



Software Modeling  
and Verification Chair

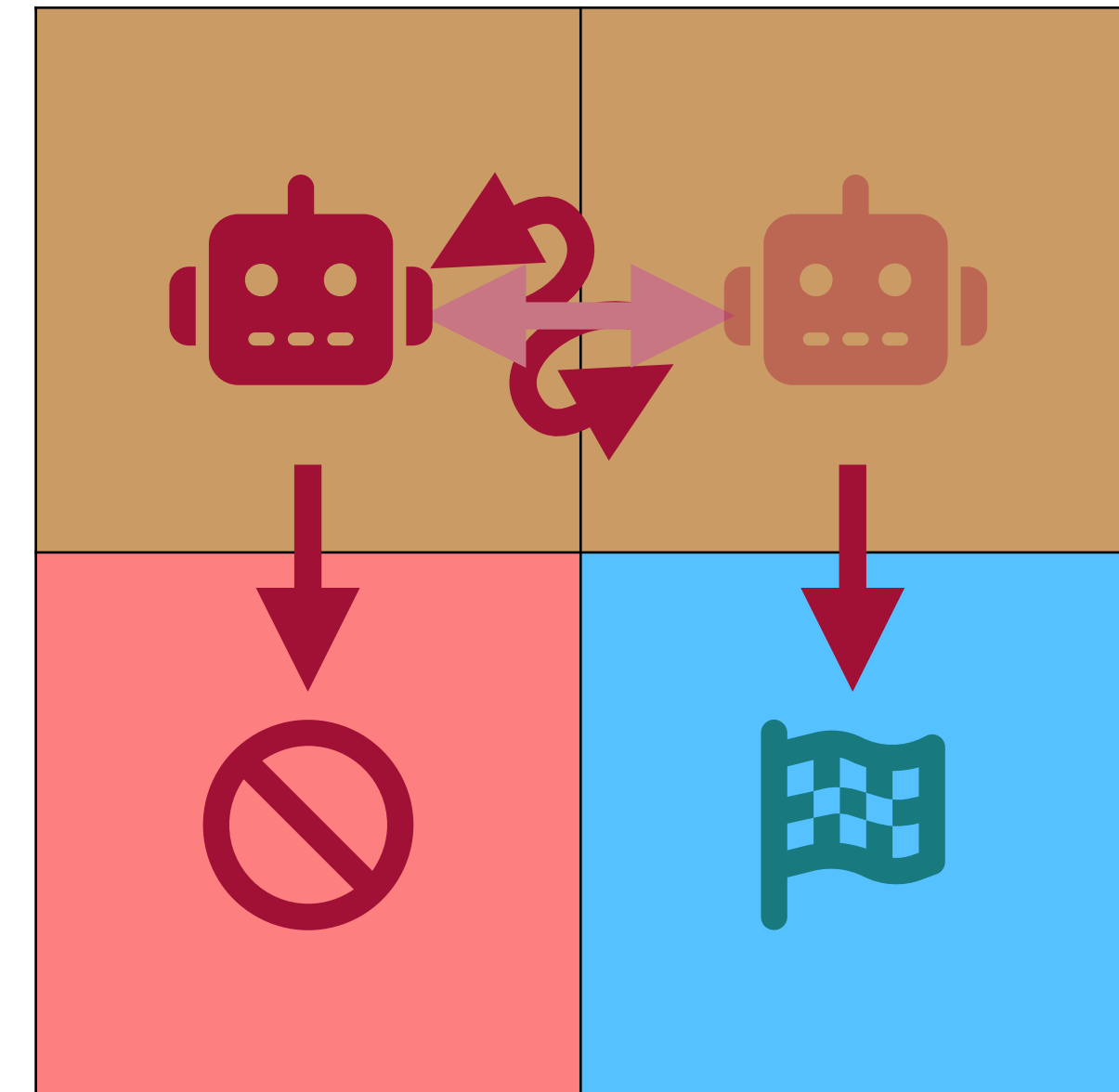
**RWTH**AACHEN  
UNIVERSITY

# Current *MOVES* in Probabilistic Model Checking

JPK 60 / Alumni Day

**Tim Quatmann**

**Alexander Bork, Hannah Mertens, Tobais Winkler**



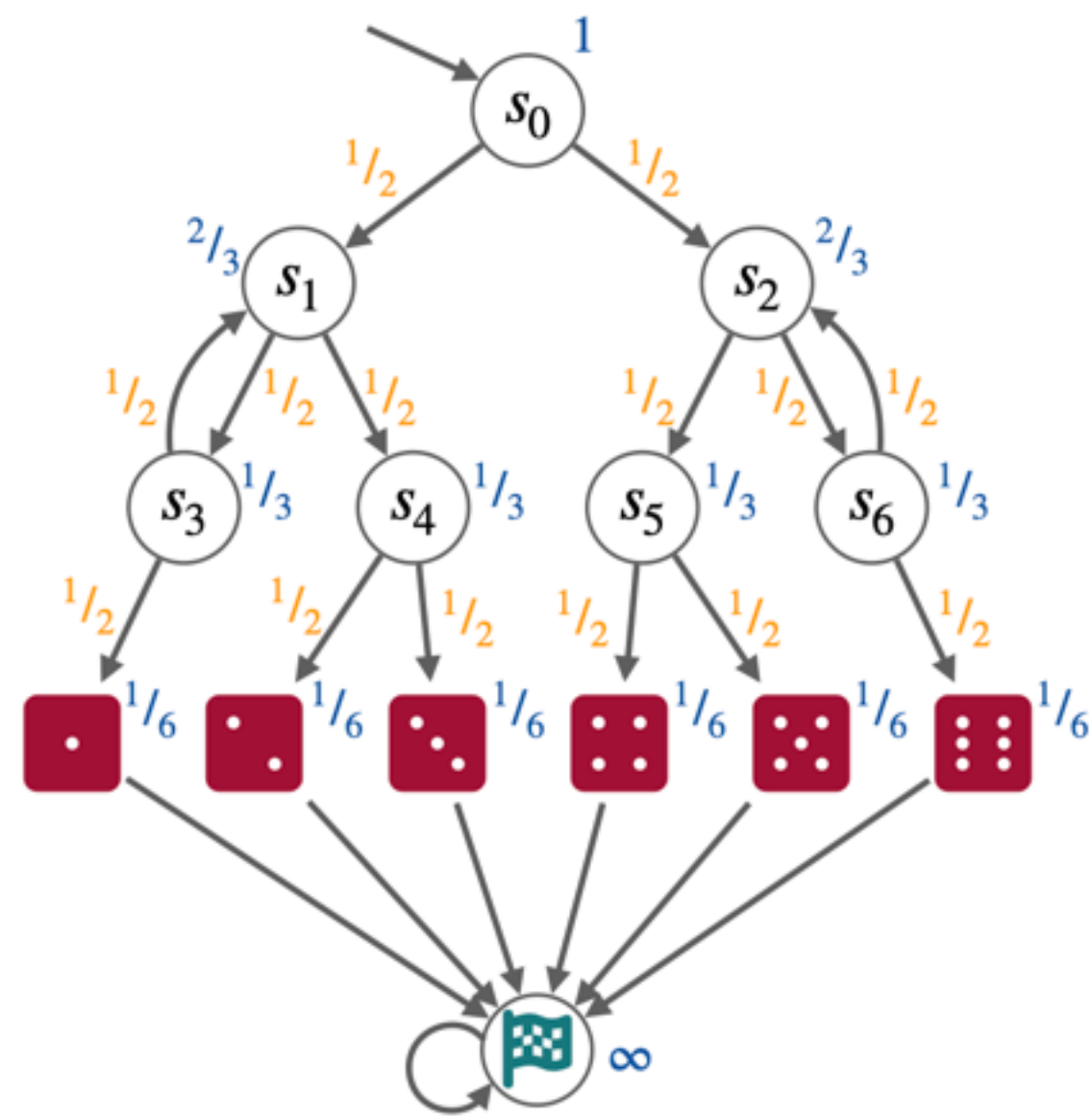
# The Probabilistic Model Checking Landscape \*

RWTH Aachen University, Germany and University of Twente, The Netherlands  
