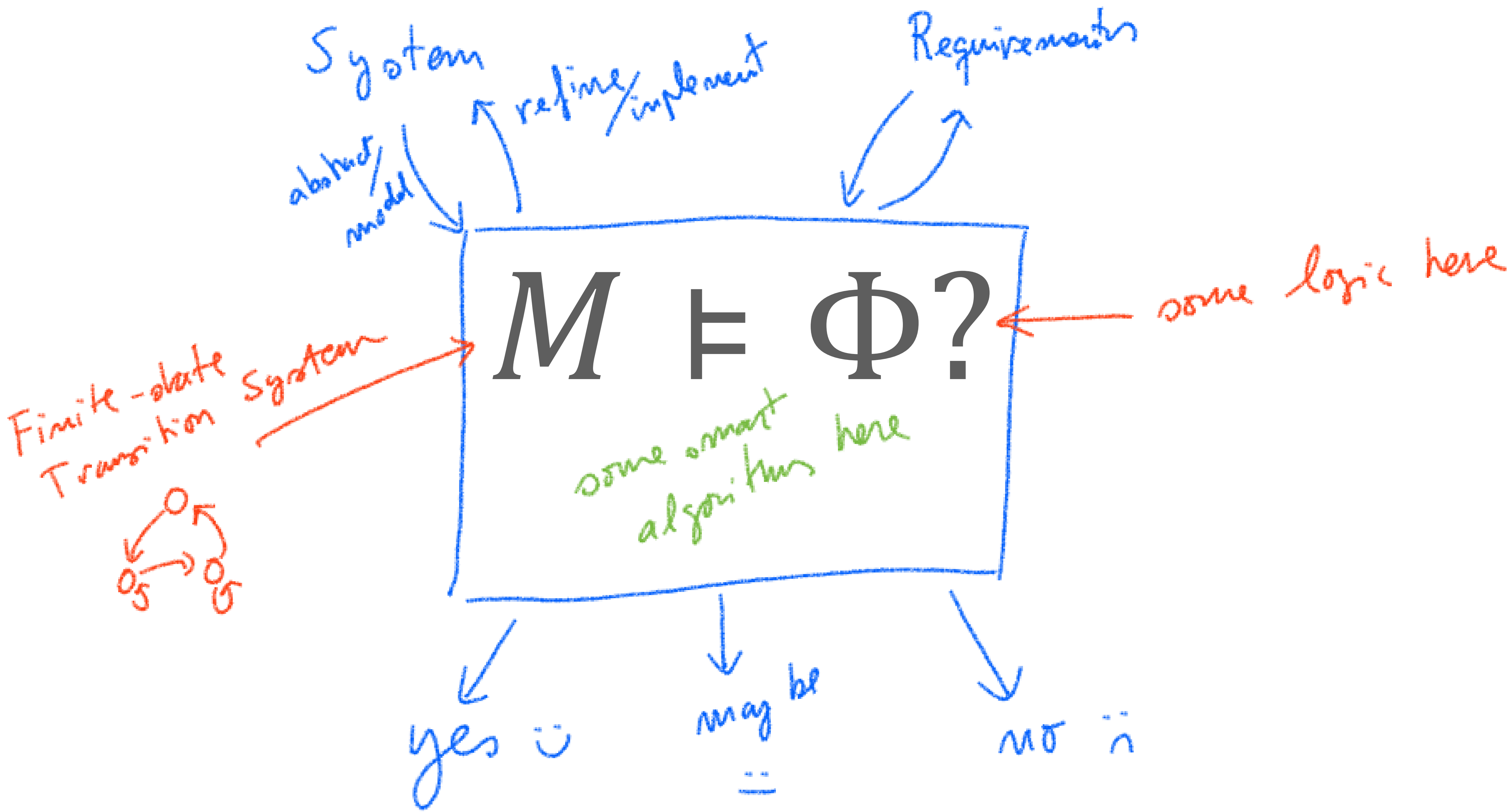
02246 - Model Checking

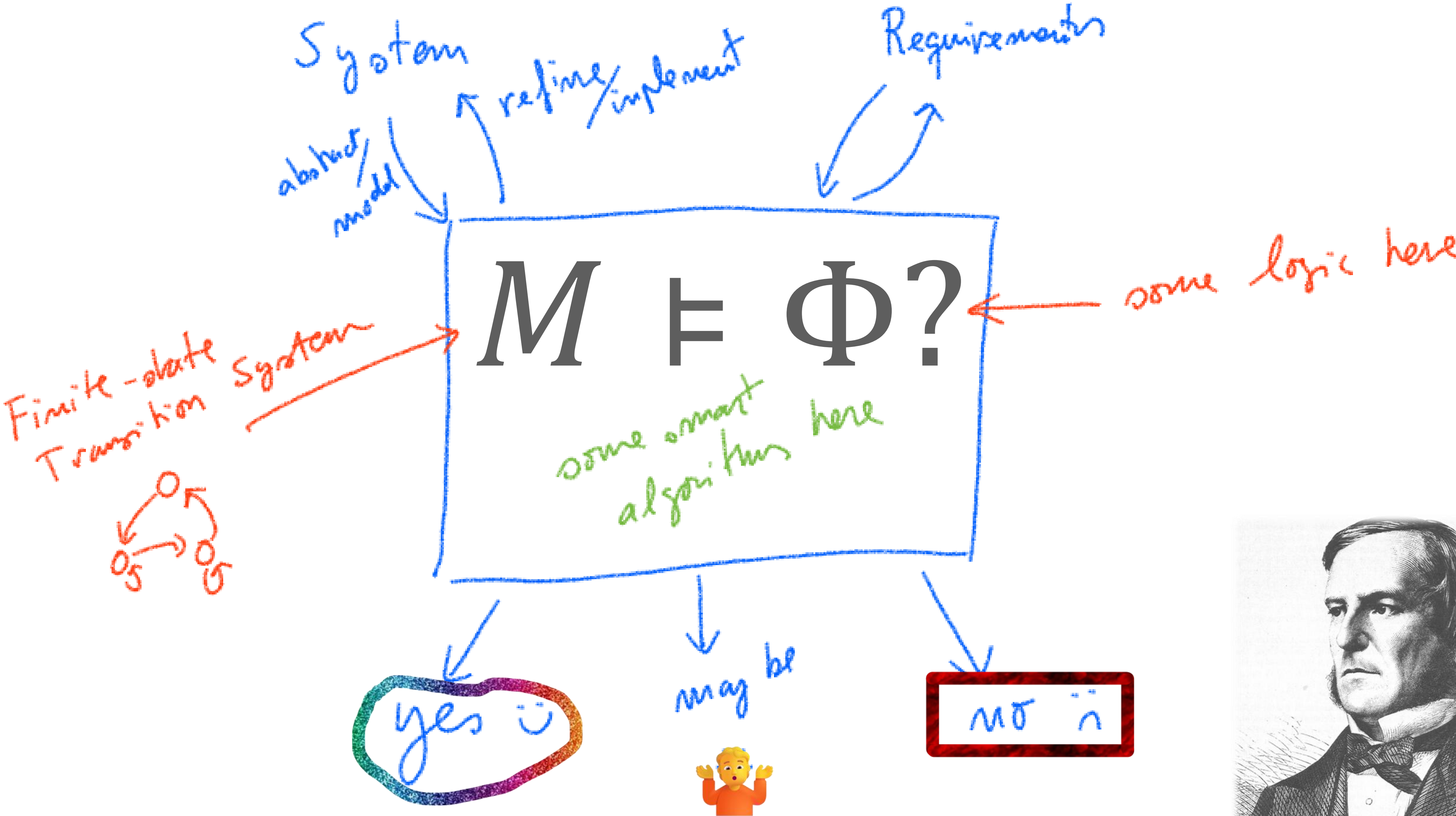
$$M \models \Phi?$$

Lecture 06 - Probabilistic Transition Systems

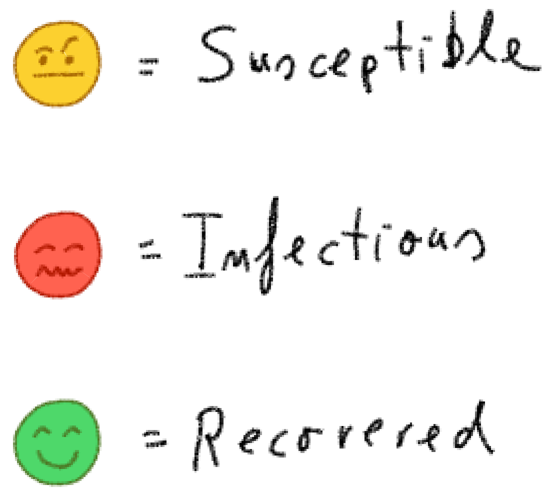
Technical University of Denmark

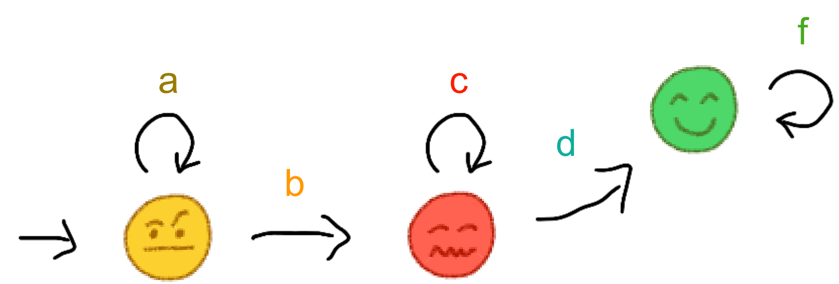


System
abstract/model
refine/implement
Requirements
$M \models \Phi$?
some logic here
Finite-state Transition System
some smart algorithms here
yes
maybe
no



$\top \leftarrow$ `$\top$` $\bot \leftarrow$ `$\bot$`


= Susceptible
= Infectious
= Recovered

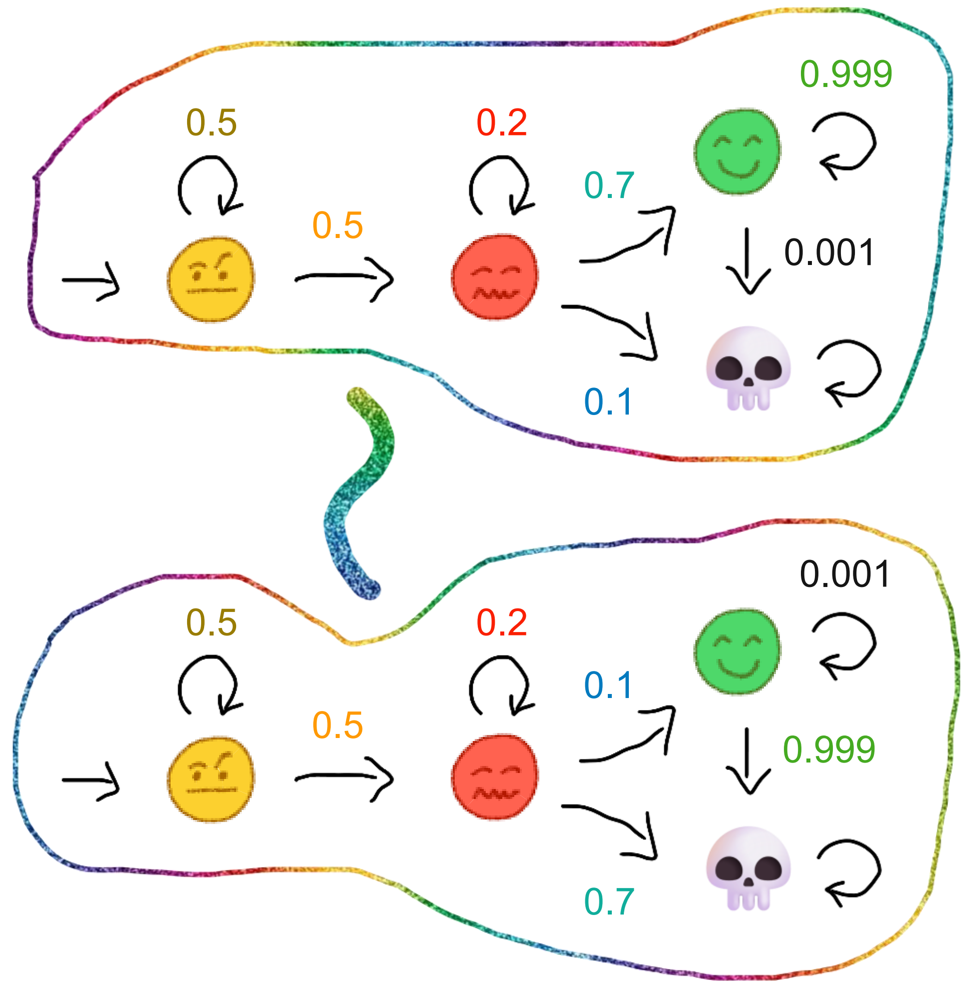

a
b
c
d
f

= Susceptible

= Infectious

= Recovered

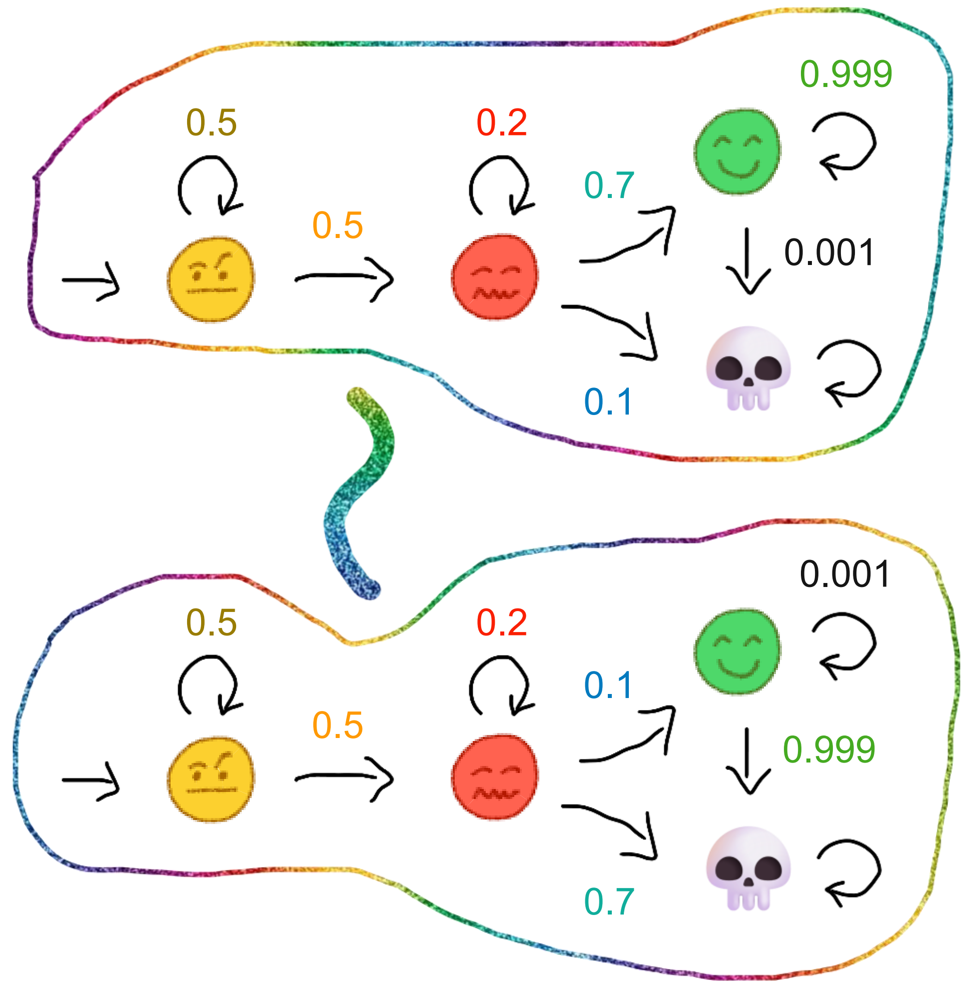
💀 = ded



$\forall \Diamond$ 💀

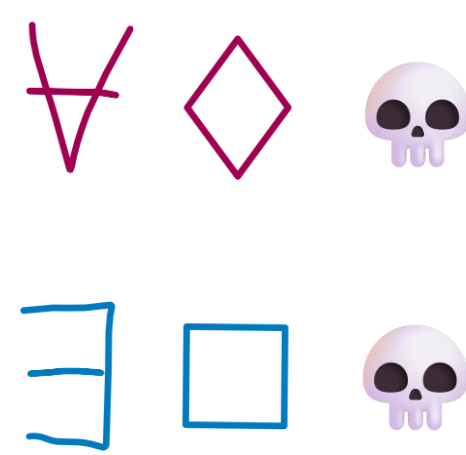
$\exists \Box$ 💀

Qua{l,nt}itative



(some) CTL formulæ

LaTeX - math	Alternative	PRISM
$\neg\varphi$	$\sim\varphi$	`!` φ
$\varphi_1 \wedge \varphi_2$	$\varphi_1 \wedge \varphi_2$	φ_1 `&` φ_2
$\varphi_1 \Rightarrow \varphi_2$	$\varphi_1 \rightarrow \varphi_2$	φ_1 `=>` φ_2
$\forall\,[\varphi_1\ U\ \varphi_2]$	$A\,[\varphi_1\ U\ \varphi_2]$	`P>=1 [`φ_1 `U` φ_2`]`
$\exists\,[\varphi_1\ U\ \varphi_2]$	$E\,[\varphi_1\ U\ \varphi_2]$	`!P<=0 [`φ_1 `U` φ_2`]`
$\forall\bigcirc\varphi$	$AX\varphi$	`P>=1 [ X` φ `]`
$\exists\square\varphi$	$EG\varphi$	`!P<=0 [ G` φ `]`
$\forall\lozenge\,[\varphi_1 \vee \varphi_2]$	$AF[\varphi_1 \vee \varphi_2]$	`P>=1 [`φ_1 `|` φ_2`]`



Qua{l,nt}itative

Chapter 10

Probabilistic Systems

Whereas model-checking techniques focus on the absolute guarantee of correctness — "it is impossible that the system fails" — in practice such rigid notions are hard, or even impossible, to guarantee. Instead, systems are subject to various phenomena of a stochastic nature, such as message loss or garbling and the like, and correctness — "with 99% chance the system will not fail" — is becoming less absolute. This chapter considers the automated verification of *probabilistic* systems, i.e., systems that exhibit probabilistic aspects[1]. Probabilistic aspects are essential for, among others:

- Randomized algorithms. Typical examples are distributed algorithms like leader election or consensus algorithms where coin-tossing experiments are used to break

Principles of Model Checking

Christel Baier and Joost-Pieter Katoen

Key points of this lecture

Definition of Discrete-Time Markov Chain (DTMC), a probabilistic variant of transition systems.

Transient distribution of a DTMC, an indication of the probability of being in each of the states after n steps.

Steady state distribution, a stationary distribution that, in some cases, coincides with the limit of the transient distribution.

How to measure the probability of simple reachability properties by hand.

