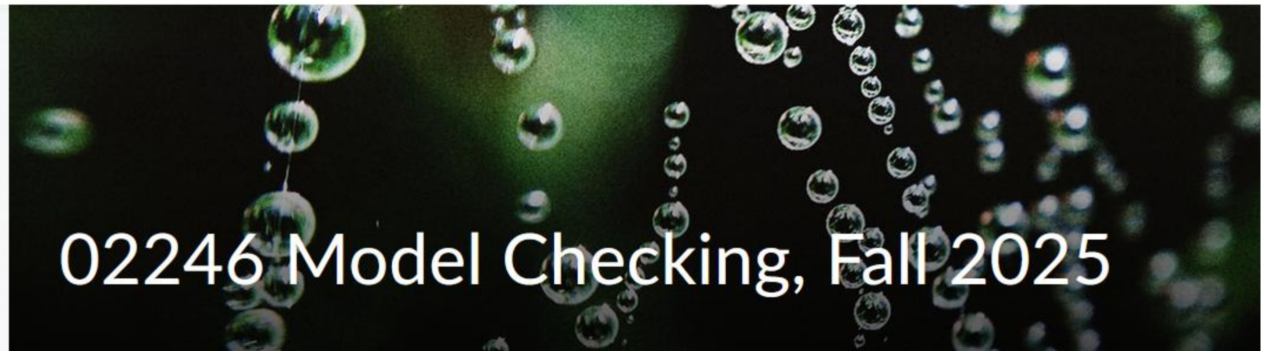
Before the lab sessions marked as "Research Lab":

- Read carefully the assignment description.
- Have a look at the recommended PRISM pages with benchmarks and case studies. This will give you an overview of different application domains where model checkers are used (distributed systems, security, biology, ...).

Research Lab 1 on Friday, 31 October

Research projects!

02246 Model Checking, Fall 2025



https://www.prismmodelchecker.org/casestudies/index.php

Case Studies

- Randomised distributed algorithms
- Communication, network and multimedia protocols
- Security
- Biology
- Planning and synthesis
- Game-theory
- Performance and reliability
- Power management
- CTMC benchmarks
- Miscellaneous

PRISM Case Studies

PRISM has been used to analyse a wide range of case studies in many different application domains. A no
detailed information about the case study, including PRISM language source code and experimental resul

We are always happy to include details of externally developed case studies. If you would like to contribut
pointer to a publication about your PRISM-related work, please contact us.

If you are interested in PRISM models for the purposes of **benchmarking**, see also the PRISM benchmark

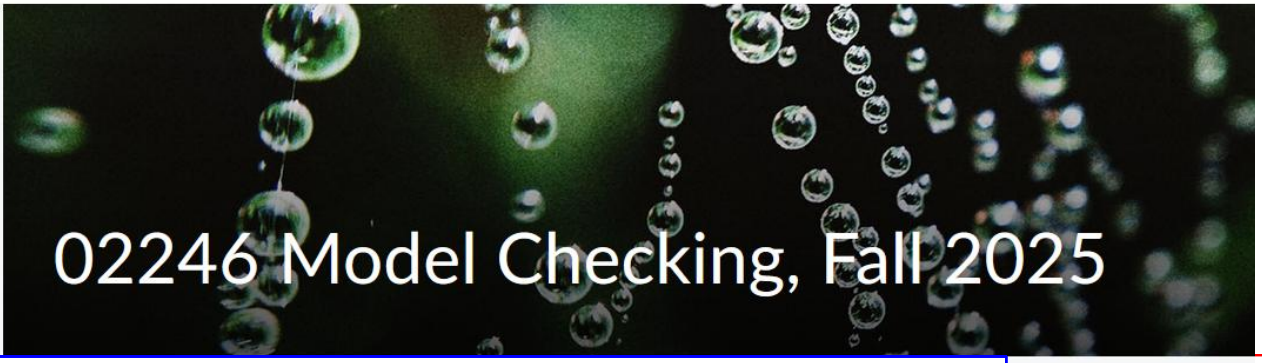
Randomised distributed algorithms

These case studies examine the correctness and performance of various *randomised distributed algorithm*