Joost-Pieter Katoen  
katoen@cs.rwth-aachen.de

**“Randomization is a key element in sequential and distributed computing.**

**Reasoning about randomized algorithms is highly non-trivial.”**

# Current Topics at the MOVES Group



**Expected Visiting Times**

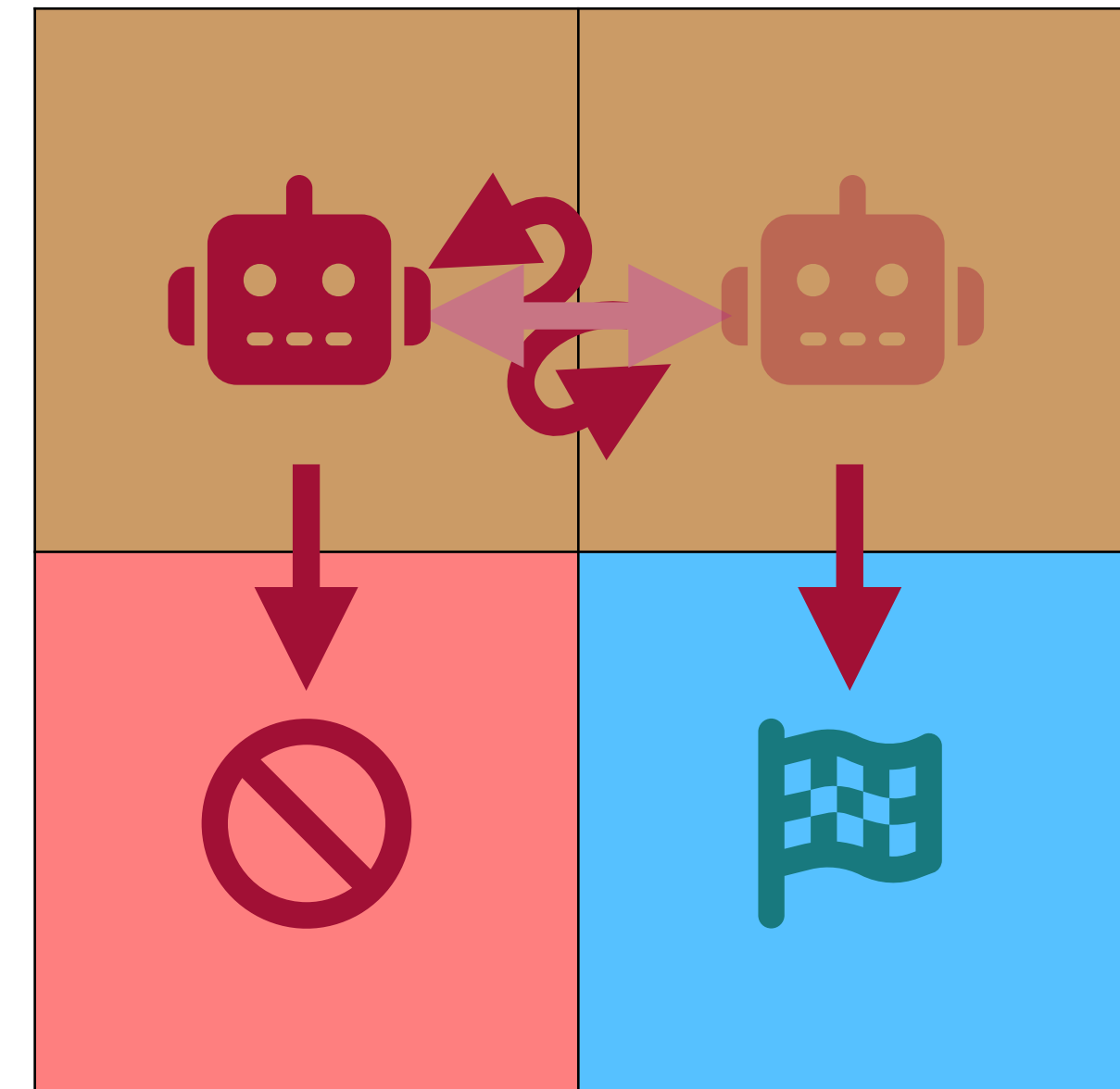
Upper bounds on minimal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\min}(x) \leq x$