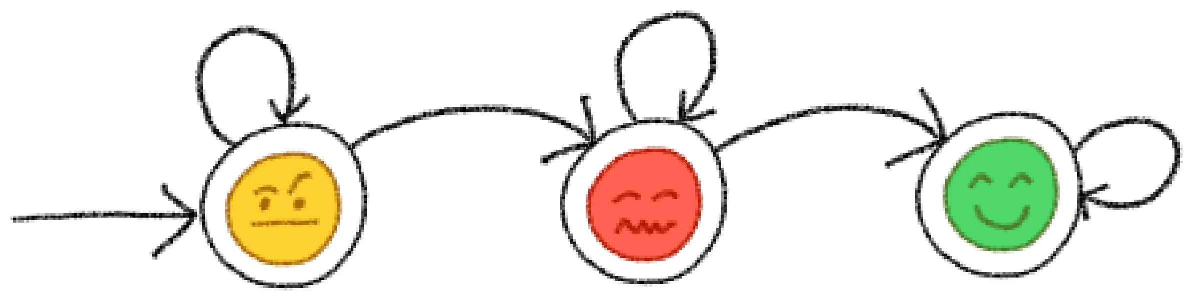
How to measure the probability of (certain) sets of paths in a DTMC.

How to use PRISM and Z3 to compute transient state distributions, steady states distributions and reachability probabilities.

Discrete-Time Markov Chains

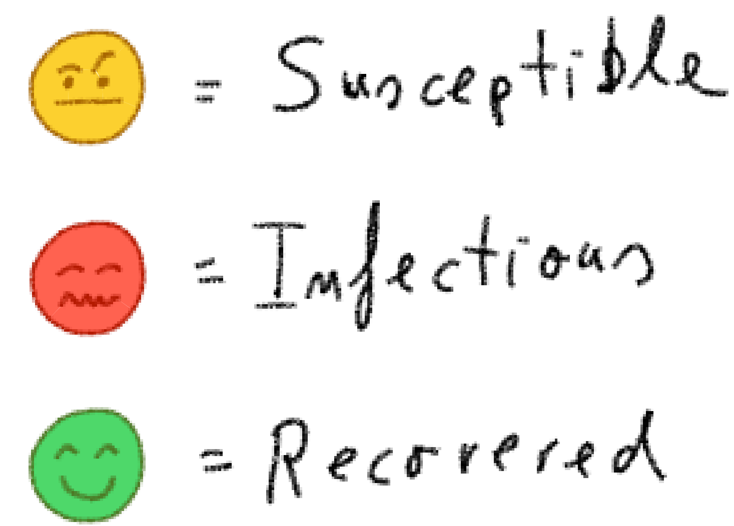
- Discrete-Time Markov Chains (DTMCs)
- Transient Distributions
- Steady State Distribution
- Reachability Probabilities
- Probabilities of Sets of Paths
- Exercises & Homework

The SIR model



Old question: can X happen?

Example: **EF** *infections*

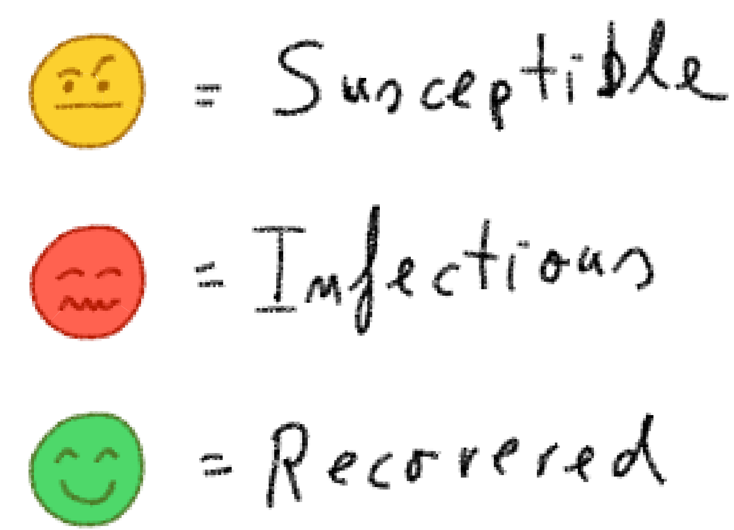


The SIR model

Move from **possibilistic** to **probabilistic** !

Old question: can X happen?

New question: what's the probability that X happens?



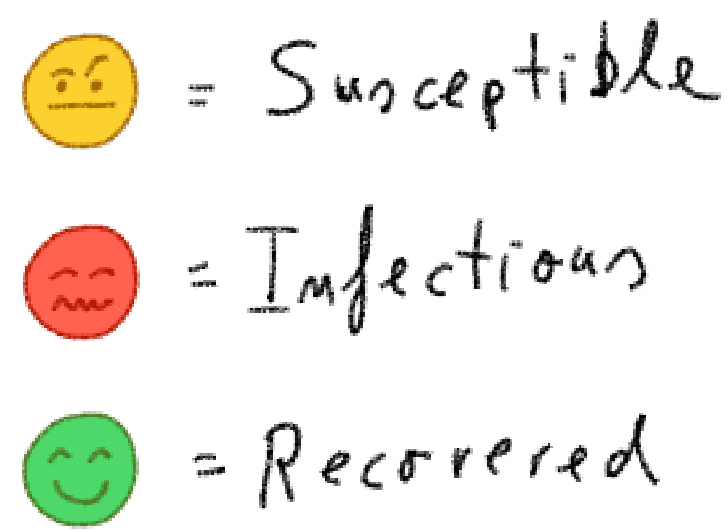
The SIR model

Old question: can X happen?

New question: what's the probability that X happens?

<u>Example-1</u>: what is the probability of getting infected in the long run?

<u>Example-2</u>: what is the probability of **never** getting infected in the long run?



Modeling in PRISM

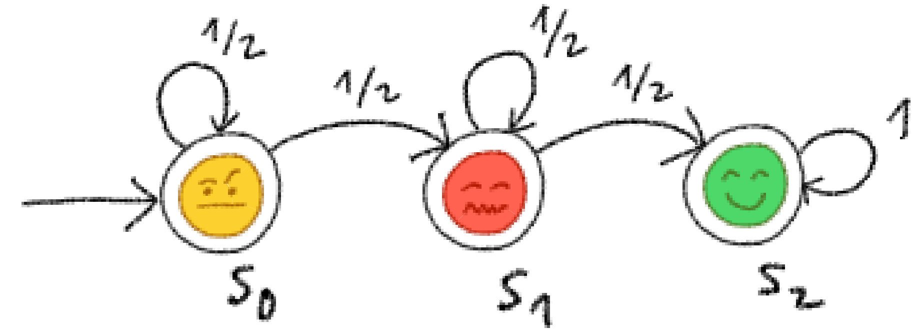
```
dtmc

module M

s : [0..2] init 0;

[] (s = 0) -> 1/2 : (s'=0)
            + 1/2 : (s'=1);

[] (s = 1) -> 1/2 : (s'=1)
            + 1/2 : (s'=2);

[] (s = 2) -> 1 : (s'=2);
endmodule
```

Notice: multiple transition options, probabilities must sum to 1

Discrete-Time Markov Chains

A **Discrete-Time Markov Chain** (DMTC) is a tuple

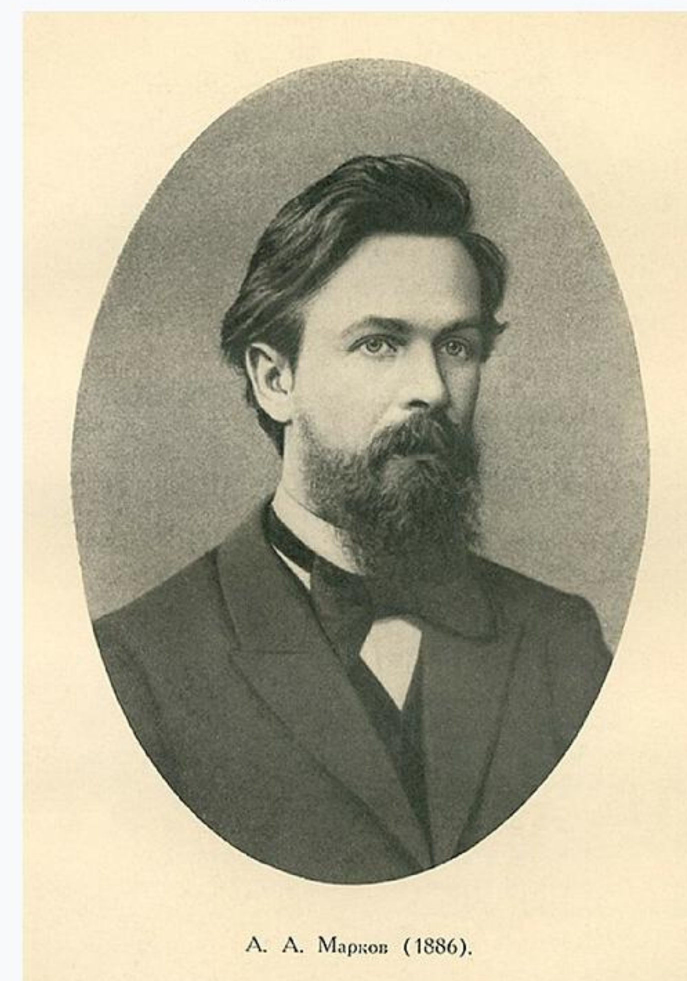
$$(S, P, \iota, AP, L)$$



such that:

- S is a finite, a non-empty set of states
- $P: S \times S \to [0,1]$ is a **probabilistic transition function**, i.e. such that for all $s' \in S$:
$$\sum_{s' \in S} P(s, s') = 1$$
- $\iota: S \to [0,1]$ is an **initial distribution**, i.e. such that
$$\sum_{s \in S} \iota(s) = 1$$
- AP is a set of atomic propositions
- L is a labelling function

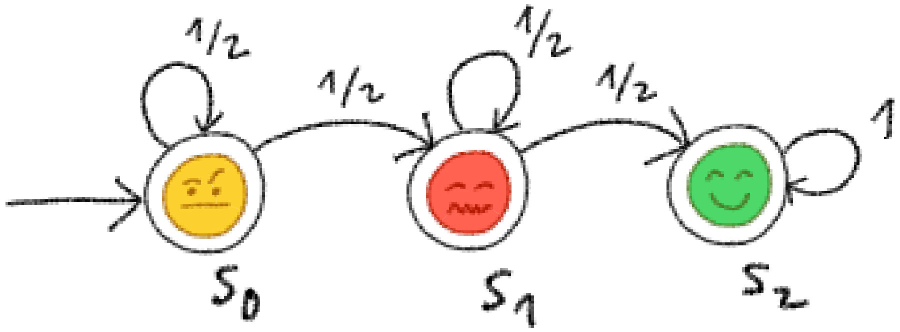
Andrey Markov
Андрей Марков



https://en.wikipedia.org/wiki/Andrey_Markov

Discrete-Time Markov Chains

A **Discrete-Time Markov Chain** (DMTC) is a tuple



$$(S, P, \iota, AP, L)$$

such that:

- S is a finite, a non-empty set of states
- $P: S \times S \to [0,1]$ is a **probabilistic transition function**, i.e. such that for all $s' \in S$:

$$\sum_{s' \in S} P(s, s') = 1$$

Probability of moving from s to s' in one step

Probability distributions evolve with every step!

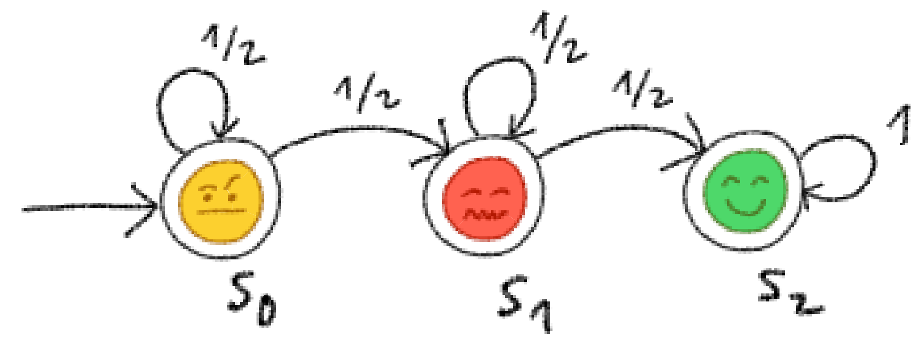
- $\iota: S \to [0,1]$ is an **initial distribution**, i.e. such that

$$\sum_{s \in S} \iota(s) = 1$$

- AP is a set of atomic propositions
- L is a labelling function

Discrete-Time Markov Chains

A **Discrete-Time Markov Chain** (DMTC) is a tuple



$$(S, P, \iota, AP, L)$$

such that:

- S is a finite, a non-empty set of states
- $P: S \times S \rightarrow [0,1]$ is a **probabilistic transition function**, i.e. such that for all $s' \in S$:
$$\sum_{s' \in S} P(s, s') = 1$$
- $\iota: S \rightarrow [0,1]$ is an **initial distribution**, i.e. such that
$$\sum_{s \in S} \iota(s) = 1$$
- AP is a set of atomic propositions
- L is a labelling function

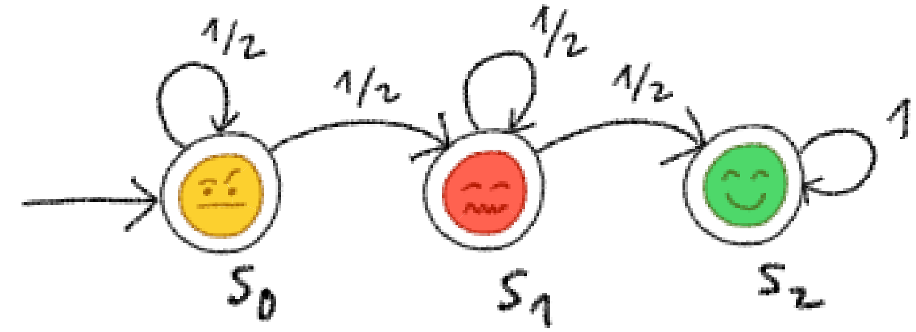
Columns: probability to enter a state from any other state

$$P = \begin{array}{c} \begin{array}{ccc} s_0 & s_1 & s_2 \end{array} \\ \begin{pmatrix} 1/2 & 1/2 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & 0 & 1 \end{pmatrix} \end{array} \begin{array}{c} s_0 \\ s_1 \\ s_2 \end{array}$$

Transition probability matrix (contains all transition probabilities)

Rows: probability from a state to its successor

Discrete-Time Markov Chains



A **Discrete-Time Markov Chain** (DMTC) is a tuple

$$(S, P, \iota, AP, L)$$

such that:

- S is a finite, a non-empty set of states
- $P: S \times S \to [0,1]$ is a **probabilistic transition function**, i.e. such that for all $s' \in S$:

$$\sum_{s' \in S} P(s, s') = 1$$

$$P = \begin{array}{ccc} s_0 & s_1 & s_2 \end{array}$$
$$P = \begin{pmatrix} 1/2 & 1/2 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & 0 & 1 \end{pmatrix} \begin{array}{c} s_0 \\ s_1 \\ s_2 \end{array}$$

- $\iota: S \to [0,1]$ is an **initial distribution**, i.e. such that

$$\sum_{s \in S} \iota(s) = 1$$

$$\iota = \begin{array}{c} \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \\ \begin{array}{ccc} s_0 & s_1 & s_2 \end{array} \end{array}$$

- AP is a set of atomic propositions
- L is a labelling function

Examples

You will find lots of examples in the book…

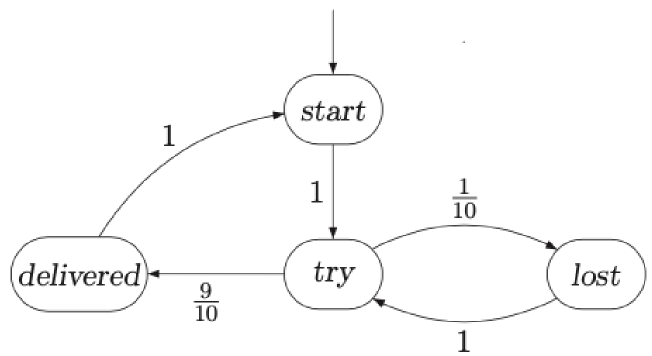


Figure 10.1: Markov chain for a simple communication protocol.

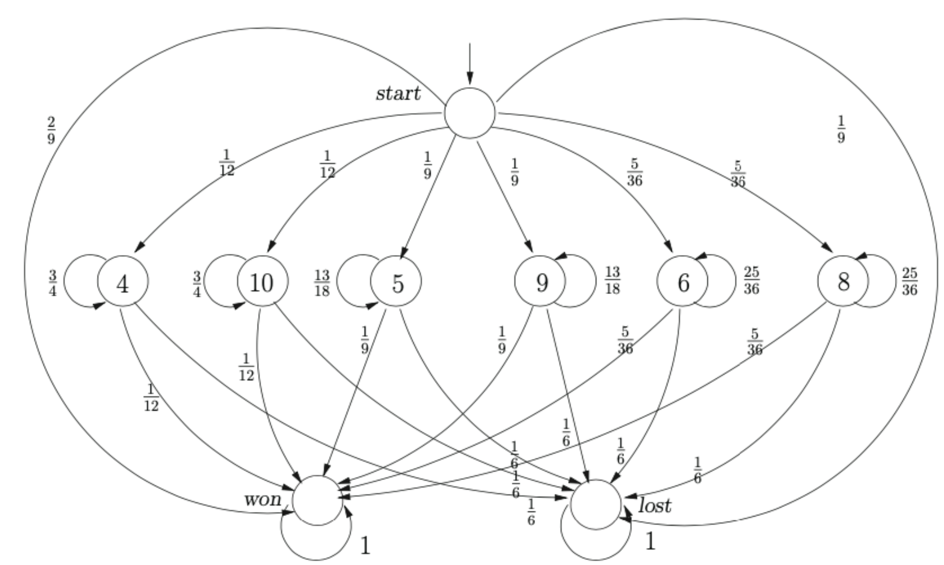


Figure 10.3: Markov chain for the behavior of the craps game.

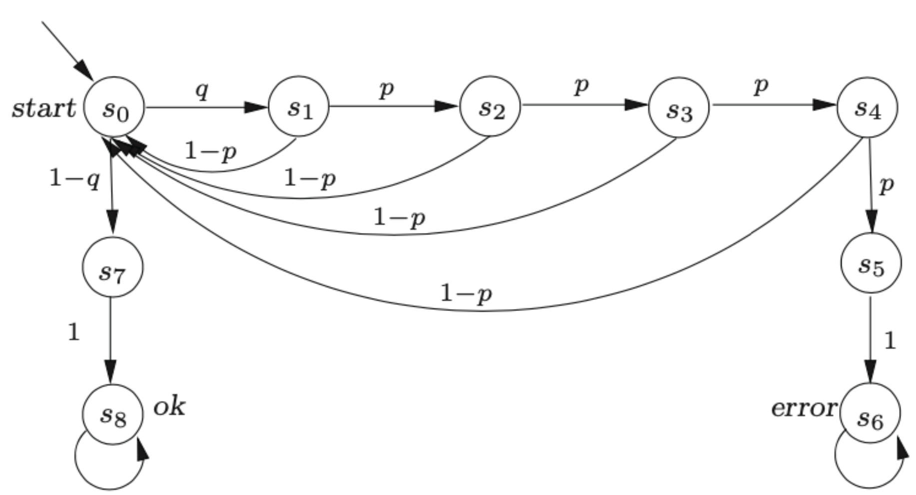
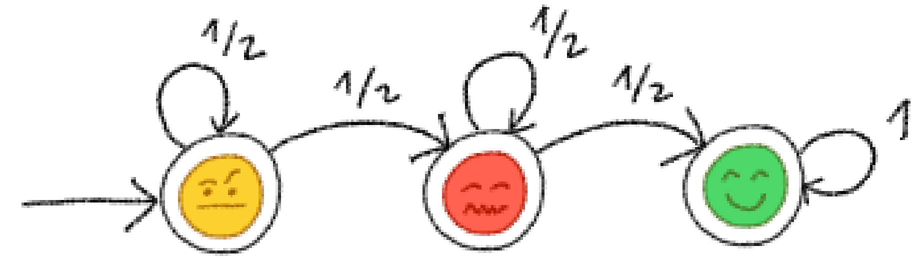


Figure 10.4: Markov chain of the IPv4 zeroconf protocol (for n=4 probes).