- Randomised self-stabilising algorithms (Herman) (Israeli & Jalfon) (Beauquier et al.) [KNP12a]
- Randomised two process wait-free test-and-set (Tromp & Vitanyi)
- Synchronous leader election protocol (Itai & Rodeh)
- Asynchronous leader election protocol (Itai & Rodeh)
- Randomised dining philosophers (Lehmann & Rabin)
- Randomised dining philosophers (Lynch, Saias & Segala)
- Dining cryptographers (Chaum)
- Randomised mutual exclusion (Rabin)
- Randomised mutual exclusion (Pnueli & Zuck)
- Randomised consensus protocol (Aspnes & Herlihy) (with Cadence SMV and PRISM) [KNS01a]
- Randomised consensus shared coin protocol (Aspnes & Herlihy) (with PRISM) [KNS01a]
- Byzantine agreement protocol (Cachin, Kursawe & Shoup) (with Cadence SMV and PRISM) [KN02]
- Byzantine agreement protocol (Cachin, Kursawe & Shoup) (with PRISM) [KN02]
- Rabin's Choice Coordination Problem [NM10]
  (contributed by Ukachukwu Ndukwu and Annabelle McIver)
- Dice programs (Knuth & Yao)

Research projects!

DTU | 02246 Model Checking, Fall 2025



https://qcomp.org/benchmarks/

https://www.prismmodelchecker.org
/casestudies/index.php

Quantitative Verification Benchmark Set

| License: CC-BY 4.0 | About | Contributing | JANI Converters

Licensing and Citations (CLOSE)

Arnd Hartmanns, Michaela Klauck, David Parker, Tim Quatmann, and Enno Ruijters: The Quantitative Verification Benchmark Set. Proceedings of the 24th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2019). Lecture Notes in Computer Science, vol. 11427, Springer, 2019.

Search

Show all models of type (all) / (all) with a (all) property and zero - infinity states

Models

Model ▼	Name	Type	Original	Params	States	Properties	Notes
beb	Bounded Exponential Ba...	MDP	Modest	3 (2/1)	4.53 k - 362 T	2 (2 × P)	(made for partial ...
bitcoin-at...	Andresen Attack on Bitc...	MA	Modest	2 (0/2)	252	2 (1 × Pb, 1 × E)	(optimal strategy ...
blockswo...	Blocksworld	MDP	PPDDL	1 (1/0)	1.13 k	1 (1 × P)	(IPPC 2008 bench...
bluetooth	Bluetooth Device Discov...	DTMC	PRISM	1 (0/1)	3.41 G - 55.3 G	1 (1 × E)	(PRISM benchmark)
boxworld	Boxworld	MDP	PPDDL	2 (2/0)		1 (1 × P)	(IPPC 2008 bench...
breakdo...	Queueing System with B...	MA	Modest	1 (0/1)	20.6 k - 242 k	2 (2 × P)	(nondeterministic ...
brp	Bounded Retransmission...	DTMC	PRISM	2 (0/2)	677 - 5.19 k	3 (3 × P)	(PRISM benchmark)
brp-pta	Bounded Retransmission...	PTA	Modest	4 (0/4)	3.96 k - 56.8 M	14 (10 × P, 2 × Pb, 2...	(scalable in multipl...
cabinets	Railway cabinets	MA	Galileo	3 (3/0)	28.3 k	2 (1 × Pb, 1 × S)	(rare event, small ...
cdrive	City Driving	MDP	PPDDL	1 (1/0)	38 - 2.19 k	1 (1 × P)	(IPPC 2006 bench...
cluster	Workstation Cluster	DTMC	PRISM	3 (0/3)	276 - 9.47 M	8 (4 × Pb, 2 × Eb, ...	(PRISM benchmark)

Research

studies in many different application domains. A no
RISM language source code and experimental resul

eveloped case studies. If you would like to contribut
k, please contact us.

of **benchmarking**, see also the PRISM benchmark

Project?

rmance of various *randomised distributed algorithm*

(Israeli & Jalfon) (Beauquier et al.) [KNP12a]
(Tromp & Vitanyi)
nmarks and case eh)
tion domains deh)
rity, biology, ...). bin)
Segala)