Upper bounds on maximal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\max}(x) \leq x$

Lower bounds on minimal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\min}(x) \geq x$   
 $r \in \bar{\mathbb{N}}^S \quad \mathcal{D}^{\max}(r) \leq r$   
 $x(s) > 0 \implies r(s) < \infty$

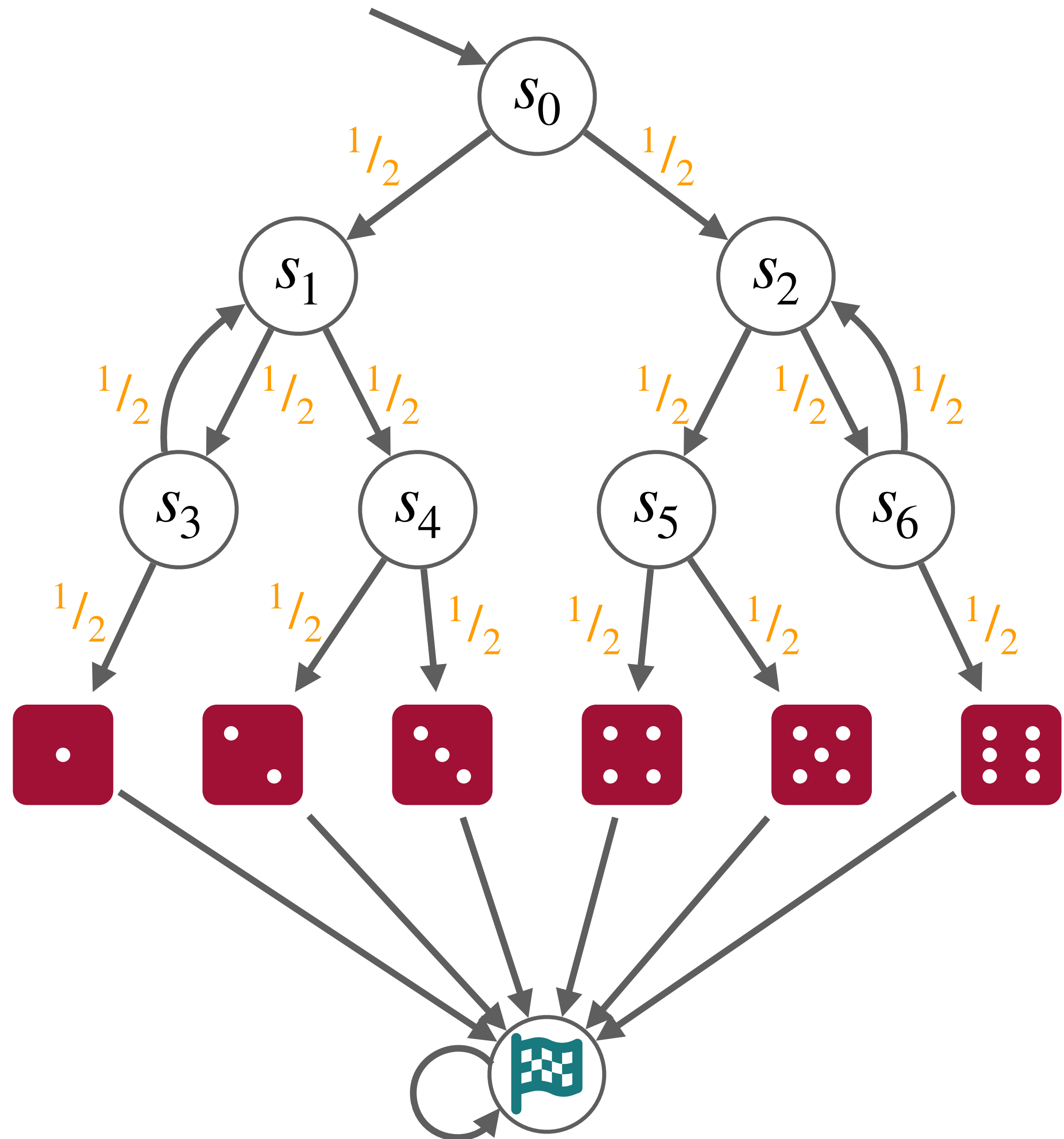
Lower bounds on maximal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\max}(x) \geq x$   
 $r \in \bar{\mathbb{N}}^S \quad \mathcal{D}_{x^\uparrow}^{\min}(r) \leq r$   
 $x(s) > 0 \implies r(s) < \infty$