… and more in the slides.

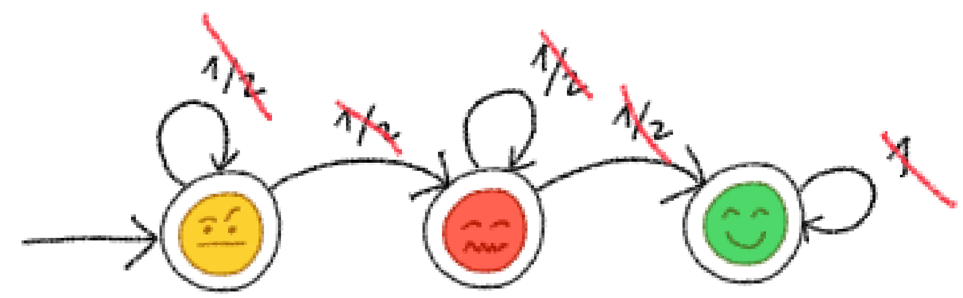
Discrete-Time Markov Chains

Given a DTMC



$$(S, P, \iota, AP, L)$$

We can define the underlying transition system



$$(S, A, \rightarrow, L, AP, I)$$

where…

$A = \{\tau\}$ *(some dummy action)*

$I = \{ s \mid \iota(s) > 0 \}$

$\rightarrow = \{ (s, \tau, s') \mid P(s, s') > 0 \}$

Discrete-Time Markov Chains

- Discrete-Time Markov Chains (DTMCs)
- Transient Distributions
- Steady State Distribution
- Reachability Probabilities
- Probabilities of Sets of Paths
- Exercises & Homework

Transient Distributions

Where is the Markov chain **after 1/2/3/…/n steps**?

Answer: in the transient distribution θ_n

Two equivalent definitions / ways to compute θ_n :

$$\theta_n = \iota \cdot P^n$$

Multiply the initial distribution vector by the transition probability matrix
P^n = make n-steps

Transient Distributions

Where is the Markov chain **after 1/2/3/…/n steps**?

Answer: in the transient distribution θ_n

Two equivalent definitions / ways to compute θ_n :

$$\theta_n = \iota \cdot P^n$$

$$\theta_0 = \iota$$

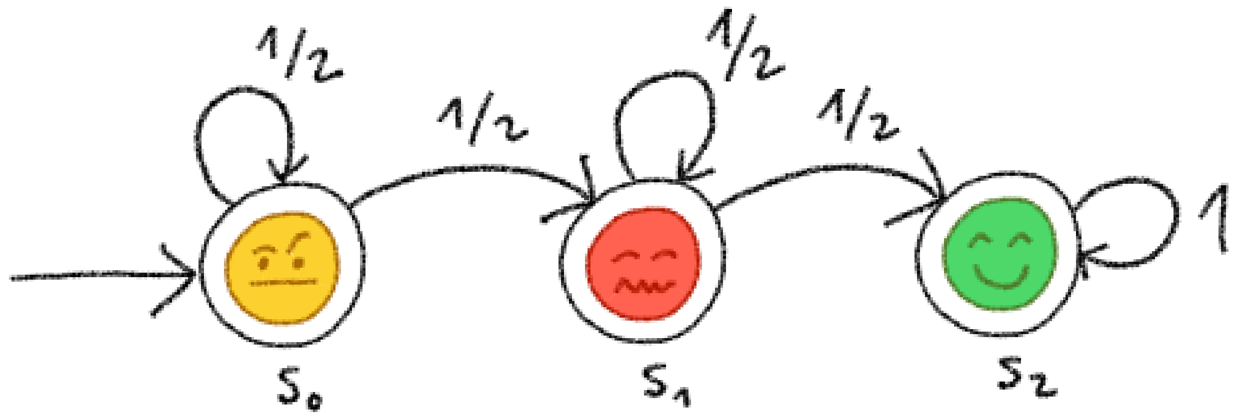
$$\theta_{n+1} = \theta_n \cdot P$$

Recursively:
- after 0-steps we're at the initial distribution;
- after (n+1)-steps we're at where we were after n-steps multiplied by the transition matrix

Transient Distributions

$\theta_0 = \iota$

$\theta_{n+1} = \theta_n \cdot P$



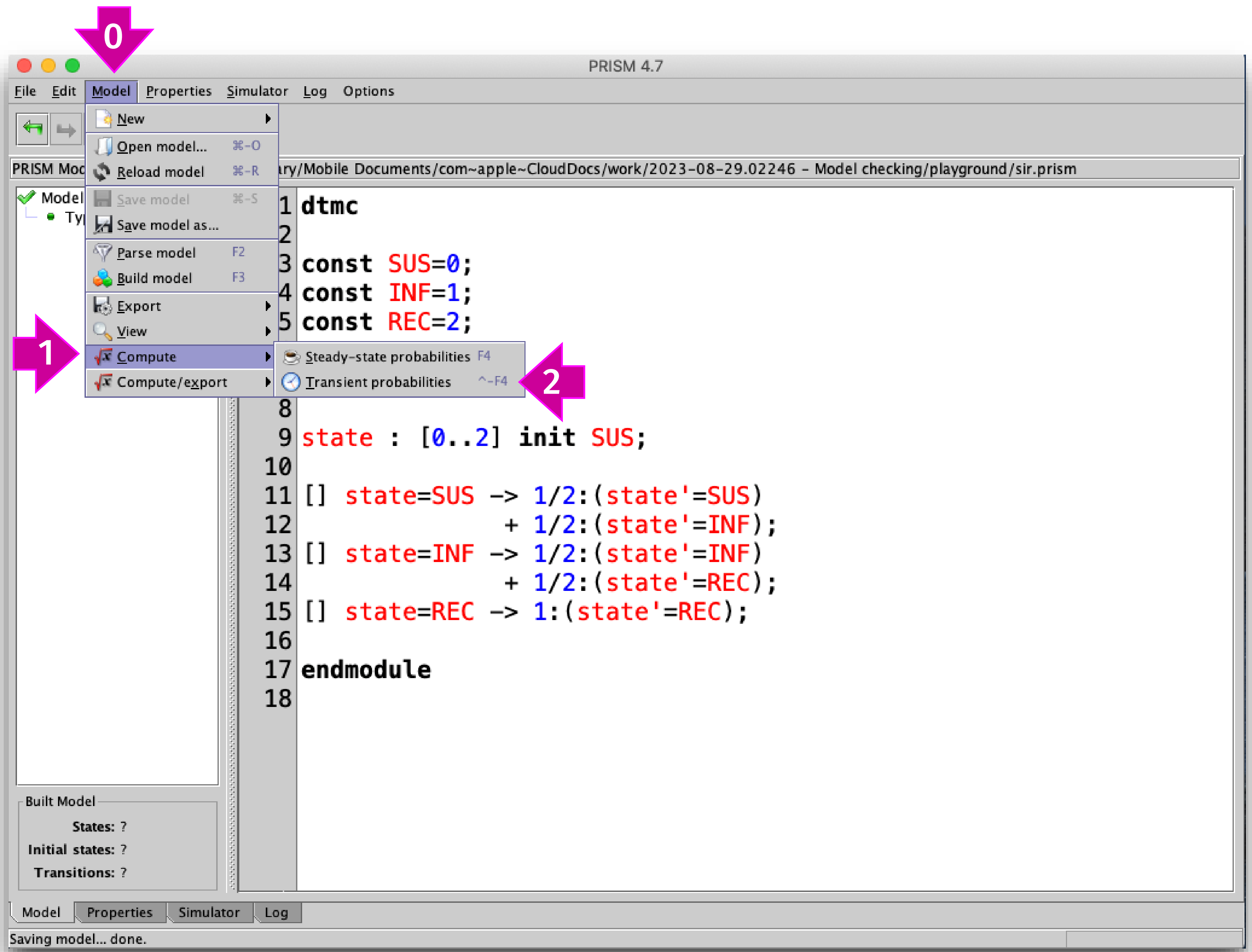
	s_0	s_1	s_2
θ_0	1	0	0
θ_1	1/2	1/2	0
θ_2	1/4	1/2	1/4
θ_3	1/8	3/8	1/2
	↓	↓	↓
...	0	0	1

$$= \underbrace{(1 \quad 0 \quad 0)}_{\theta_0} \times \underbrace{\begin{pmatrix} 1/2 & 1/2 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & 0 & 1 \end{pmatrix}}_{P}$$

This happens if we continue computing transient distributions

Using PRISM

PRISM supports transient distributions \o/



Using PRISM

www.prismmodelchecker.org/manual/PropertySpecification

www.prismmodelchecker.org/manual/PropertySpecification/ThePOperator

www.prismmodelchecker.org

Home • About • Downloads • Documentation • Manual • Publications • Case Studies • Support • Develope

PRISM Manual

Property Specification

- Introduction
- Identifying A Set Of States
- **The P Operator**
- The S Operator
- Reward-based Properties
- Multi-objective Properties
- Real-time Models
- Partially Observable Models
- Uncertain Models
- Non-probabilistic Properties
- Syntax And Semantics
- Filters
- Properties Files

Property Specification /

The P Operator

One of the most important operators in the PRISM property specification language is the ... used to reason about the probability of an event's occurrence. This operator was original... logic PCTL but also features in the other logics supported by PRISM, such as CSL. The... applicable to all types of models supported by PRISM.

Informally, the property:

```
P bound [ pathprop ]
```

bla bla bla …

Transient probabilities

We can also use the bounded `F` operator to refer to a single time instant, e.g.:

```
P=? [ F[10,10] y=6 ]
```

or, equivalently:

```
P=? [ F=10 y=6 ]
```

	s_0	s_1	s_2
θ_0	1	0	0
θ_1	1/2	1/2	0
θ_2	1/4	1/2	1/4

PRISM 4.9

File Edit Model Properties Strategie

Properties list: <Untitled>*

Properties

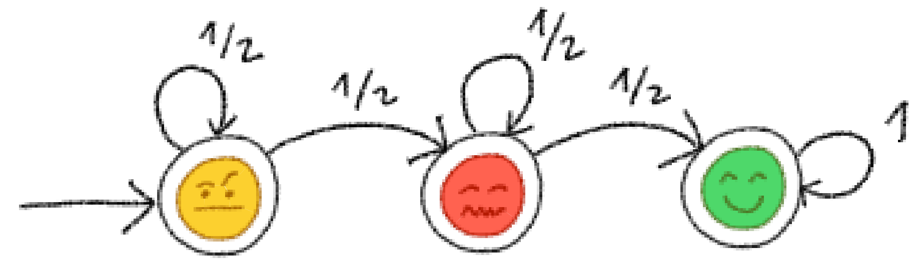
- P=? [F=1 (s=SUS)]
- P=? [F=1 (s=INF)]
- P=? [F=1 (s=REC)]
- P=? [F=2 (s=SUS)]
- P=? [F=2 (s=INF)]
- P=? [F=2 (s=REC)]

Discrete-Time Markov Chains

- Discrete-Time Markov Chains (DTMCs)
- Transient Distributions
- **Steady State Distribution**
- Reachability Probabilities
- Probabilities of Sets of Paths
- Exercises & Homework

Steady State

Where is the Markov chain in the long term?



Answer: in the limit of θ_n

Two ways to compute $\pi = limit_{n\to\infty}\theta_n$

(1) By iterative approximations → *compute lots of transient distributions*

(2) As the (unique) stationary distribution, i.e. a distribution that satisfies

$\pi = \pi \cdot P$ → *a “fixpoint” condition*

Steady State

Just the variables for which we need to find values

$$\lim_{n \to \infty} \theta_n = \left(\underset{\pi_1}{\underline{\qquad}} , \underset{\pi_2}{\underline{\qquad}} , \underset{\pi_3}{\underline{\qquad}} \right) ?$$

Calculate π by solving $\underline{\pi = \pi \cdot P}$ and $\underline{\pi_1 + \pi_2 + \pi_3 = 1}$

Steady State

$$\lim_{n \to \infty} \theta_n = (\underline{\quad}_{\pi_1}, \underline{\quad}_{\pi_2}, \underline{\quad}_{\pi_3})?$$

Calculate π by solving $\pi = \pi \cdot P$ and $\pi_1 + \pi_2 + \pi_3 = 1$

$$\pi_0 = \pi_0 \cdot 1/2$$

this is not matrix-vector multiplication, **we're using intuition**

π_i is the probability of getting into state s_i

Steady State

$$\lim_{n \to \infty} \theta_n = (0,\ 0,\ 1)\ ?$$

Calculate π by solving $\pi = \pi \cdot P$ and $\cancel{\pi_1 + \pi_2} + \pi_3 = 1$

$$\pi_0 = \pi_0 \cdot 1/2 \rightarrow \pi_0 = 0$$

$$\pi_1 = \cancel{\pi_0 \cdot 1/2} + \pi_1 \cdot 1/2 \rightarrow \pi_1 = 0$$

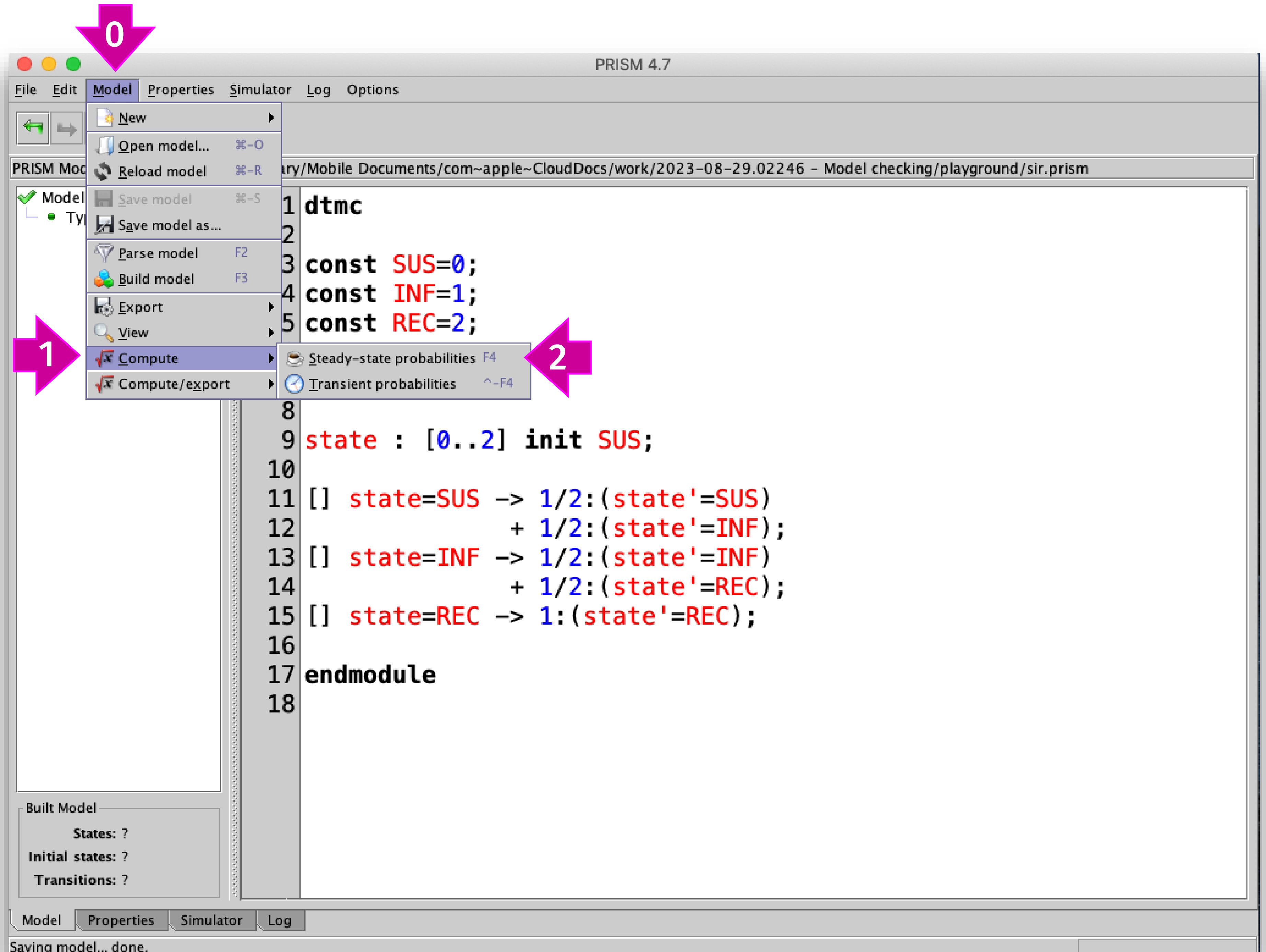
$$\pi_2 = \pi_2 \cdot 1 + \cancel{\pi_1 \cdot 1/2}$$

$$\pi_0 + \pi_1 + \pi_2 = 1$$

$$\pi_3 = 1$$

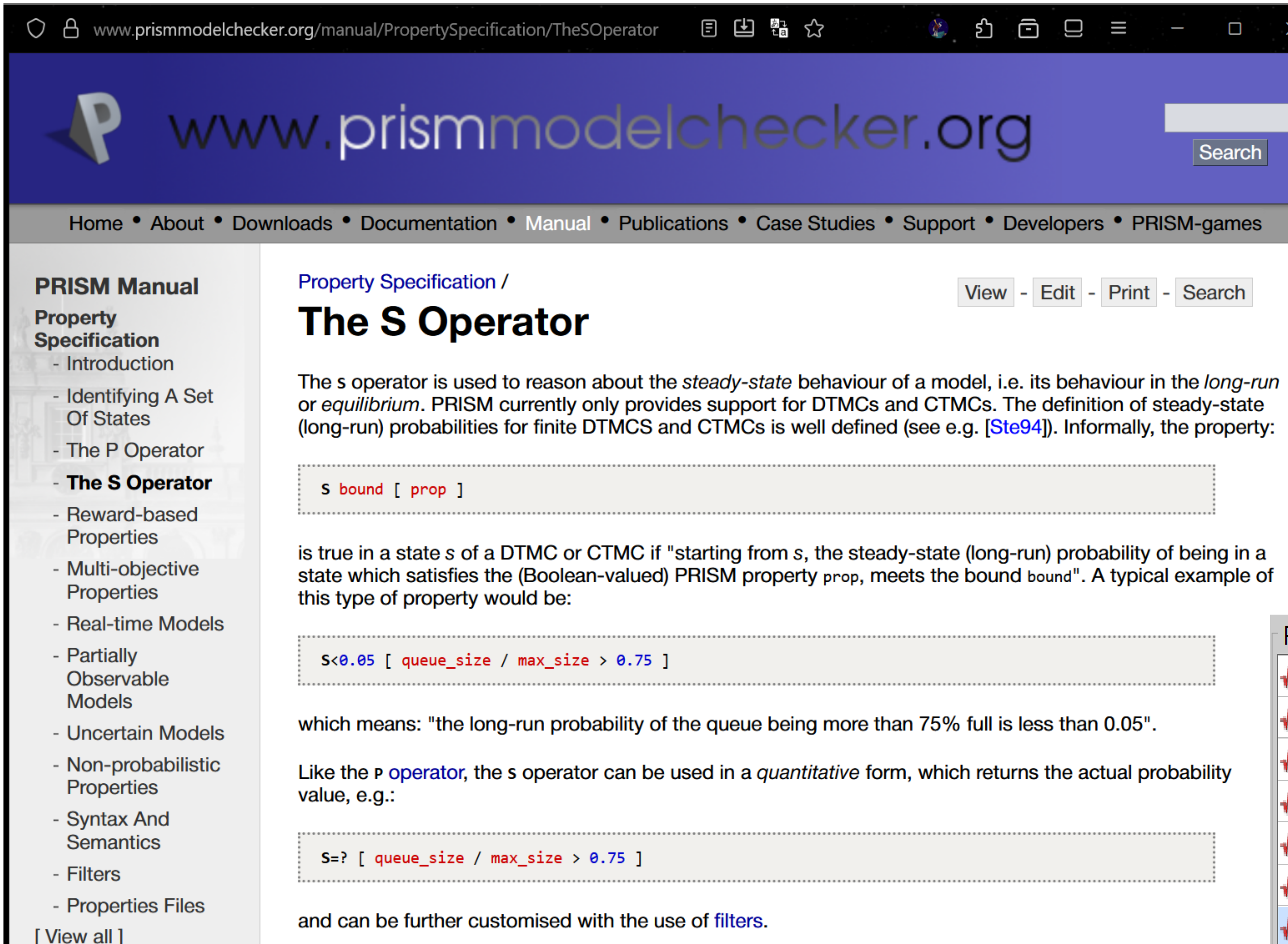
Using PRISM

PRISM supports **transient distributions**, *and also* steady state distributions!   \o/