(Pnueli & Zuck)
ol (Aspnes & Herlihy) (with Cadence SMV and PRISM) [KNS01a]
coin protocol (Aspnes & Herlihy) (with PRISM) [KNS01a]
Cachin, Kursawe & Shoup) (with Cadence SMV and PRISM) [KN02]
Cachin, Kursawe & Shoup) (with PRISM) [KN02]
oblem [NM10]
ukwu and Annabelle McIver)

Probabilistic CTL

- Simple reachability probabilities
- PCTL Syntax
- PCTL Semantics
- Probabilistic Bounded Reachability
- Probabilistic Unbounded Reachability
- PCTL vs other Properties
- Exercises & Homework

APPENDIX: Exercises

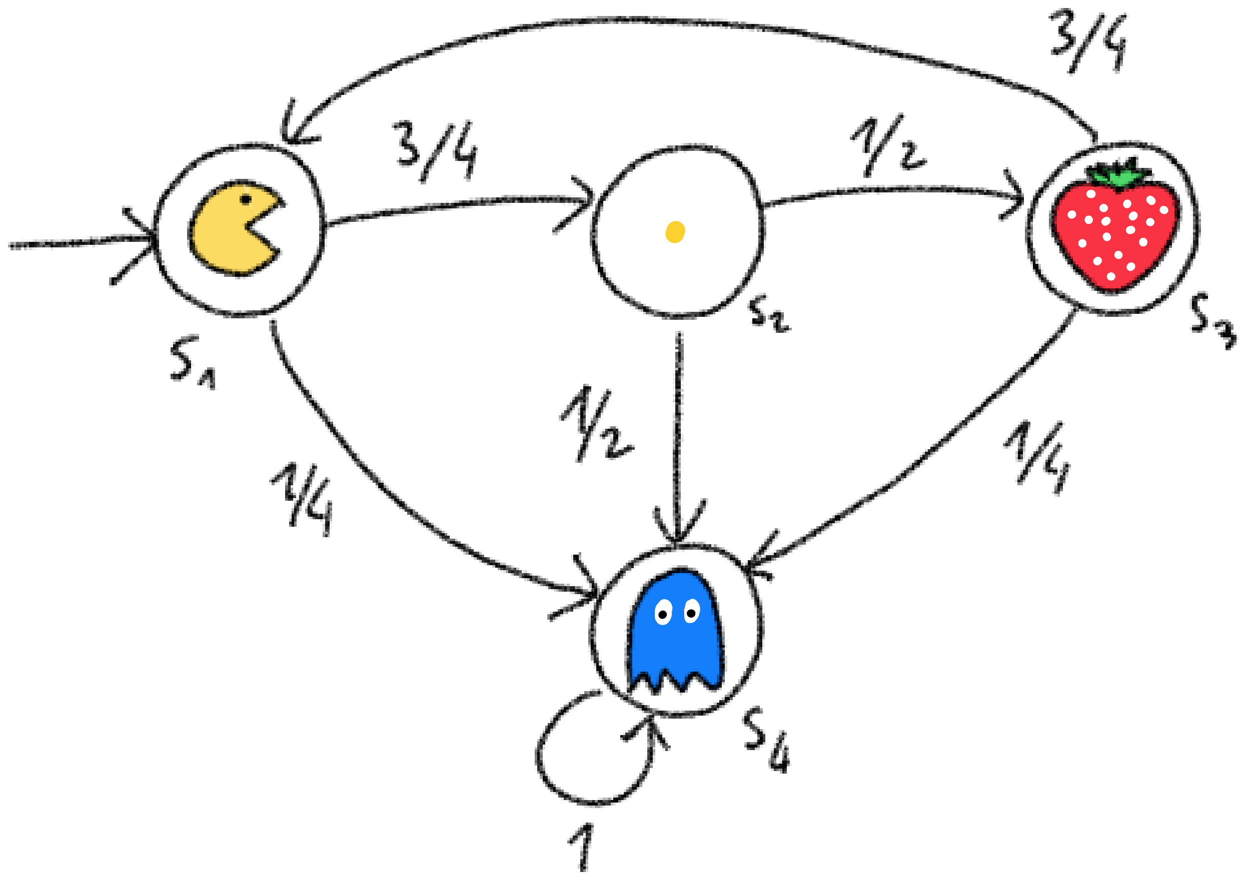
Exercise 07.1

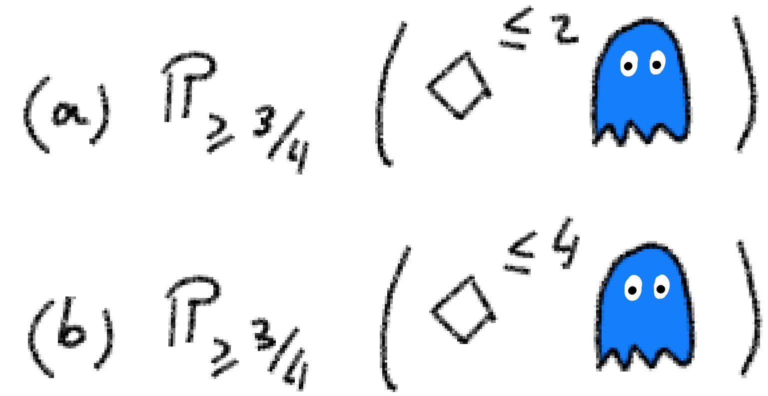
Write PCTL formulas for the following properties:

1. The probability that Pacman encounters a ghost is less than 20%.
2. Pacman almost never encounters a ghost.
3. The probability that Pacman reaches a strawberry within 10 transitions is higher than 25%.
4. The probability that Pacman reaches a strawberry without encountering a ghost is 2/3.

Exercise 07.2

For the transition system below verify if the initial state satisfies the following PCTL formulas:

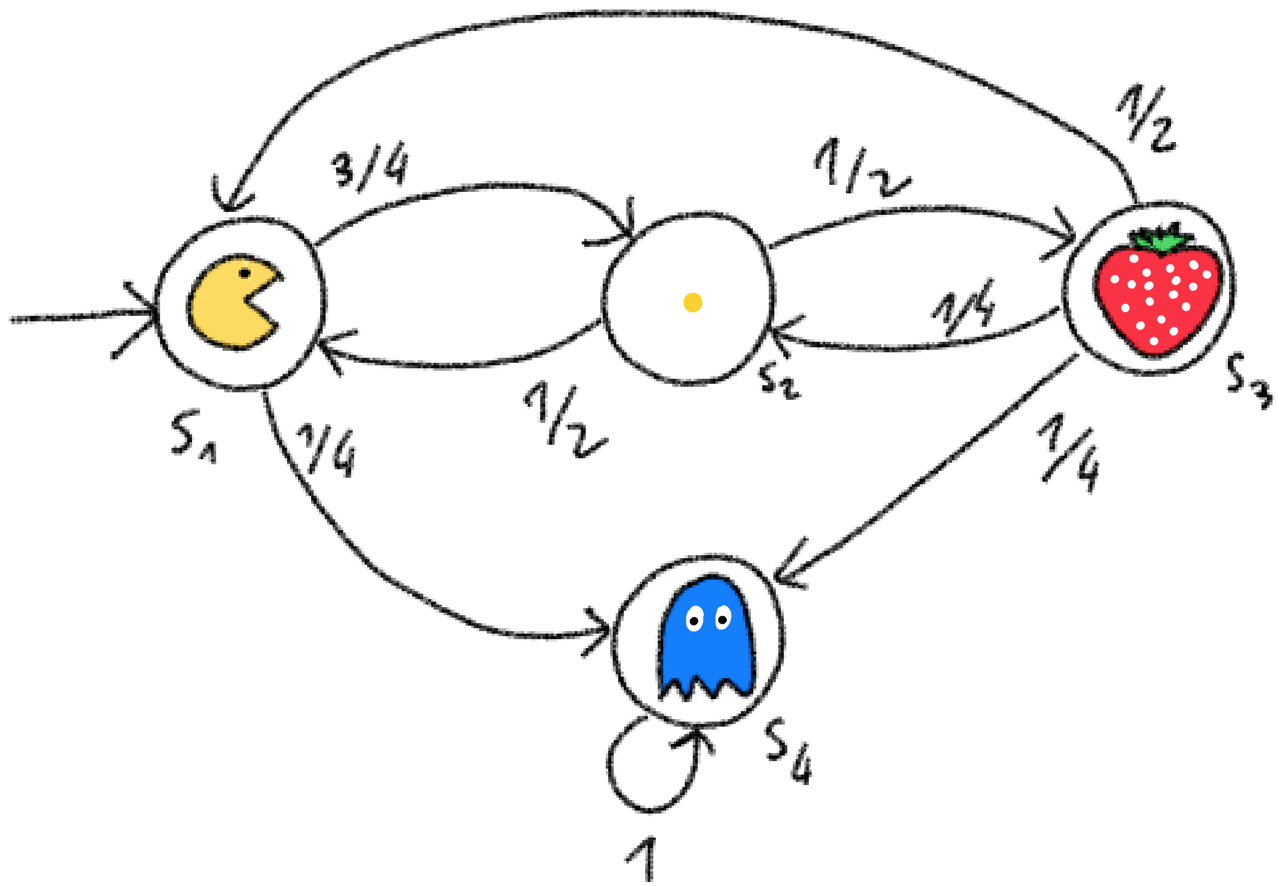


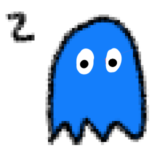


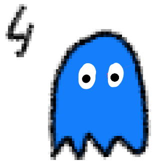
NOTE: *Do the computations using cylinder sets. You can then double-check your results with PRISM.*