**Certificates**



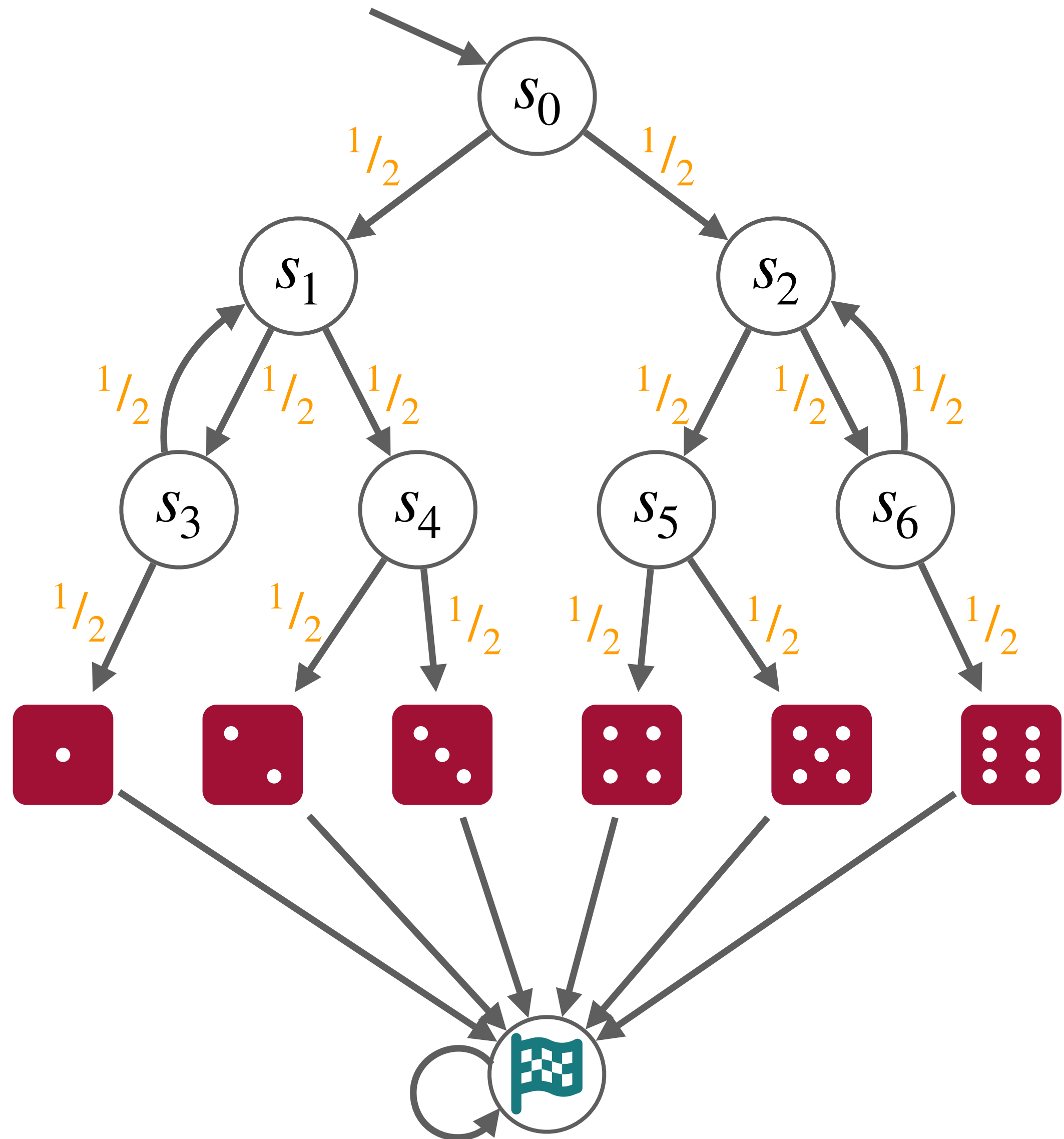
**Partially Observable MDPS**



# Kuth-Yao's Dice



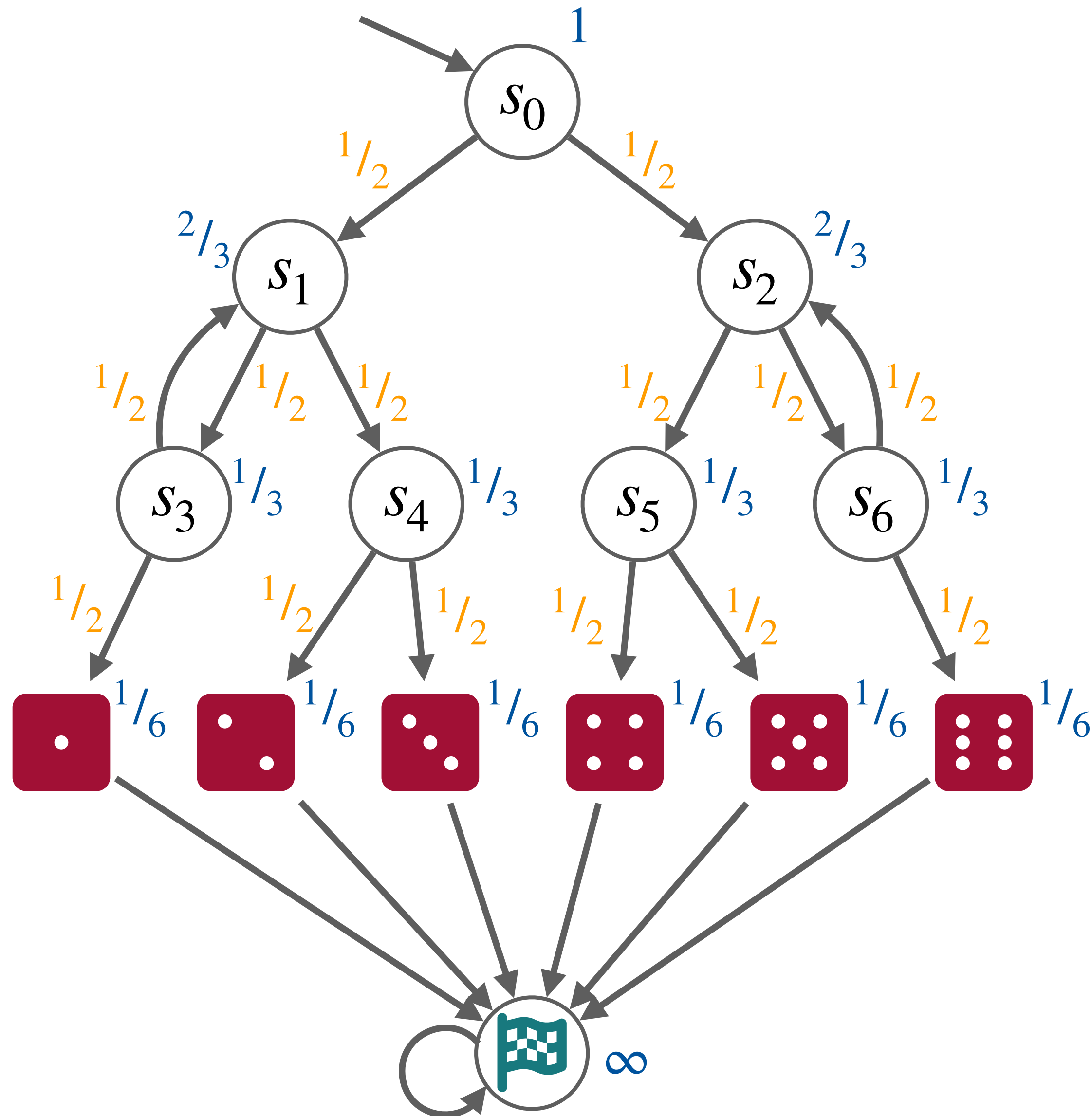
- Simulate 6-sided dice by a 2-sided coin
- Verify that the distribution is indeed uniform
- Traditional approach: compute reachability probabilities for each outcome  ... 
  - i.e. solve **six** equation systems



# Kuth-Yao's Dice



- Simulate 6-sided dice by a 2-sided coin
- Verify that the distribution is indeed uniform
- Traditional approach: compute reachability probabilities for each outcome  ... 