Using PRISM

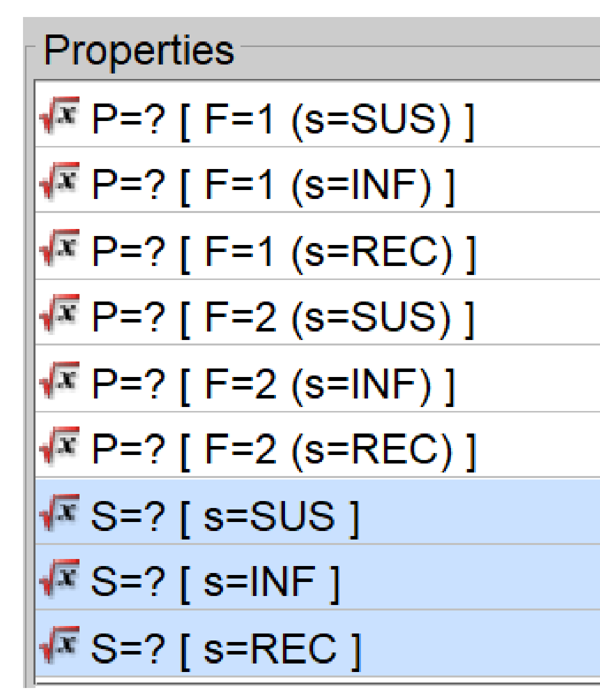
www.prismmodelchecker.org/manual/PropertySpecification



$\rightarrow \pi_0 = 0$

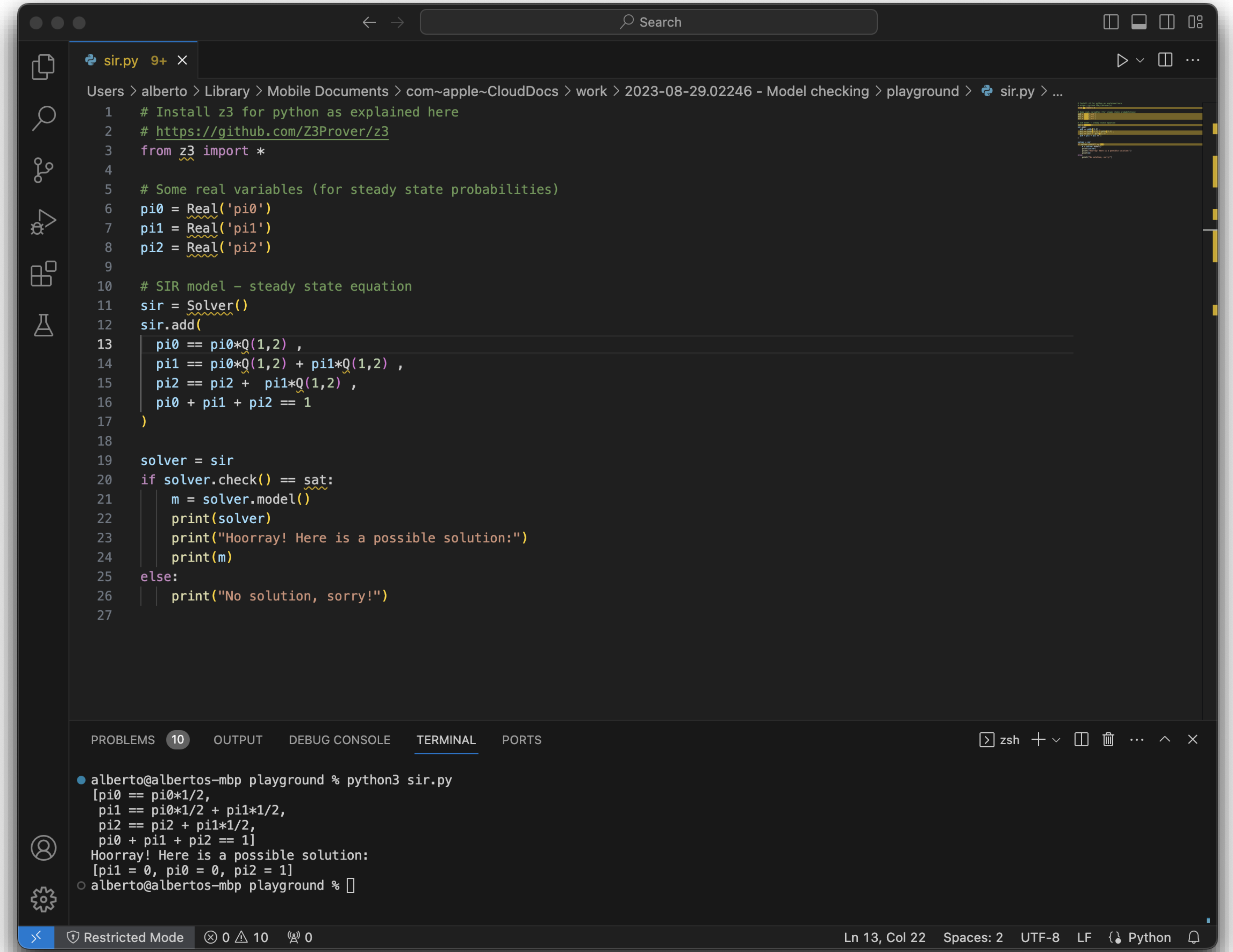
$\rightarrow \pi_1 = 0$

$\rightarrow \pi_2 = 1$



Using PRISM and Z3

We can also use the SMT solver Z3 to do some of these calculations



Steady State

It is **not always** the case that

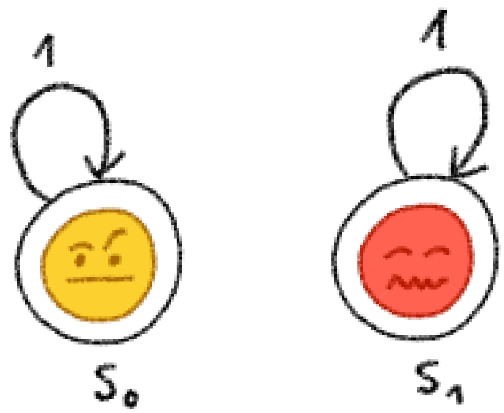
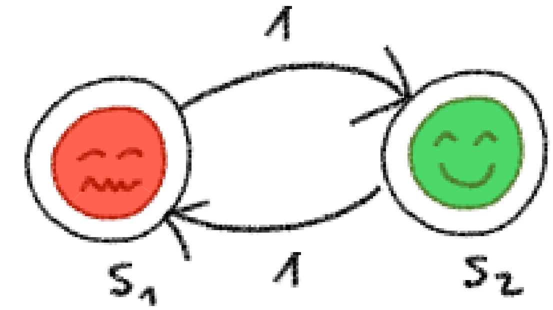
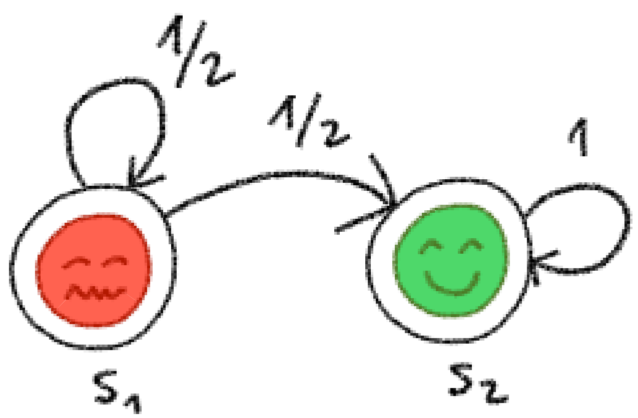
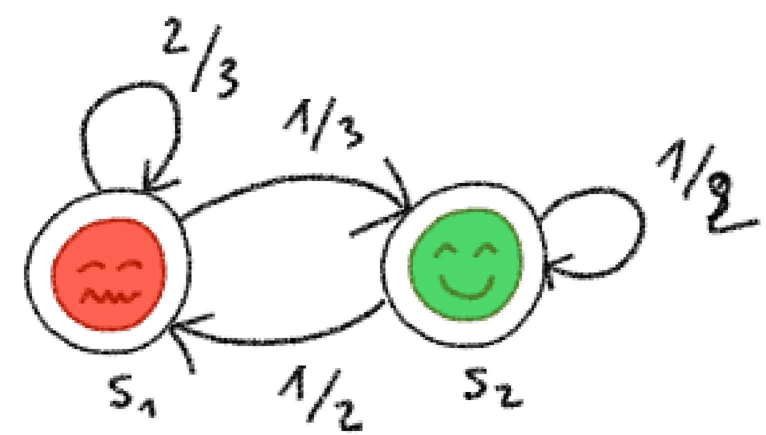
$$\pi = lim_{n \to \infty} \theta_n$$

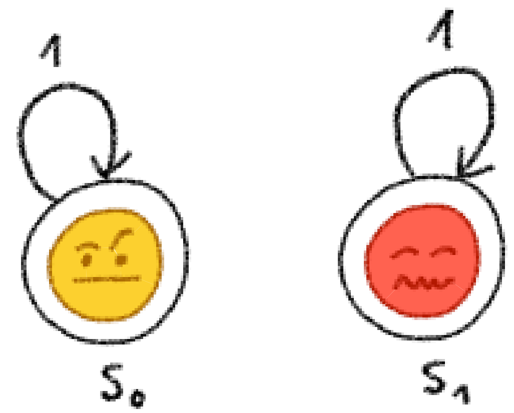
is well defined and can be computed as the (unique) stationary distribution:

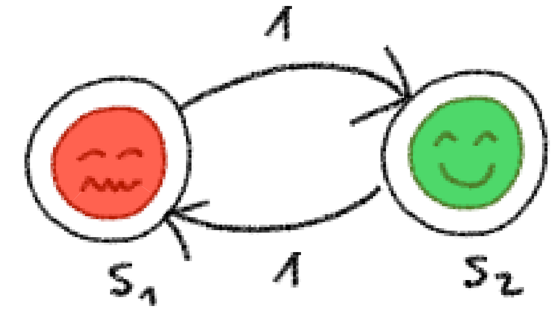
$$\pi = \pi \cdot P$$

There are **cases** where :

- the limit is simply not well-defined;
- the limit depends on the initial distribution;
- the stationary distribution is not unique (the equation has more than 1 solution).


1
1
s0
s1

1
1
s1
s2

1/2
1/2
1
s1
s2

2/3
1/3
1/2
1/2
s1
s2



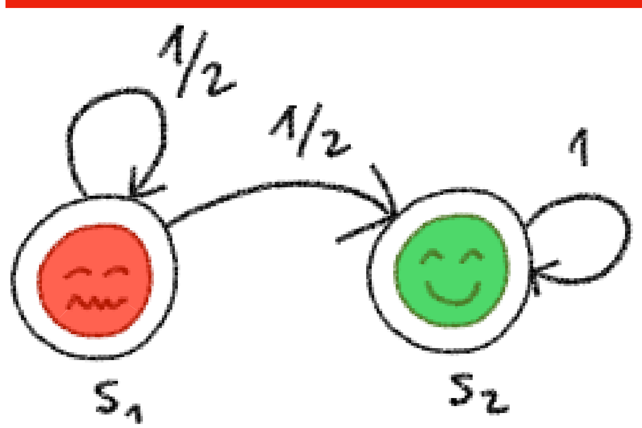


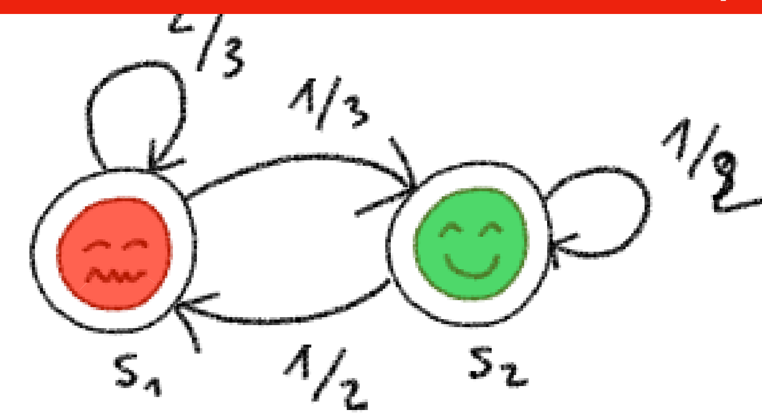
$$\pi_0 = \pi_0$$

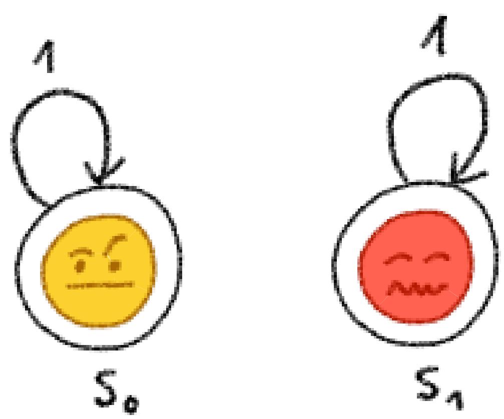
$$\pi_1 = \pi_1$$

$$\pi_0 + \pi_1 = 1$$

Infinitely many solutions! → cannot apply to DTMCs with disconnected components

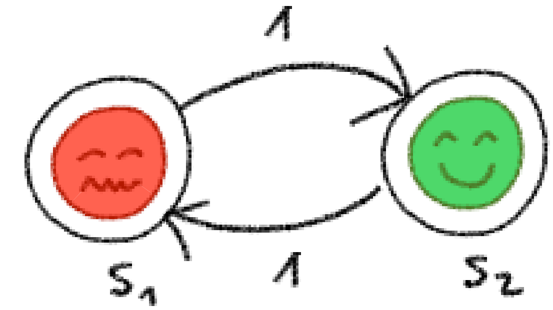




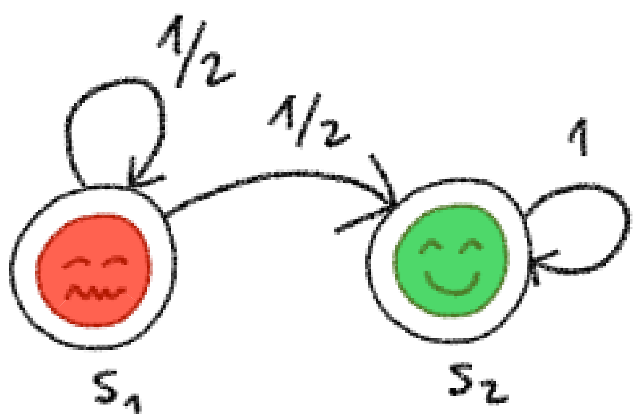


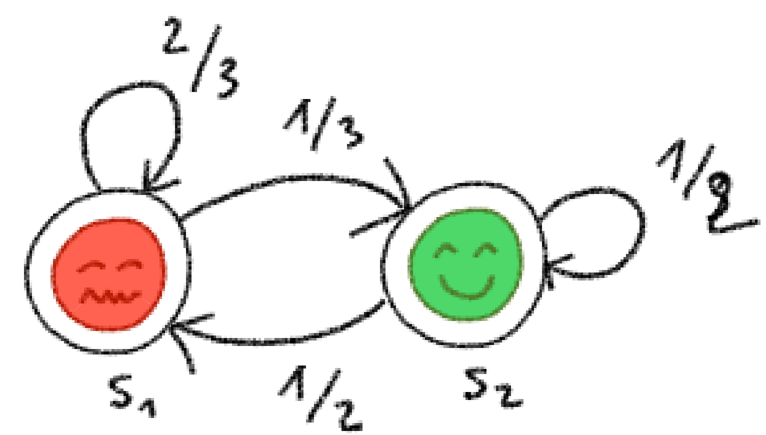
$$\pi_0 = \pi_0$$
$$\pi_1 = \pi_1$$
$$\pi_0 + \pi_1 = 1$$