Exercise 07.3

For the transition system below verify if the initial state satisfies the following PCTL formulas:



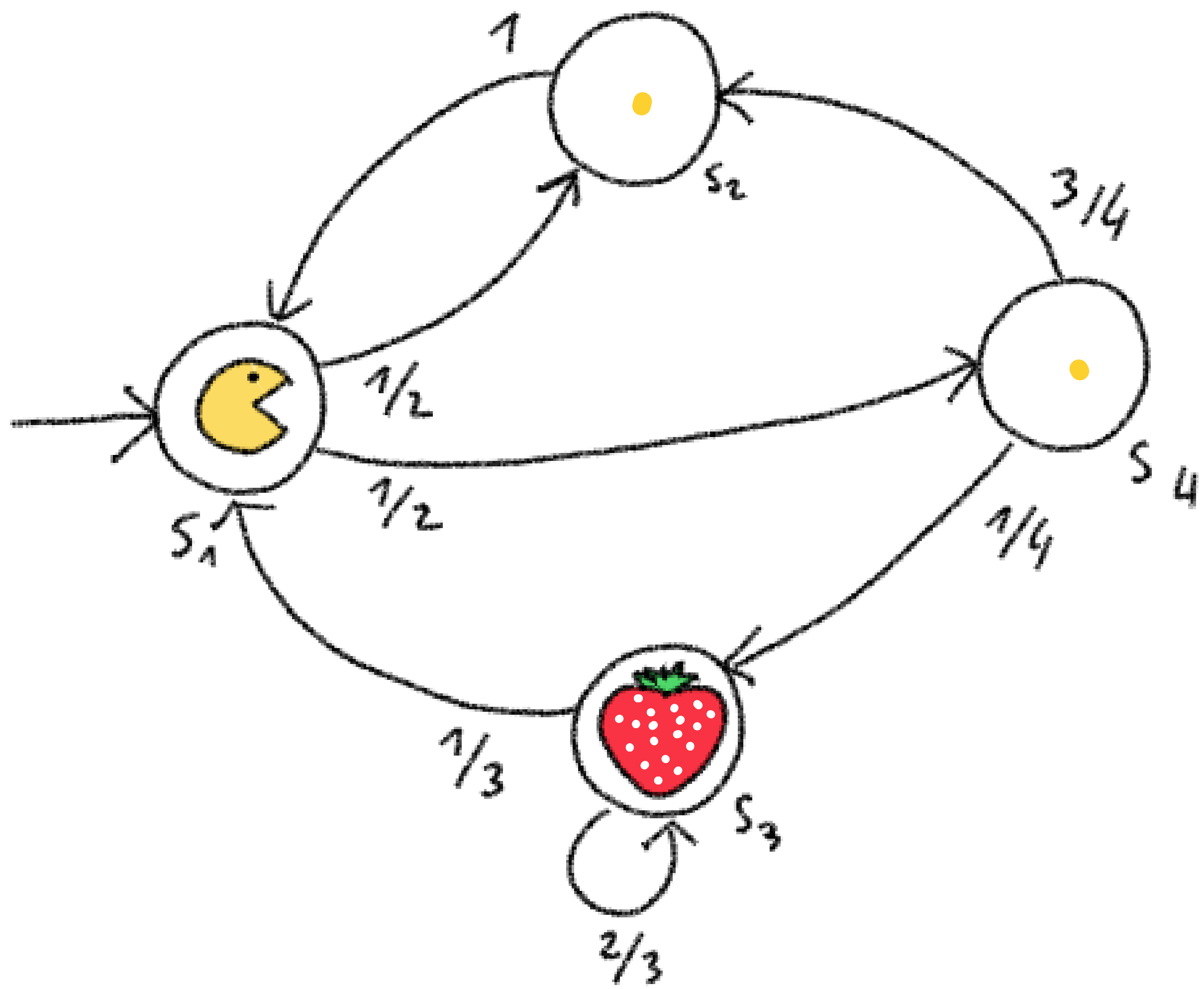
(a) $\mathbb{P}_{\geq 1/2}\left(\Diamond^{\leq 2}\right.$  $\left.\right)$