  - i.e. solve **six** equation systems
- Alternative: **Expected Visiting Times (EVTs)**
  - Requires solving a **single** equation system

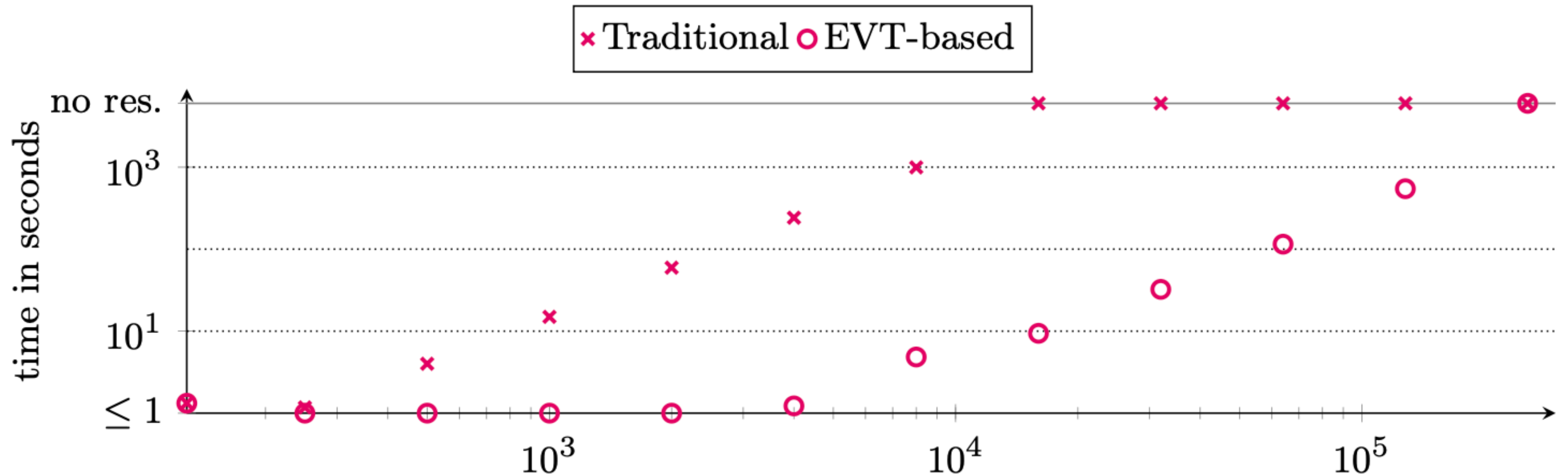
# Kuth-Yao's Dice



- Simulate 6-sided dice by a 2-sided coin
- Verify that the distribution is indeed uniform
- Traditional approach: compute reachability probabilities for each outcome  ... 
  - i.e. solve **six** equation systems
- Alternative: **Expected Visiting Times (EVTs)**
  - Requires solving a **single** equation system