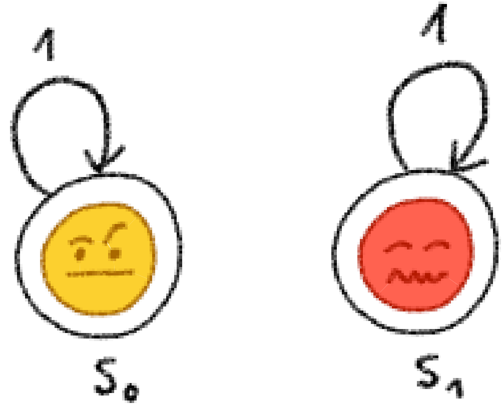
Not converging to any stable distribution → oscillating



$$\pi_0 = \pi_1$$
$$\pi_1 = \pi_0$$
$$\pi_0 + \pi_1 = 1$$



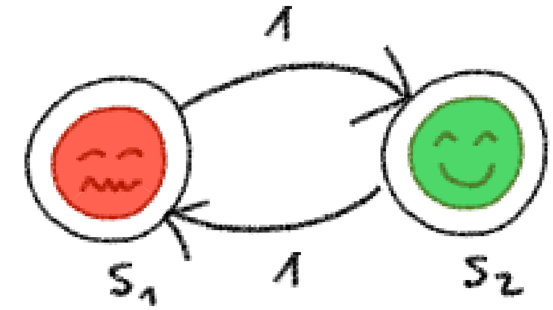




$\pi_0 = \pi_0$

$\pi_1 = \pi_1$

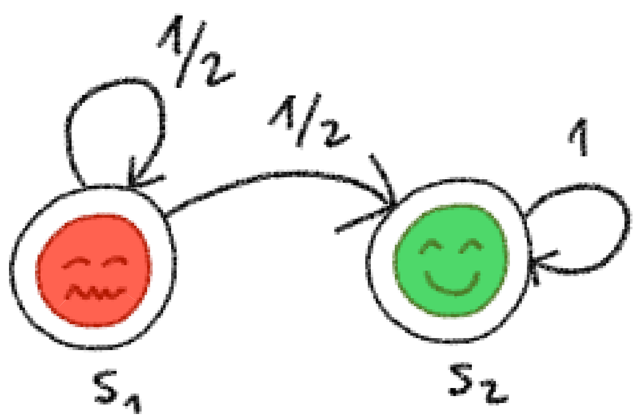
$\pi_0 + \pi_1 = 1$



$\pi_0 = \pi_1$

$\pi_1 = \pi_0$

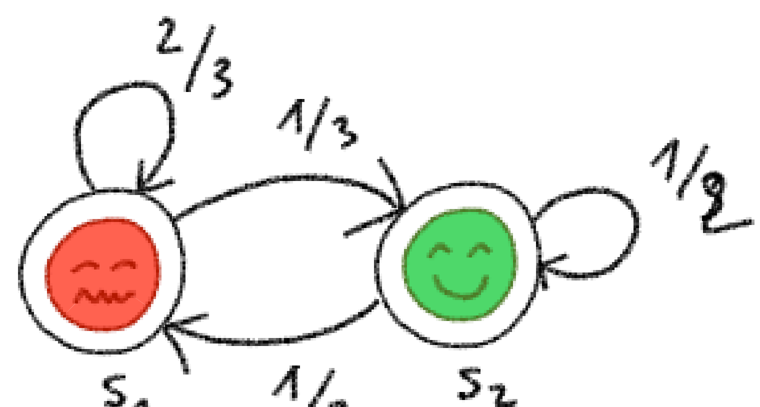
$\pi_0 + \pi_1 = 1$

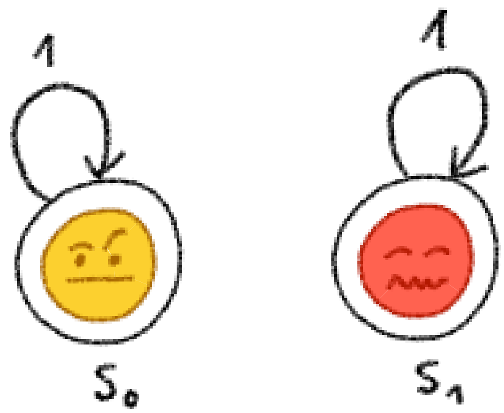


$\pi_1 = 1/2\,\pi_1 = 0$

$\pi_2 = 1/2\,\pi_1 + \pi_2 = 1$

$\pi_1 + \pi_2 = 1$

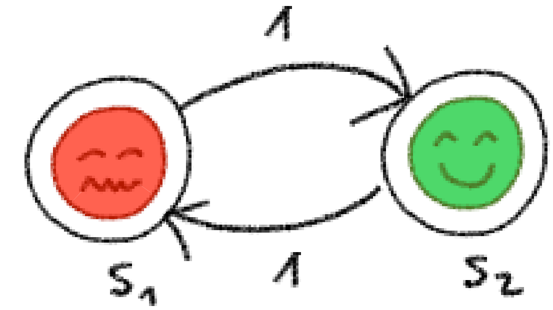




$\pi_0 = \pi_0$

$\pi_1 = \pi_1$

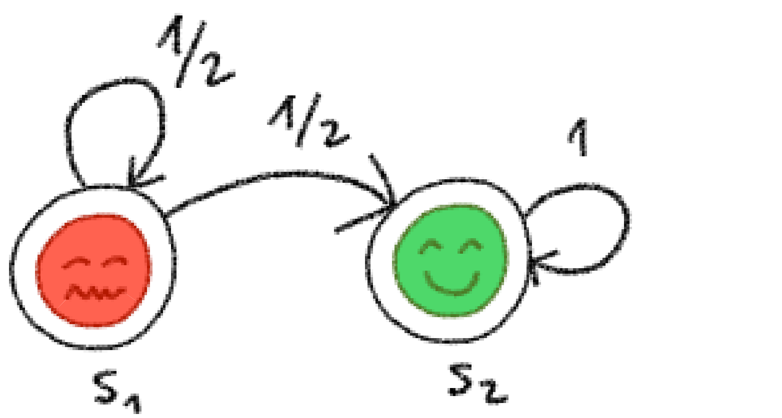
$\pi_0 + \pi_1 = 1$



$\pi_0 = \pi_1$

$\pi_1 = \pi_0$

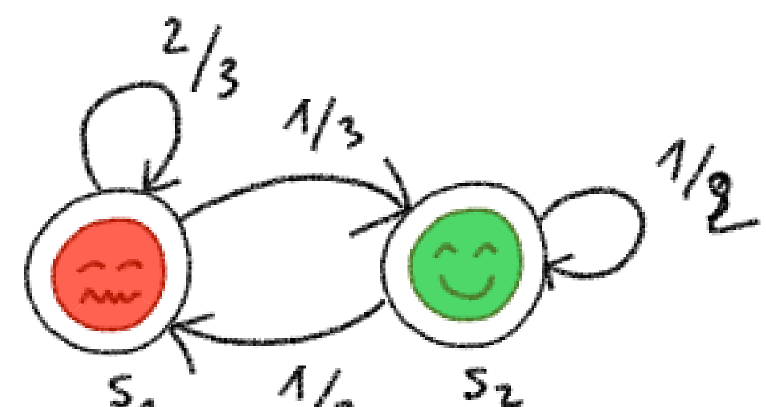
$\pi_0 + \pi_1 = 1$



$\pi_1 = 1/2\,\pi_1 = 0$

$\pi_2 = 1/2\,\pi_1 + \pi_2 = 1$

$\pi_1 + \pi_2 = 1$



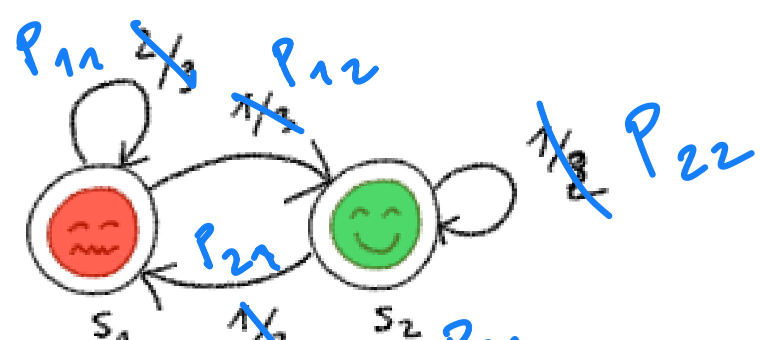
$\pi_1 = 2/3\,\pi_1 + 1/2\,\pi_2$

$\pi_2 = 1/2\,\pi_2 + 1/3\,\pi_1$

$\pi_1 + \pi_2 = 1$

Example of application of SMT

How should probabilities $p_{11}, p_{12}, p_{21}, p_{22}$ be if, ***in the long term***, we want to be in state s_2 (recovered) 99% of the time?

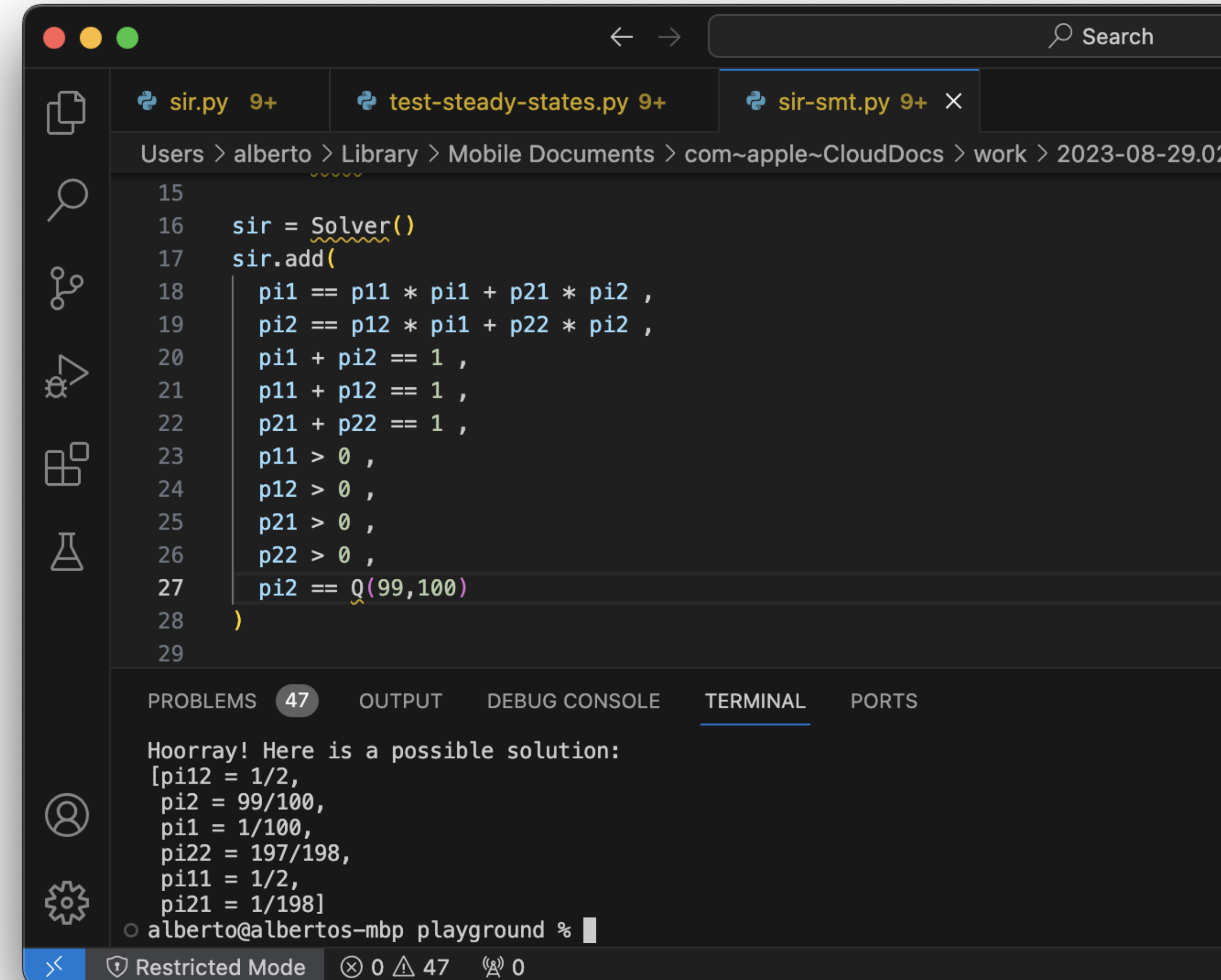


$\pi_1 = \overset{p_{11}}{\cancel{1/3}}\, \pi_1 + \overset{p_{21}}{\cancel{1/2}}\, \pi_2$

$\pi_2 = \underset{p_{21}}{\cancel{1/2}}\, \pi_2 + \underset{p_{12}}{\cancel{1/3}}\, \pi_1$

$\pi_1 + \pi_2 = 1$

$\pi_2 = 99/100$



Easy to pose as an SMT query (e.g. in Z3)

Steady State

For the limit

$$\pi = limit_{n \to \infty} \theta_n$$

to be computed as the (unique) stationary distribution

$$\pi = \pi \cdot P$$

of the DTMC T, there exist **sufficient conditions**:

(1) T must be aperiodic*

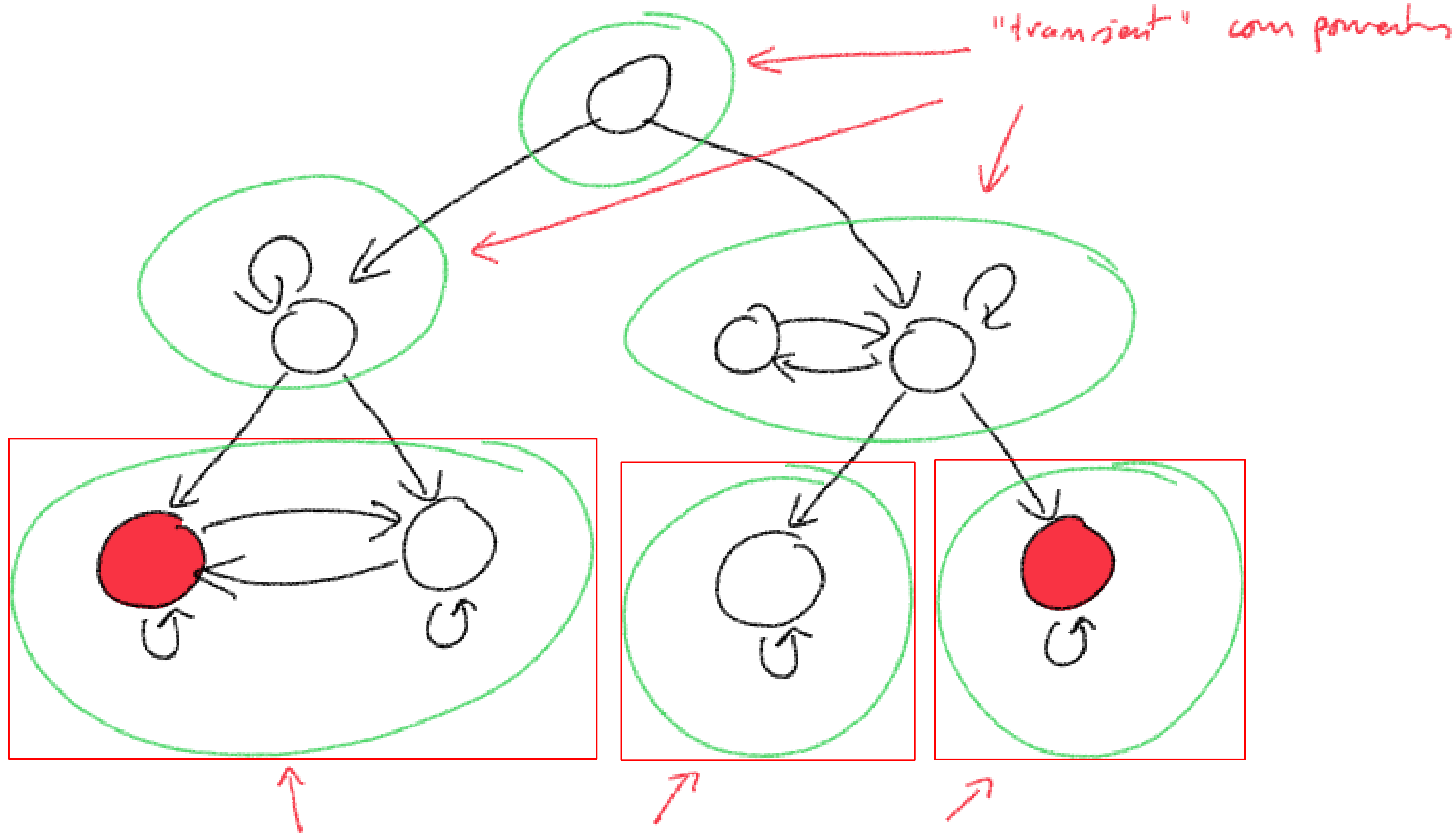
(2) T must be strongly connected.

If (1) and (2) do not hold: pay attention to the computation of steady states, because *it may not mean what you have in mind*.

If (1) and (2) hold, we can compute the limit precisely and independently of the initial distribution.

(*) T is *aperiodic* if the GCD of all cycle lengths is 1—check stats.stackexchange.com/a/48861

Where does the probability mass go?



Bottom Strongly Connected Components are SCCs without outgoing edges

In the long-term, the probability mass resides in the BSCCs.

The initial distribution determines how much goes to each BSCC.

Sometimes the entire DTMC forms one BSCC—it is then called ***ergodic*** or ***irreducible***.