(b) $\mathbb{P}_{\geq 1/2}\left(\Diamond^{\leq 4}\right.$  $\left.\right)$

***NOTE**: Do the computations using cylinder sets. You can then double-check your results with PRISM.*

Exercise 07.4

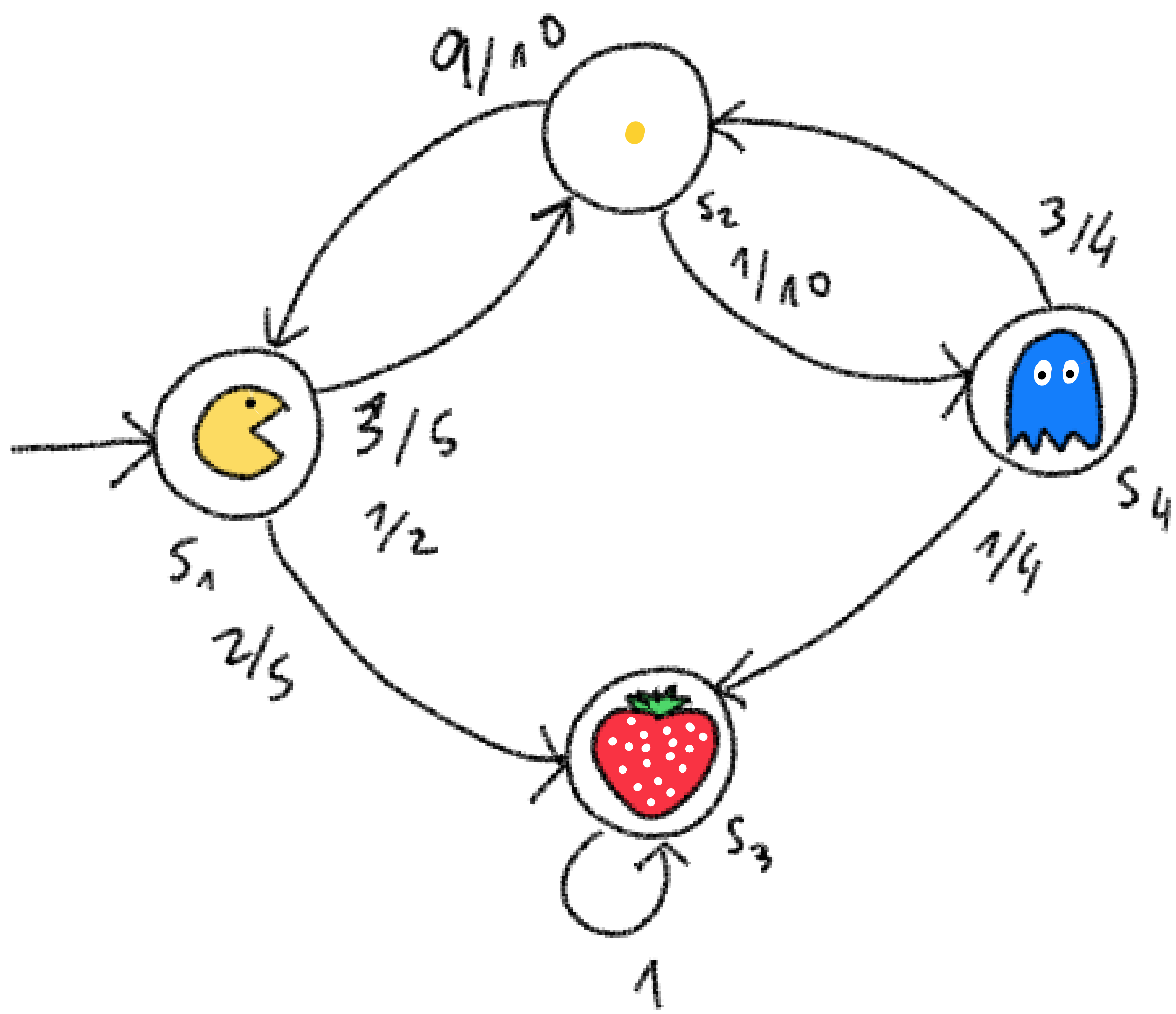
For the transition system below verify if the initial state satisfies the following PCTL formulas:

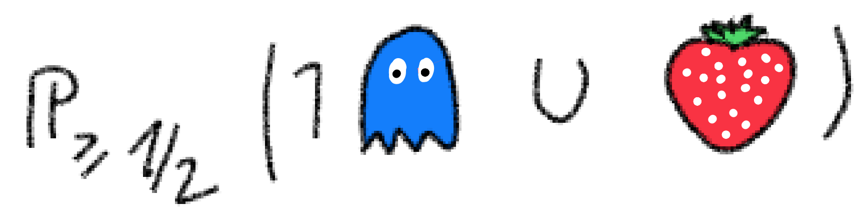


***NOTE**: Do the computations using cylinder sets. You can then double-check your results with PRISM.*

Exercise 07.5

For the transition system below verify if the initial state satisfies the following PCTL formulas:





NOTE: *Do the computations using cylinder sets. You can then double-check your results with PRISM.*

Exercise 07.6

For each of the following pairs of PTCL formulas, determine whether they are equivalent, one implies the other, or neither implies the other.

(a) $\mathbb{P}_{=1}(\Diamond\phi_1) \vee \mathbb{P}_{=1}(\Diamond\phi_2)$ vs $\mathbb{P}_{=1}(\Diamond(\phi_1 \vee \phi_2))$

(b) $\mathbb{P}_{\geq\frac{1}{4}}(\Diamond\phi_1) \vee \mathbb{P}_{\geq\frac{1}{4}}(\Diamond\phi_2)$ vs $\mathbb{P}_{\geq\frac{1}{4}}(\Diamond(\phi_1 \vee \phi_2))$

(c) $\mathbb{P}_{=1}(\bigcirc\mathbb{P}_{=1}(\Diamond^{\leq 1}\phi))$ vs $\mathbb{P}_{=1}(\Diamond^{\leq 2}\phi)$

(d) $\mathbb{P}_{\geq\frac{1}{2}}(\bigcirc\mathbb{P}_{\geq\frac{1}{2}}(\Diamond^{\leq 1}\phi))$ vs $\mathbb{P}_{\geq\frac{1}{2}}(\Diamond^{\leq 2}\phi)$

Use the formal semantics to argue in the positive cases, and counterexamples to argue in the negative cases.