# Computing Expected Visiting Times

Benchmarks on Lumbroso's  $N$ -sided Dice Roller — powered by **Storm** 

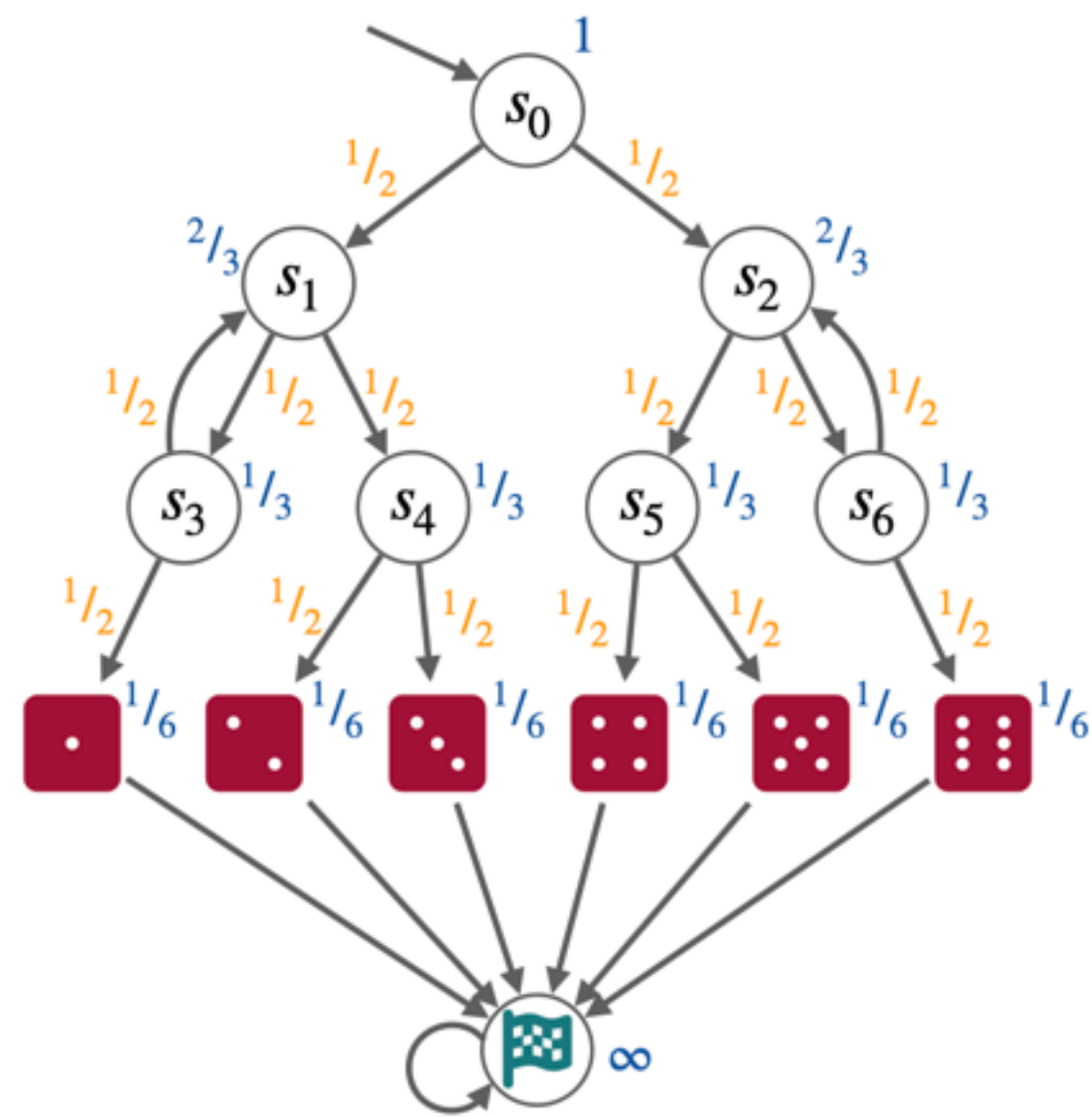


# Current Developments @i2

- **Sound** approximative methods for EVTs
  - Interval Iteration
  - Optimistic Value Iteration
- Connection to **Steady State Analysis**
- Preservation under **backward bisimulation**