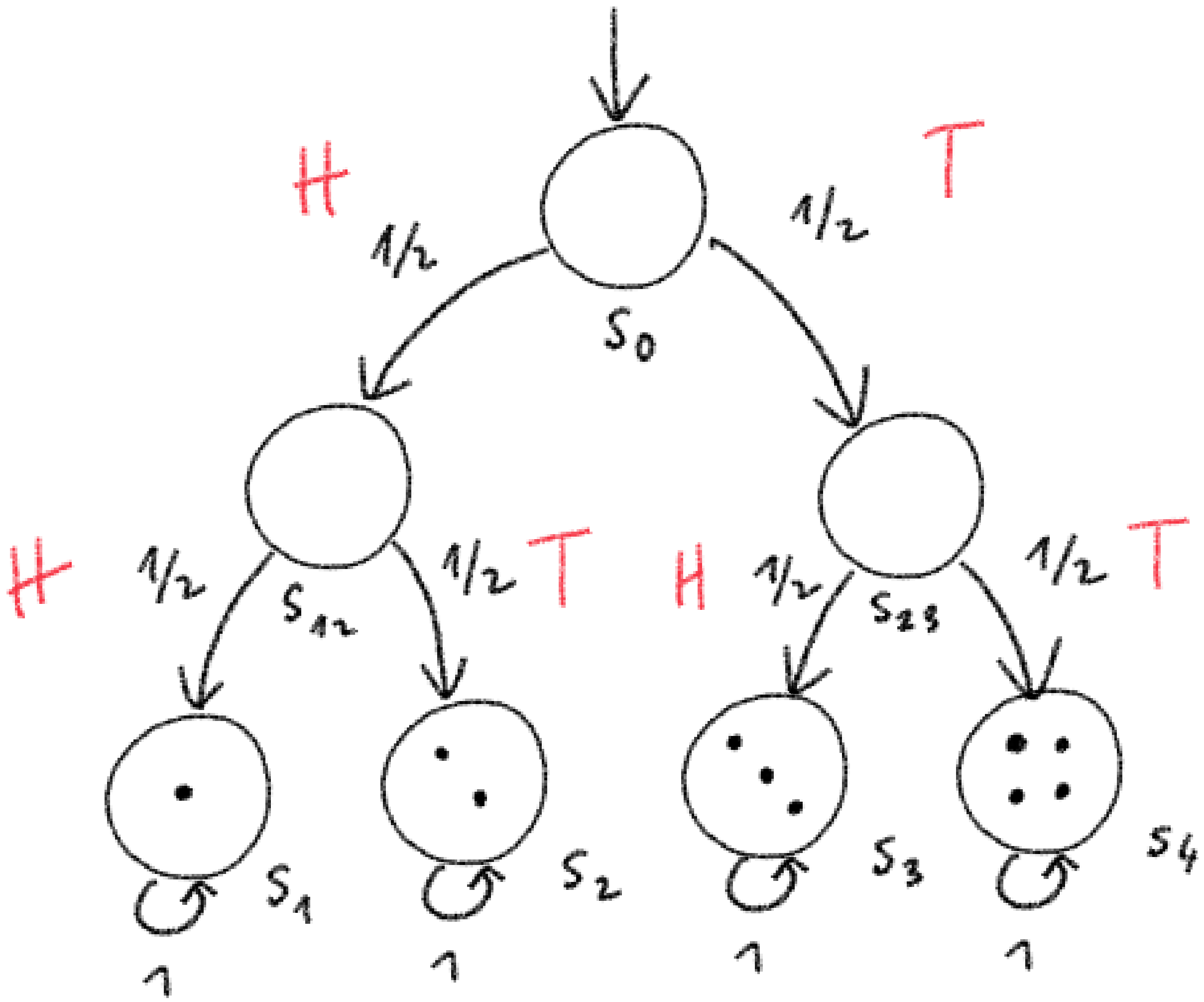
Discrete-Time Markov Chains

- Discrete-Time Markov Chains (DTMCs)
- Transient Distributions
- Steady State Distribution
- Reachability Probabilities
- Probabilities of Sets of Paths
- Exercises & Homework

Simulating a 4-faced dice with a coin

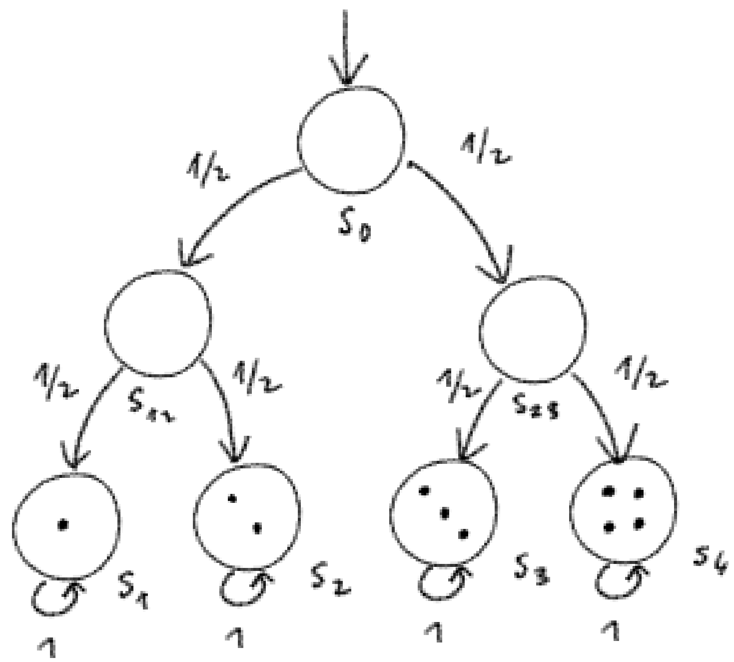
Let’s see how to use DTMCs to measure probability of eventually reaching some states

Simulating a 4-faced dice with a coin

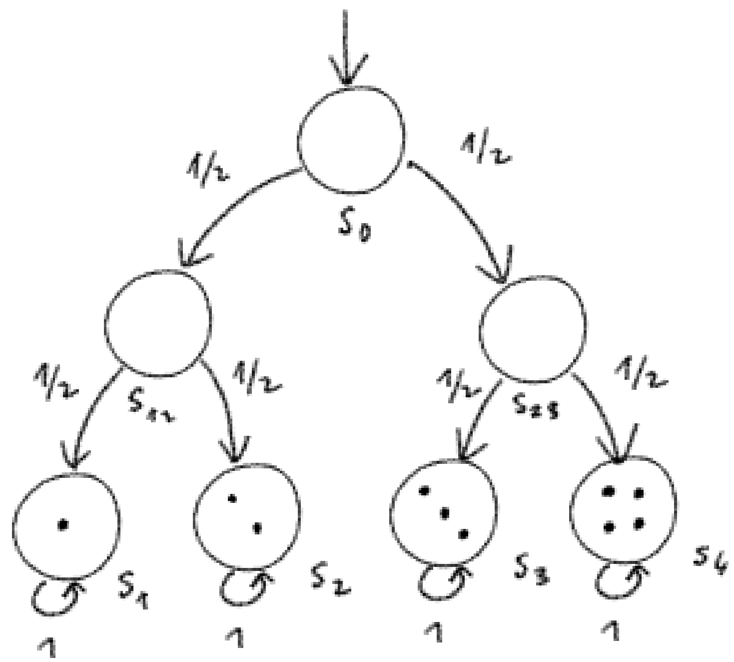


Are we sure the odds of each outcome are equal?

How can we compute the probability of outcome X?

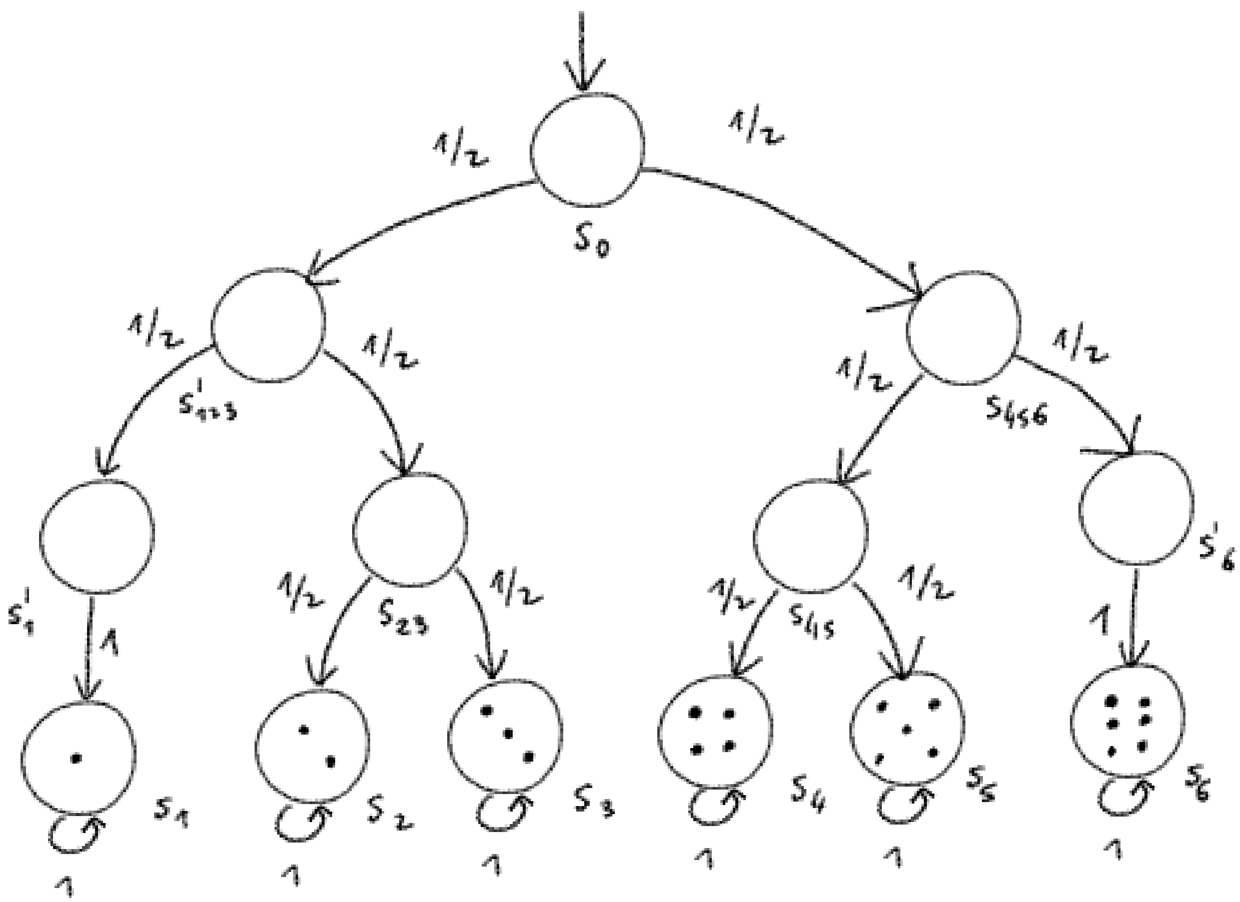


$$Pr(\lozenge \bullet) = \;??$$



$$P_r(\Diamond \,\cdot) = P_r(\{ s_0 \overset{1/2}{\curvearrowright} s_{12} \overset{1/2}{\curvearrowright} s_1^{\omega} \}) = 1/2 \cdot 1/2 = 1/4$$

Simulating a 6-faced dice with a coin



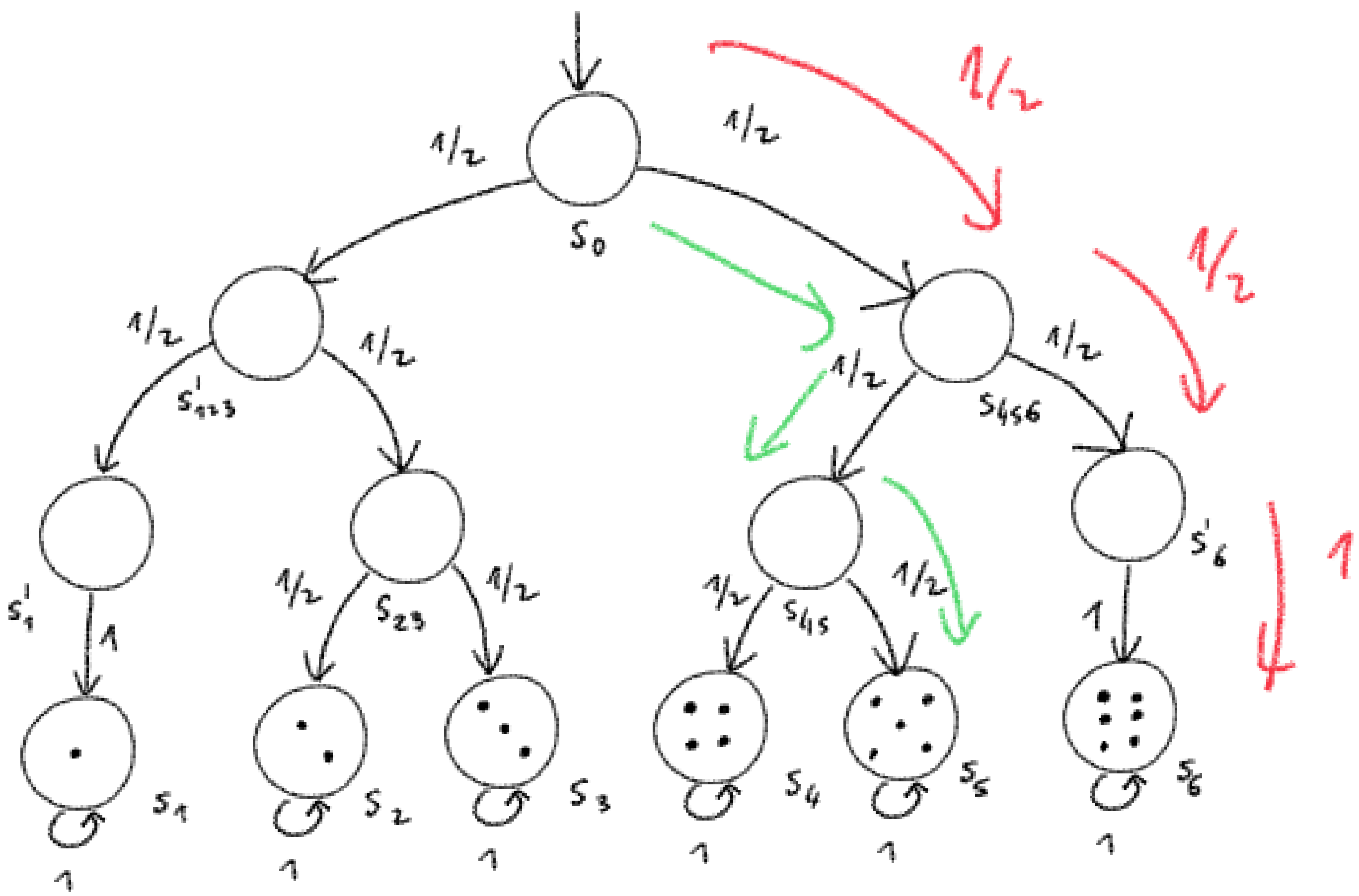
I get to choose 3 numbers, and you take the rest

If the outcome is one of my numbers, I win.
If the outcome is one of your numbers, you win.

Shall we play?

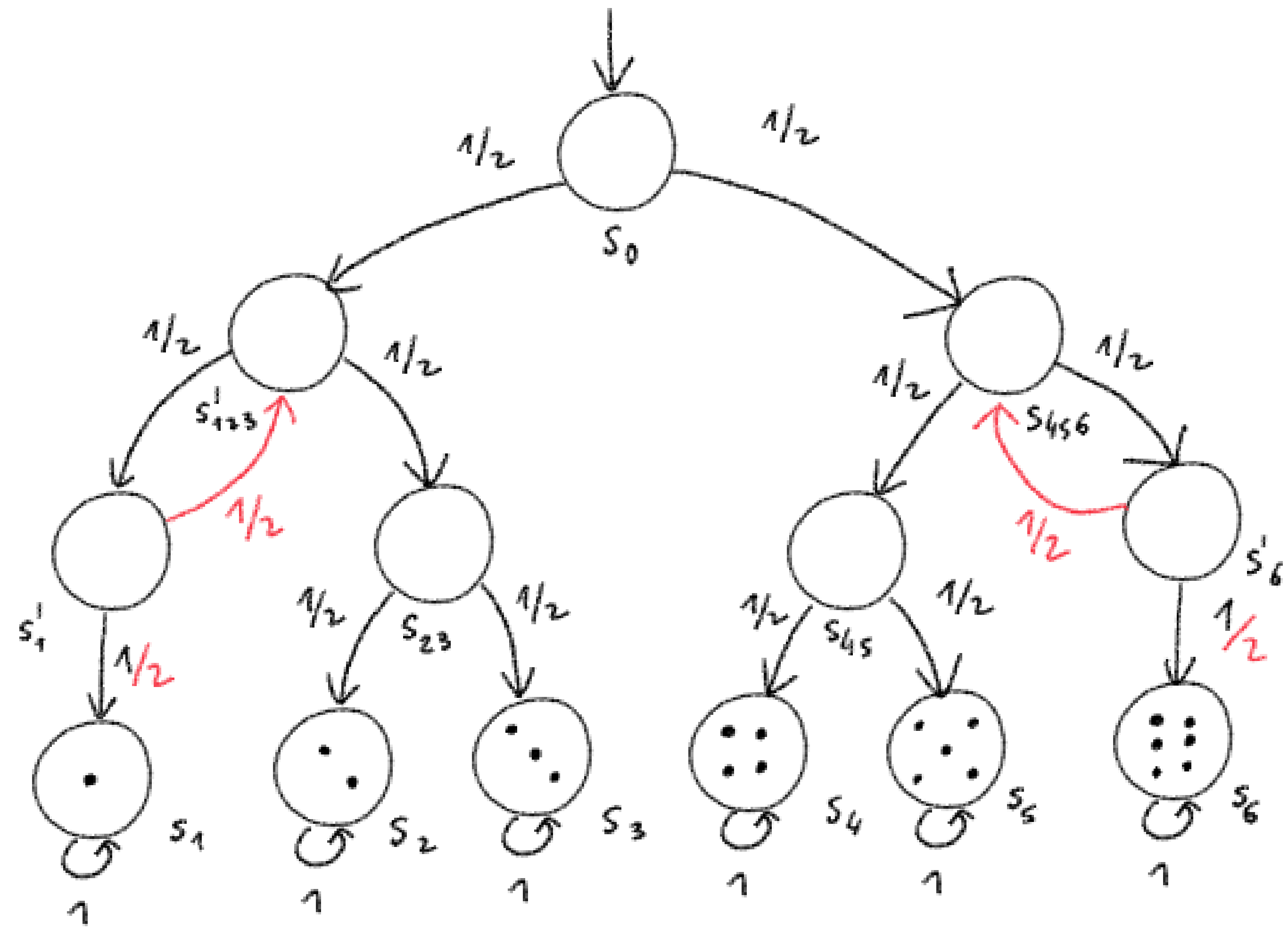
Guess probabilities for 5 and 6

Simulating a 6-faced dice with a coin

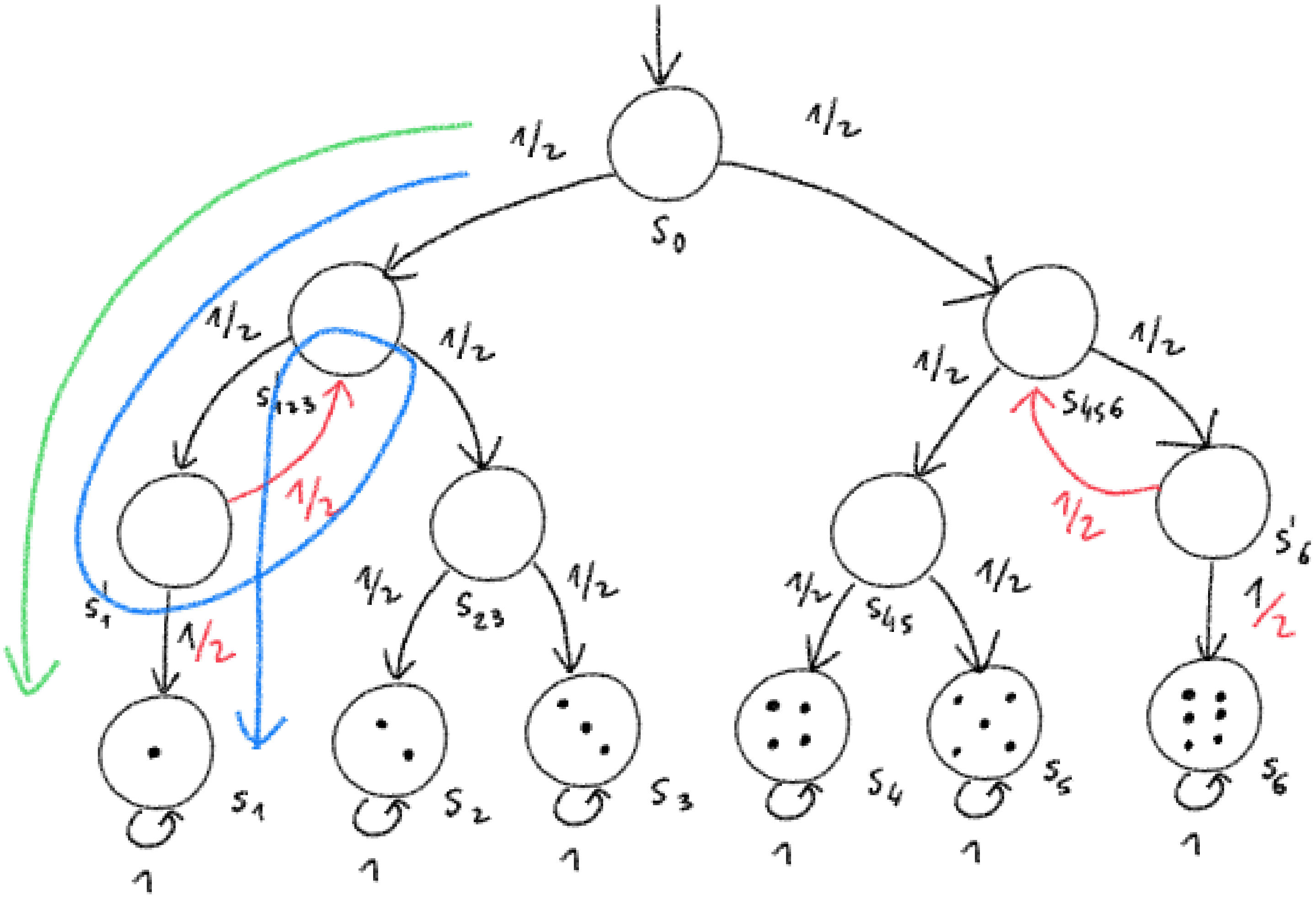


$$\tfrac{1}{2} \cdot \tfrac{1}{2} \cdot 1 = \tfrac{1}{4}$$

$$\tfrac{1}{2} \cdot \tfrac{1}{2} \cdot \tfrac{1}{2} = \tfrac{1}{8}$$



Let's make the game fair(?) again. Shall we play now?



$$S_0\, S_{123}\, S_1'\, S_1 \to \left(1/2\right)^3$$

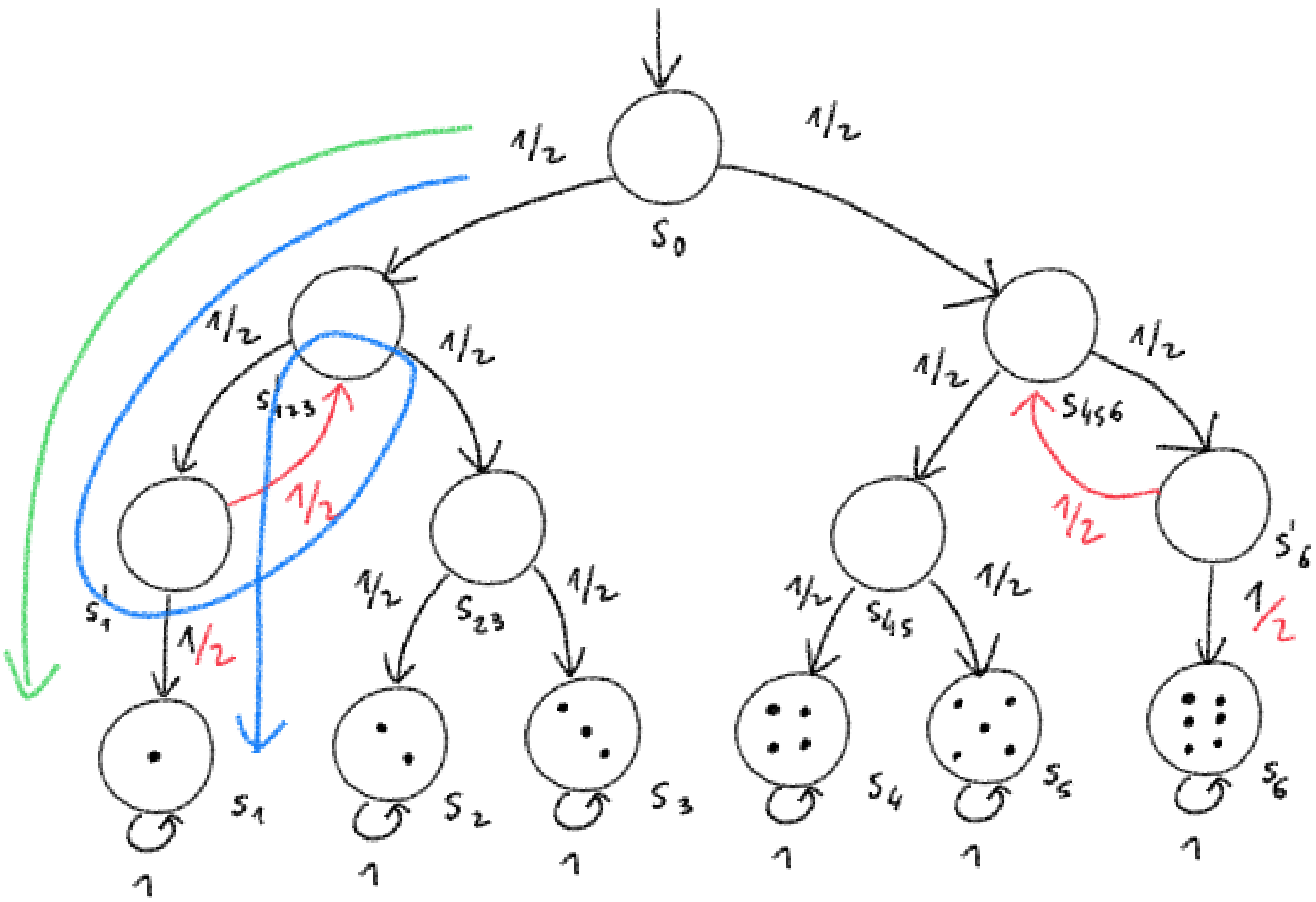
$+$

$$S_0\, S_{123}\, S_1'\, S_{123}\, S_1'\, S_1 \to \left(1/2\right)^5$$

$$S_0 \;\dots\dots \to \left(1/2\right)^7$$

$\downarrow$

$$\sum_{i=1}^{\infty} \left(1/2\right)^{2i+1}$$



$s_0\, s_{123}\, s_1'\, s_1 \to (1/2)^3$

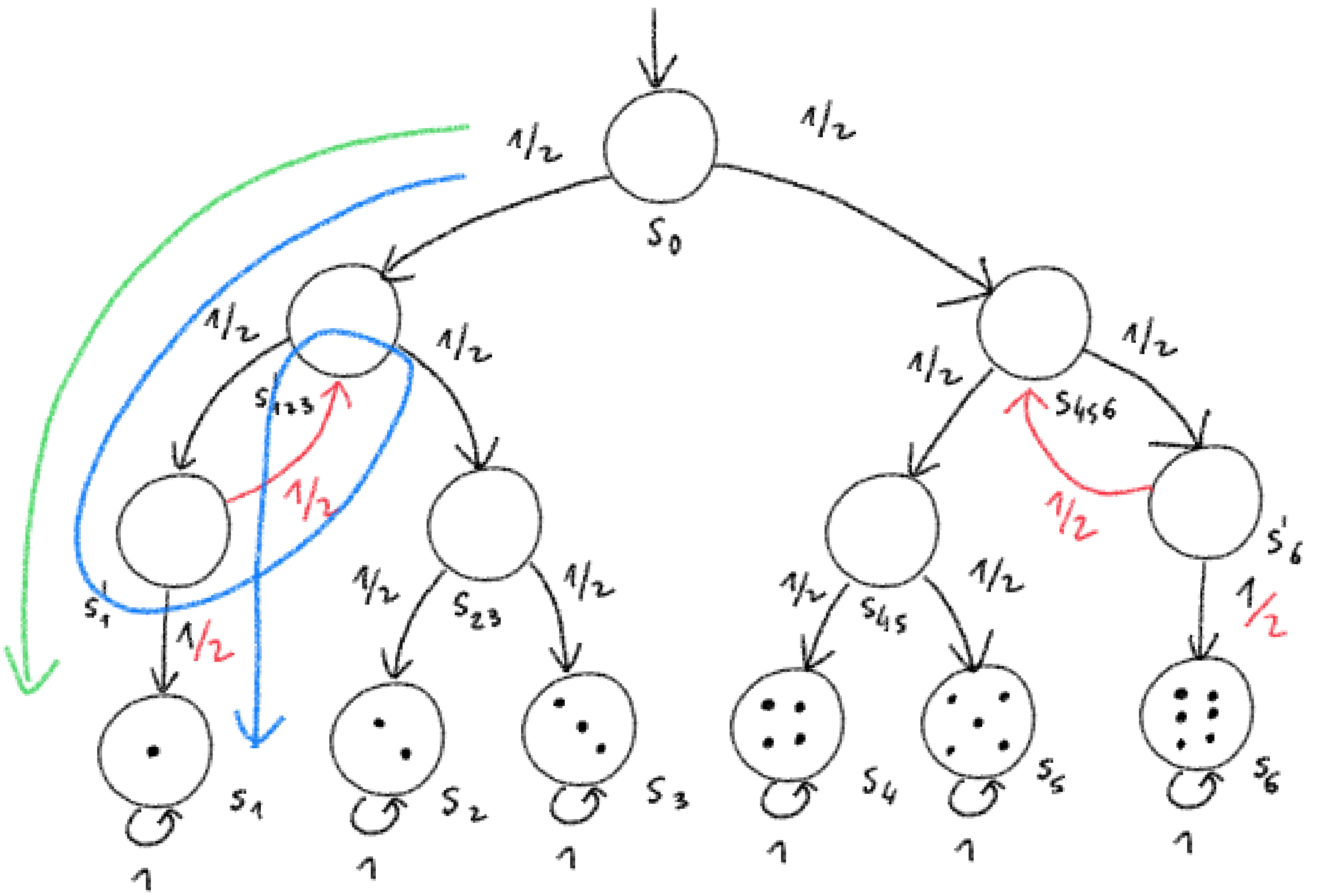
$+$

$s_0\, s_{123}\, s_1'\, s_{123}\, s_1'\, s_1 \to (1/2)^5$

$s_0 \, \ldots\ldots \to (1/2)^7$

$$\sum_{i=1}^{\infty} (1/2)^{2i+1}$$

Let’s compute the probability of (potentially) infinitely long traces!



$S_0\ S_{123}\ S_1'\ S_1 \rightarrow (1/2)^3$

$+$

$S_0\ S_{123}\ S_1'\ S_{123}\ S_1'\ S_1 \rightarrow (1/2)^5$

$S_0 \ldots\ldots \rightarrow (1/2)^7$

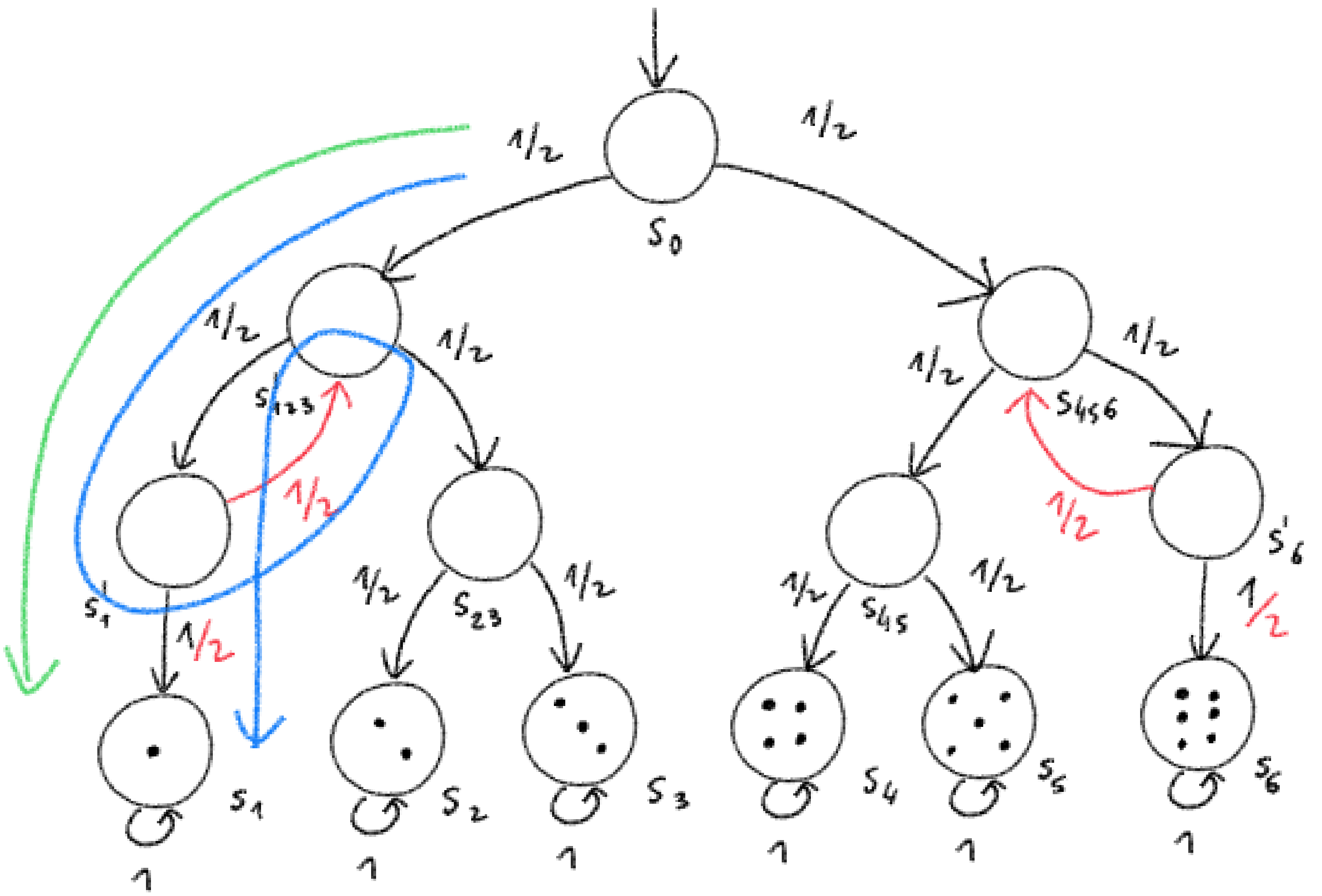
$\downarrow$

$$\sum_{i=1}^{\infty} (1/2)^{2i+1}$$

$$Pr\left(\bigcup_{n=0}^{\infty} \left(\{S_0\, S_{123}\, S_1'\, (S_{123}\, S_1')^n\, S_1^{\omega}\}\right)\right)$$

$$\sum_{n=0}^{\infty} Pr\left(\{S_0 \xrightarrow{1/2} S_{123} \xrightarrow{1/2} S_1'\, (S_{123}\, S_1')^n\, S_1^{\omega}\}\right)$$

$$\sum_{n=0}^{\infty} 1/2 \cdot 1/2 \cdot (1/2 \cdot 1/2)^n \cdot 1/2 = 1/8 \cdot \sum_{n=0}^{\infty} (1/4)^n$$



$S_0\, S_{123}\, S_1'\, S_1 \to (1/2)^3$

$+$

$S_0\, S_{123}\, S_1'\, S_{123}\, S_1'\, S_1 \to (1/2)^5$

$S_0 \ldots\ldots \to (1/2)^7$

$$\downarrow$$

$$\sum_{i=1}^{\infty} (1/2)^{2i+1}$$

$$Pr\left(\bigcup_{n=0}^{\infty} \left(\{S_0\, S_{123}\, S_1'\, (S_{123}\, S_1')^n\, S_1^{\omega}\}\right)\right)$$

$$\sum_{n=0}^{\infty} Pr\left(\{S_0 \xrightarrow{1/2} S_{123} \xrightarrow{1/2} S_1'\, (S_{123}\, S_1')^n\, S_1^{\omega}\}\right)$$

$$\sum_{n=0}^{\infty} 1/2 \cdot 1/2 \cdot (1/2 \cdot 1/2)^n \cdot 1/2 = 1/8 \sum_{n=0}^{\infty} (1/4)^n = 1/8 \cdot \frac{1}{1-\frac{1}{4}}$$

$$= 1/8 \cdot 4/3 = \frac{4}{24} = 1/6$$

https://en.wikipedia.org/wiki/Geometric_series#Convergence_of_the_series_and_its_proof

Discrete-Time Markov Chains

- Discrete-Time Markov Chains (DTMCs)
- Transient Distributions
- Steady State Distribution
- Reachability Probabilities
- Probabilities of Sets of Paths
- Exercises & Homework

Probability measures

Let $\mathcal{S}$ be a non-empty set of "outcomes" and $\mathcal{E}$ be a set of "events" such that

- $\mathcal{E} \subseteq 2^{\mathcal{S}}$
- $\emptyset \in \mathcal{E}$
- $\mathcal{E}$ is closed under countable union and complement

A function $\mu : \mathcal{E} \to [0,1]$ is a probability measure if it satisfies the following conditions

- $\mu(\bigcup_{i\geq 0} C_i) = \sum_{i\geq 0} \mu(C_i)$ for *pairwise disjoint* sets $C_0, C_1, \ldots$
- $\mu(\mathcal{S} \setminus C) = 1 - \mu(C)$
- $\mu(\emptyset) = 0$

$$\mu(\mathcal{S}) = \mu(\mathcal{S} \setminus \emptyset) = 1 - 0 = 1$$

Probability measures

Simple example of throwing a coin:

- $\mathcal{S}$ = {T,H}
- $\mathcal{E}$ = { Ø , {T}, {H} , {T,H} }

We are free to choose a probability measure $\mu : \mathcal{E} \rightarrow [0,1]$ as long as…

- μ(Ø) = 0
- μ({T,H}) = $\mu(\mathcal{S})$ = 1
- μ({T}) = $\mu(\mathcal{S}\backslash$ {H}) = 1 - μ({H})

… and some other (redundant) conditions …

Probability measure for sets of paths

We will use a measure where:

$\mathcal{S}$ → set containing all single paths from $\mathcal{M}$,

$\mathcal{E} \subseteq 2^{\mathcal{S}}$ → sets of paths from $\mathcal{M}$.

Probability measure based on "cylinder sets"

Probability measure for sets of paths

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**:

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

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

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

probabilities of moving from one state to the next

Probability measure for sets of paths

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**:

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

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

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

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)

Cylinder set probability measure at work

The reachability probabilities we have seen before (e.g. in the dice examples) are all based on cylinder sets. *That's why our calculations were well-founded*.