# Current Topics at the MOVES Group



**Expected Visiting Times**

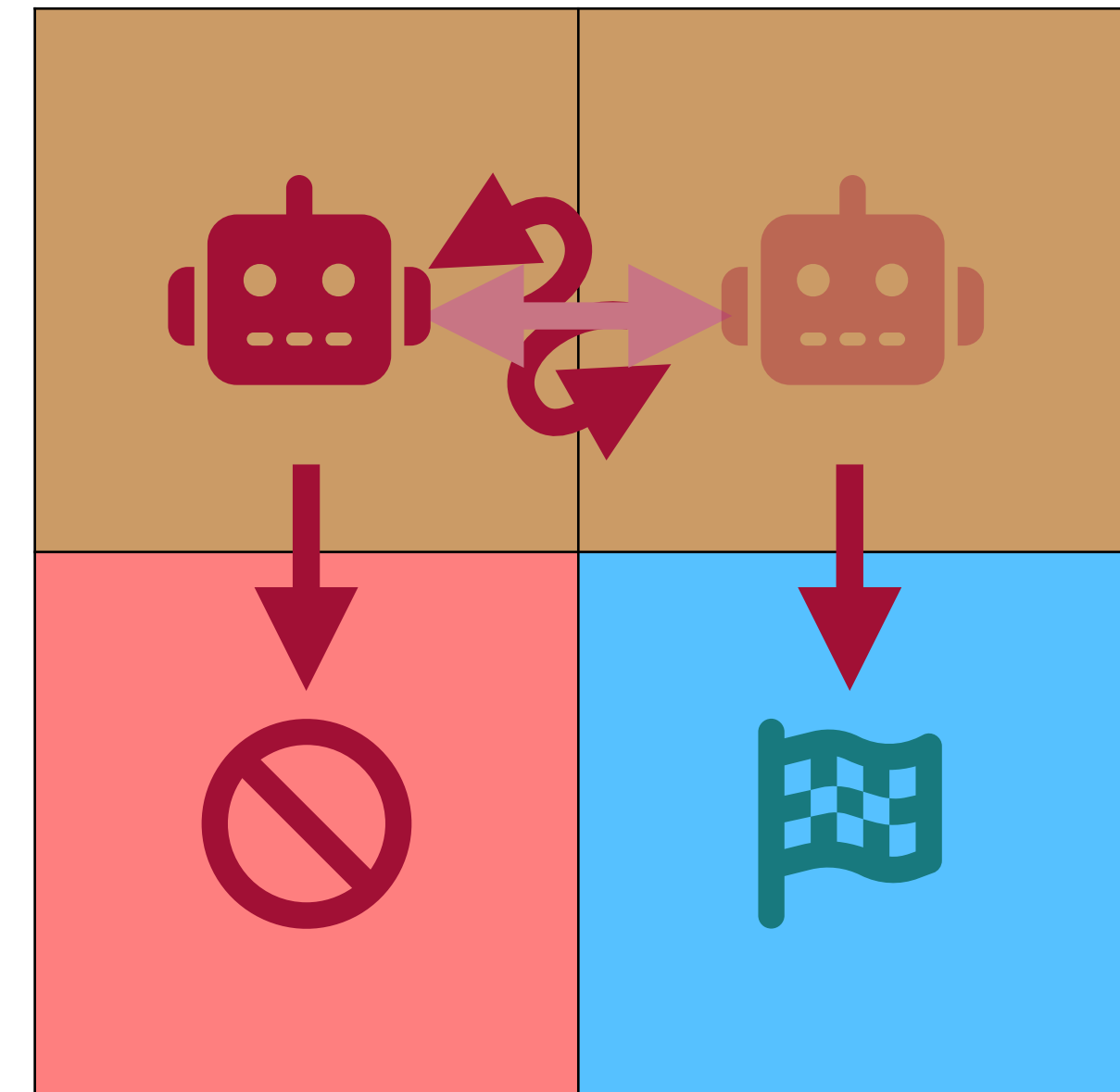
Upper bounds on minimal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\min}(x) \leq x$

Upper bounds on maximal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\max}(x) \leq x$

Lower bounds on minimal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\min}(x) \geq x$   
 $r \in \bar{\mathbb{N}}^S \quad \mathcal{D}^{\max}(r) \leq r$   
 $x(s) > 0 \implies r(s) < \infty$

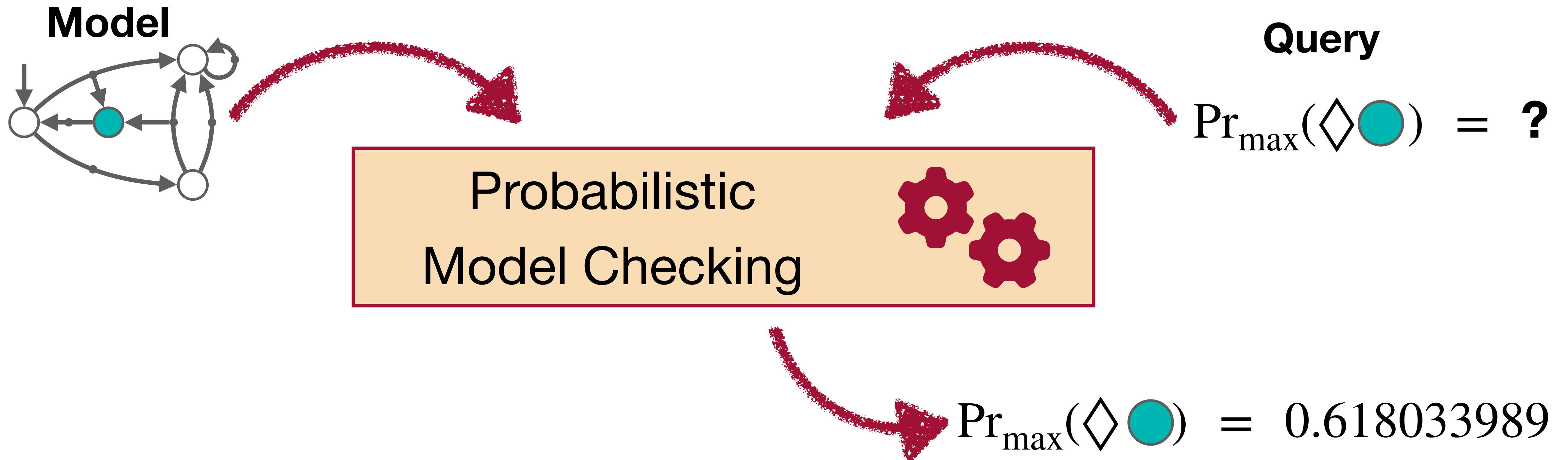
Lower bounds on maximal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\max}(x) \geq x$   
 $r \in \bar{\mathbb{N}}^S \quad \mathcal{D}_{x^\uparrow}^{\min}(r) \leq r$   
 $x(s) > 0 \implies r(s) < \infty$