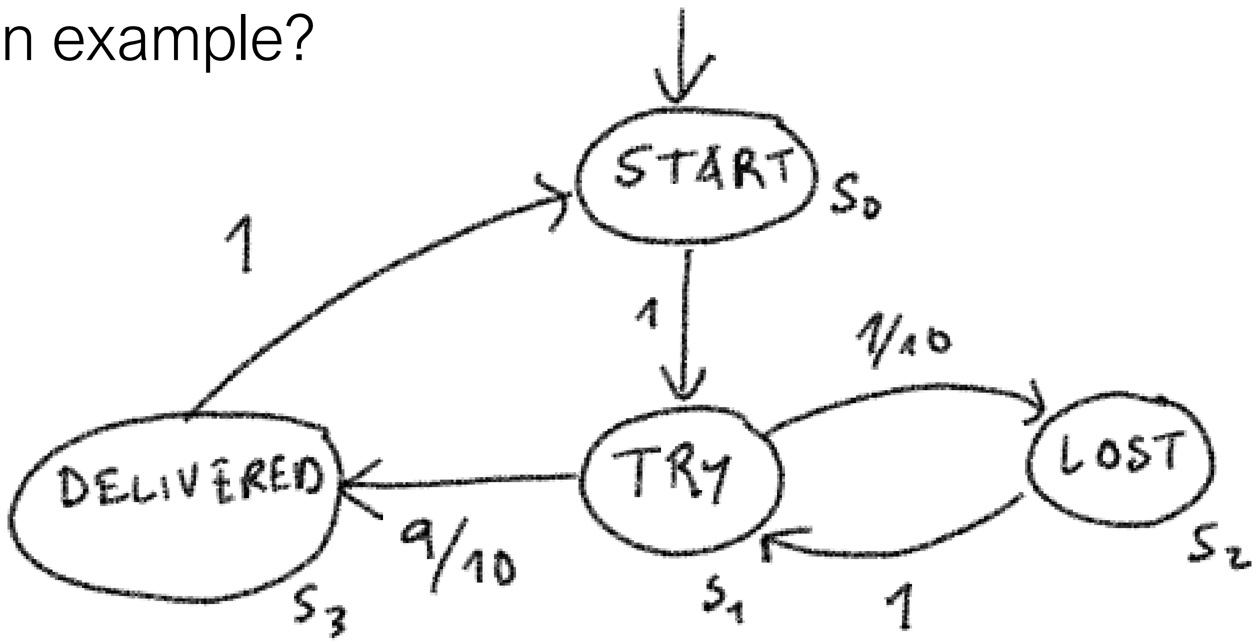
In the next lecture we will introduce **Probabilistic CTL** and we will see that the semantics is based on measuring the probabilities of sets of paths (based on cylinder sets).

If you want to measure the probability of a set of paths by hand, you need to decompose the set as a combination (complement/union/negation…) of cylinder sets. If you can't do that, then the probability of the set of paths cannot be measured. We have exercises on this, and you can also try with the examples in the textbook—see § 10.1.

In practice, efficient algorithms exist to measure probabilities of interesting sets of paths, e.g. expressed in PCTL. We will see this in a next lecture. Yay!

Cylinder set probability measure at work

Shall we try an example?



$$Pr_{s_0}(\Diamond\, \text{DELIVERED})\,?$$

$$\| $$

$$Pr_{s_0}\Big(\bigcup_{n \geq 0} \{ s_0\ s_1\ (s_2\ s_1)^n\ s_3 \ldots \}\Big)$$

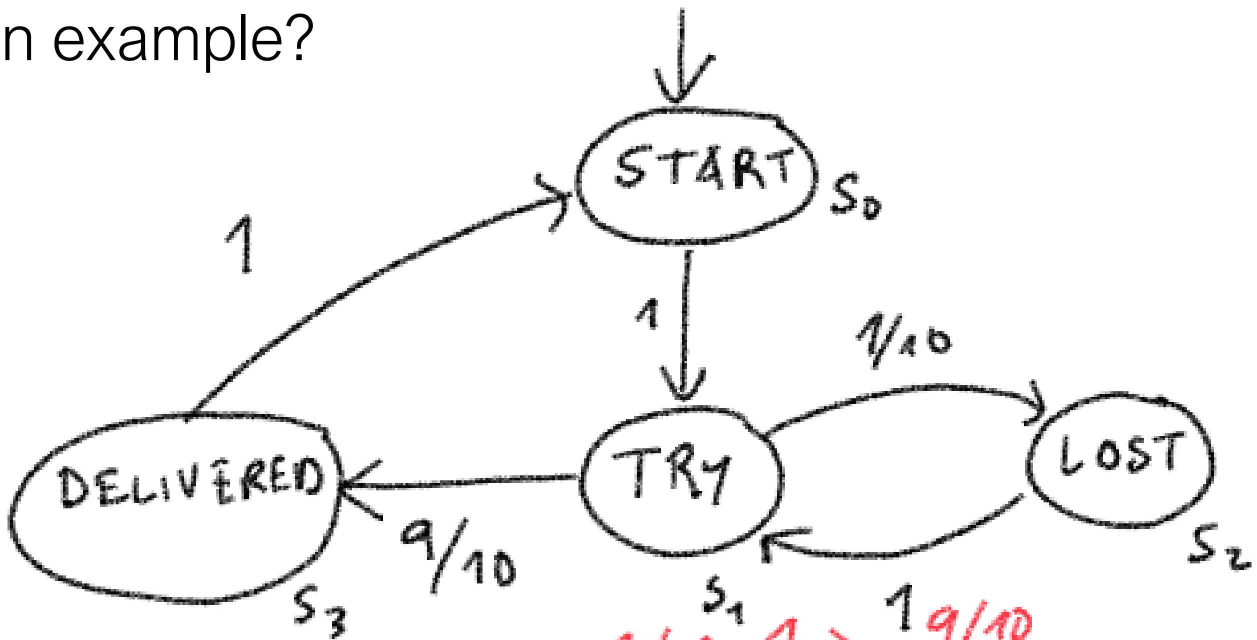
$$\| $$

$$\sum_{n \geq 0} \Big(Pr_{s_0}\big(\{ s_0\ s_1\ (s_2\ s_1)^n\ s_3 \ldots \}\big)\Big)$$

$$\sum_{n \geq 0} \Big(Pr_{s_0}\big(cyl\,(s_0\ s_1\ (s_2\ s_1)^n s_3)\big)\Big)$$

Cylinder set probability measure at work

Shall we try an example?



$$\sum_{n\geq 0}\left(Pr_{s_0}\left(cyl\left(s_0 \xrightarrow{1} s_1 \xrightarrow{1/10} (s_2 \xrightarrow{1} s_1)^n \xrightarrow{9/10} s_3 \right)\right)\right)$$

$$\sum_{n\geq 0} (1/10)^n \cdot 9/10 = 9/10 \cdot \frac{1}{1-\frac{1}{10}} = 9/10 \cdot \frac{10}{9} = 1$$

Discrete-Time Markov Chains

- Discrete-Time Markov Chains (DTMCs)
- Transient Distributions
- Steady State Distribution
- Reachability Probabilities
- Probabilities of Sets of Paths
- Exercises & Homework

Key points of this lecture

Definition of Discrete-Time Markov Chain (DTMC), a probabilistic variant of transition systems.

Transient distribution of a DTMC, an indication of the probability of being in each of the states after n steps.

Steady state distribution, a stationary distribution that, in some cases, coincides with the limit of the transient distribution.

How to measure the probability of simple reachability properties by hand.

How to measure the probability of (certain) sets of paths in a DTMC.

How to use PRISM and Z3 to compute transient state distributions, steady states distributions and reachability probabilities.

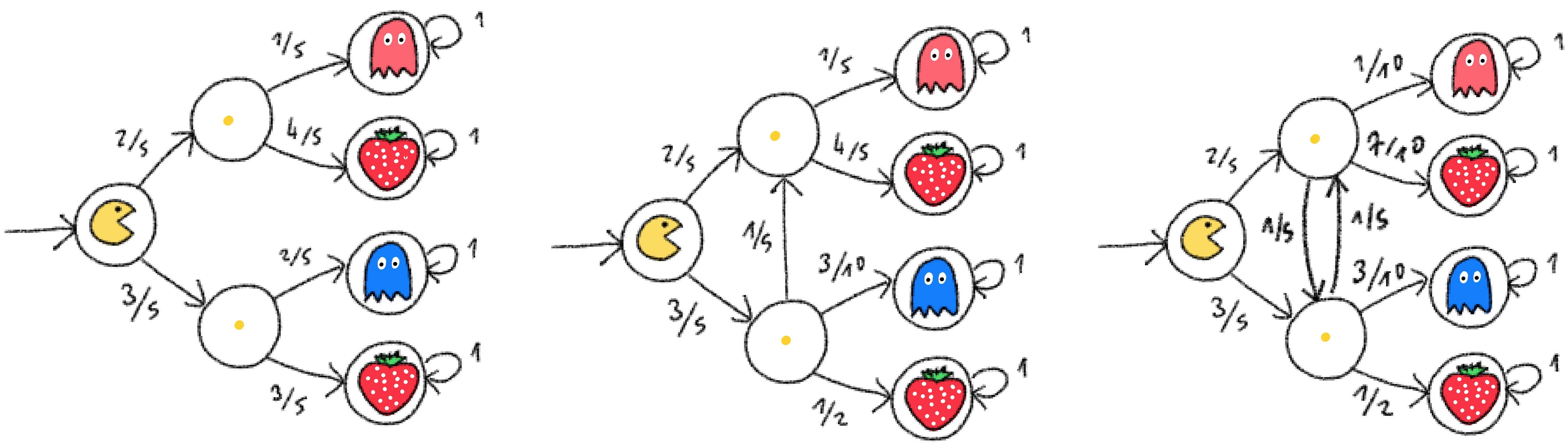
Discrete-Time Markov Chains

- Discrete-Time Markov Chains (DTMCs)
- Transient Distributions
- Steady State Distribution
- Reachability Probabilities
- Probabilities of Sets of Paths
- Exercises & Homework

APPENDIX: Exercises

Exercise 06.1

Consider the following DTMCs that describe how PACMAN can move through different places (states) while everything else (e.g. ghosts) is frozen.



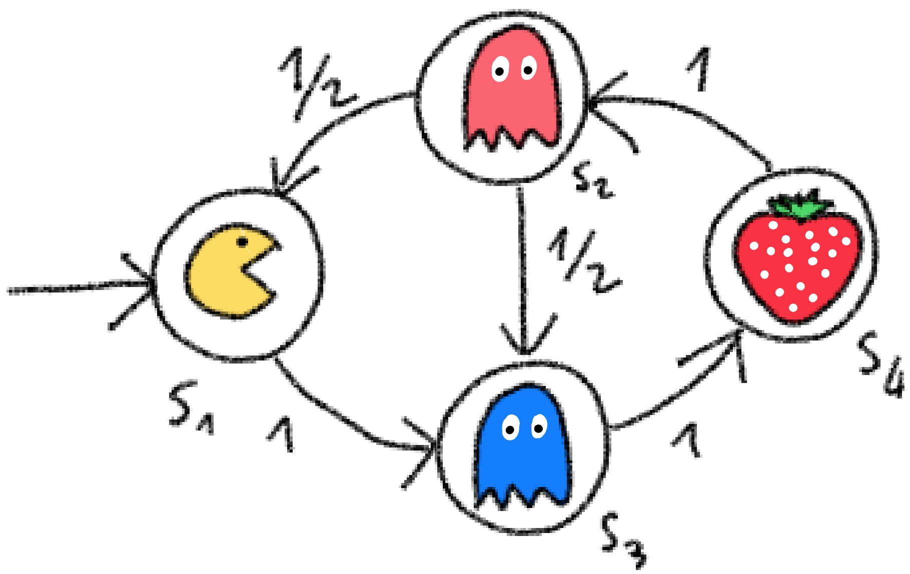
(a) (b) (c)

Calculate the probability that PACMAN reaches a strawberry.
Base your computations on the probability measure Pr.

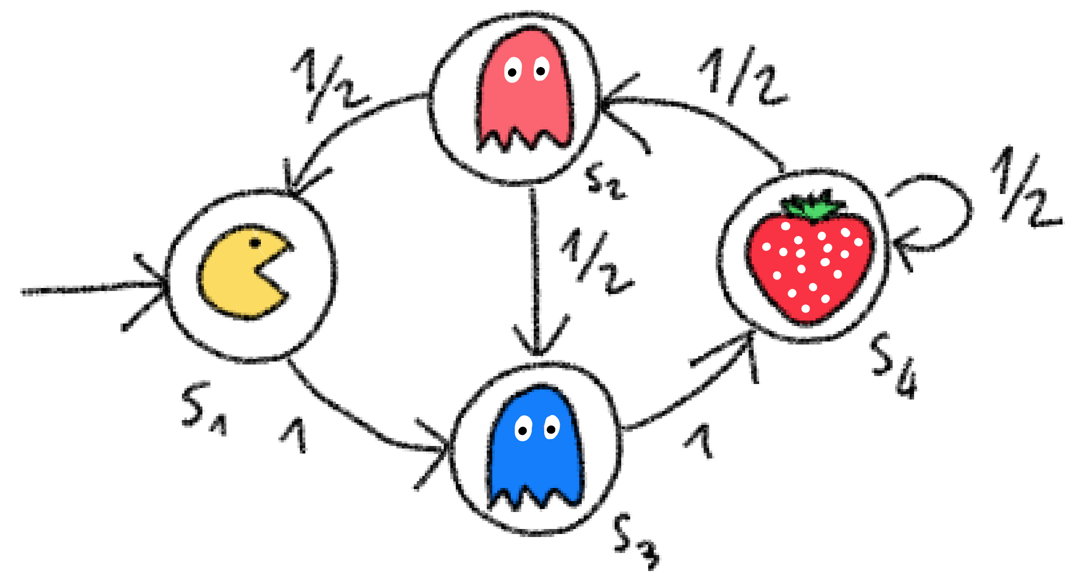
Double-check your results with PRISM.

Exercise 06.2

For each of the following DTMCs calculate the transient distribution θ_n for n = 2, 4, 8.



(a)



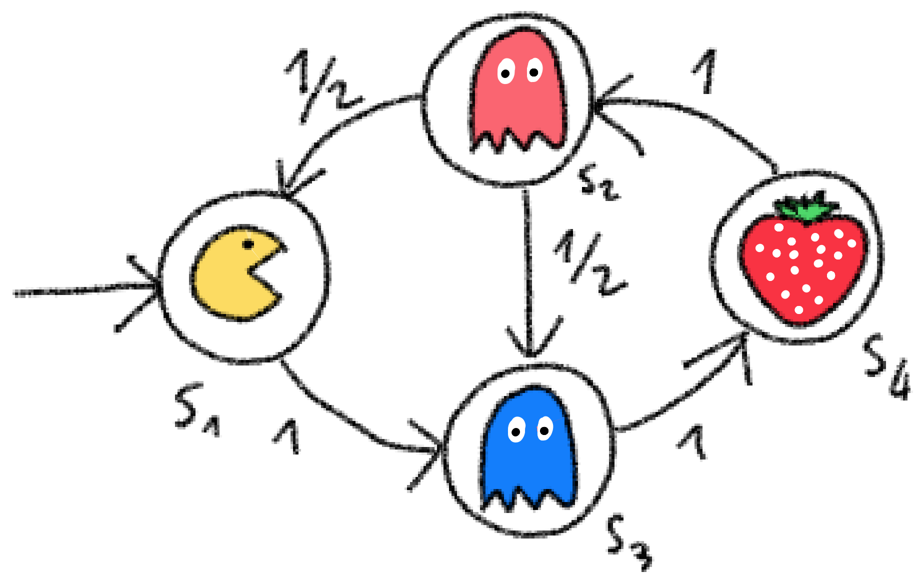
(b)

Do the calculations by hand.

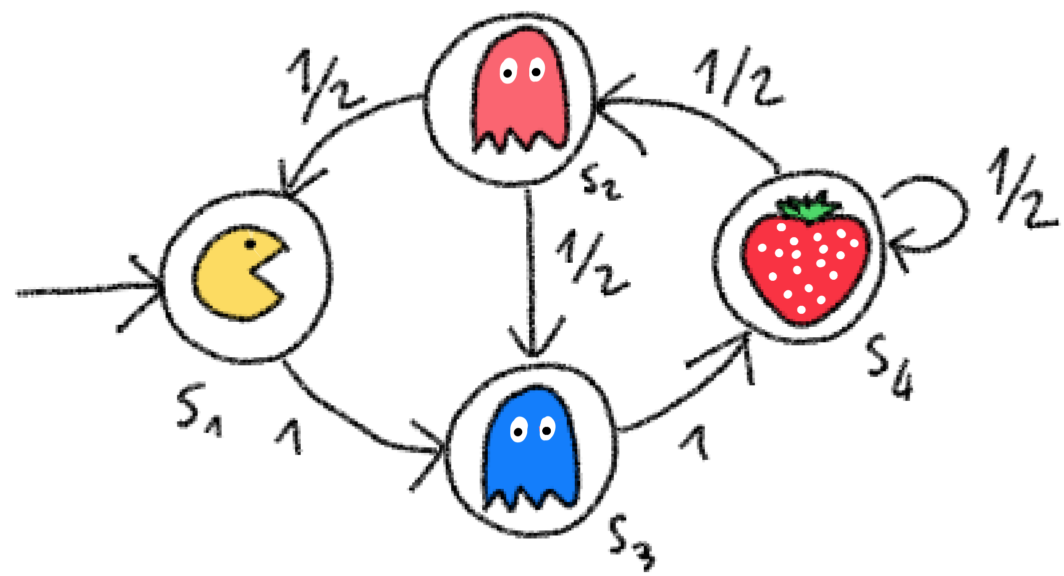
Double-check your results with PRISM.

Exercise 06.3

For each of the following DTMCs calculate the steady-state probability. What is the steady state probability of states where PACMAN coincides with a ghost?



(a)



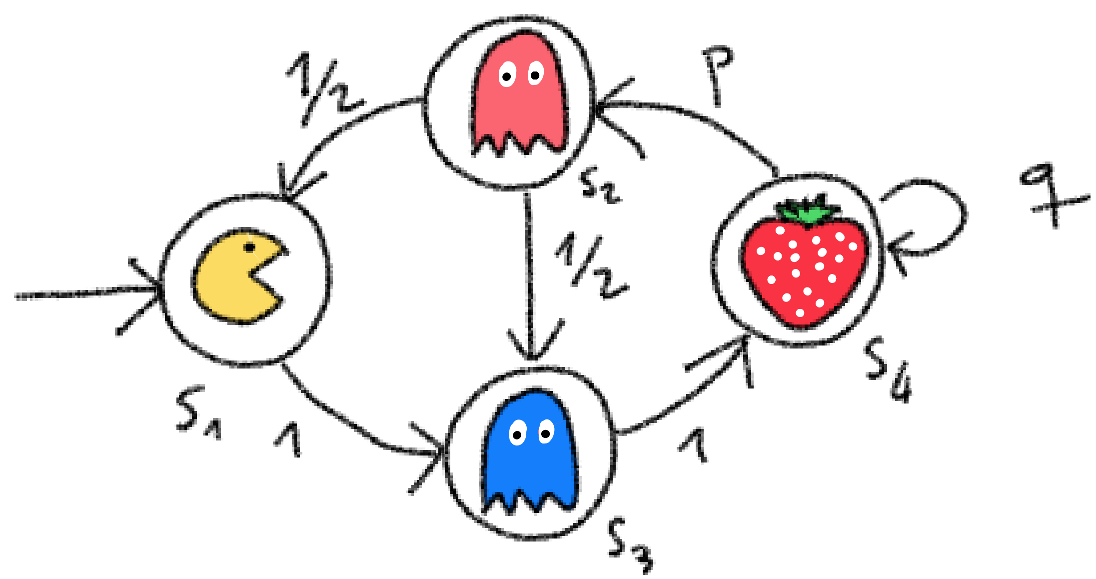
(b)

Do the calculations by first writing down the system of equations whose solution is the steady state. Solve the equations by hand and using Z3.

Double-check your result in PRISM.

Exercise 06.4

Consider the following DTMC where p and q are unknown.



Find values for p and q such that in the steady state, the probability of being in the strawberry state is above 8/10 and below 9/10.

Use Z3 to solve the exercise.