**Certificates**



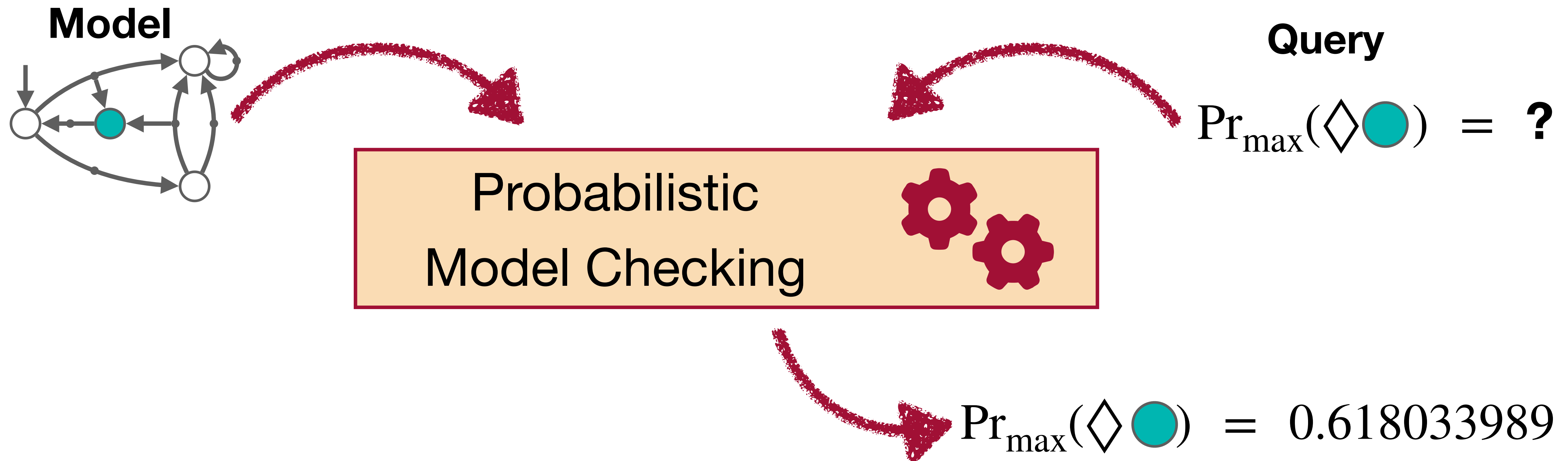
**Partially Observable MDPS**

# Can the model checking result be trusted?



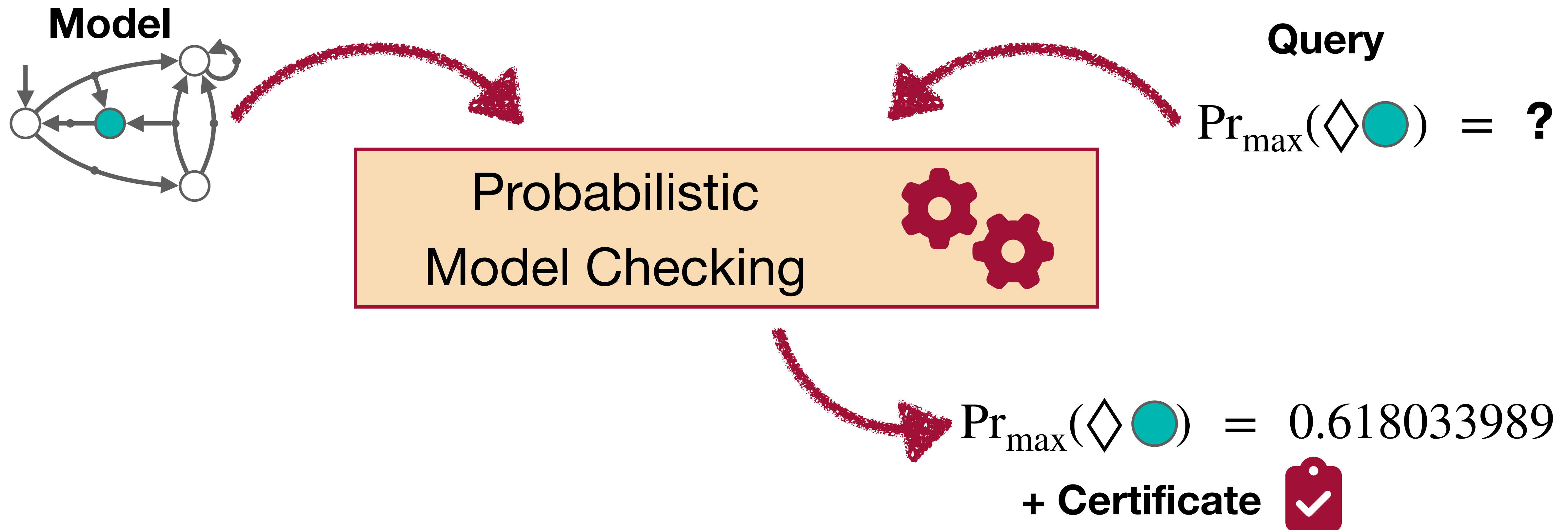
# Can the model checking result be trusted? **NO!**

- Approximative algorithms / floating point inaccuracies
- Implementation bugs



# Remedy: Certificates

- Easy to check for validity
- Certificate valid  $\implies$  Result correct



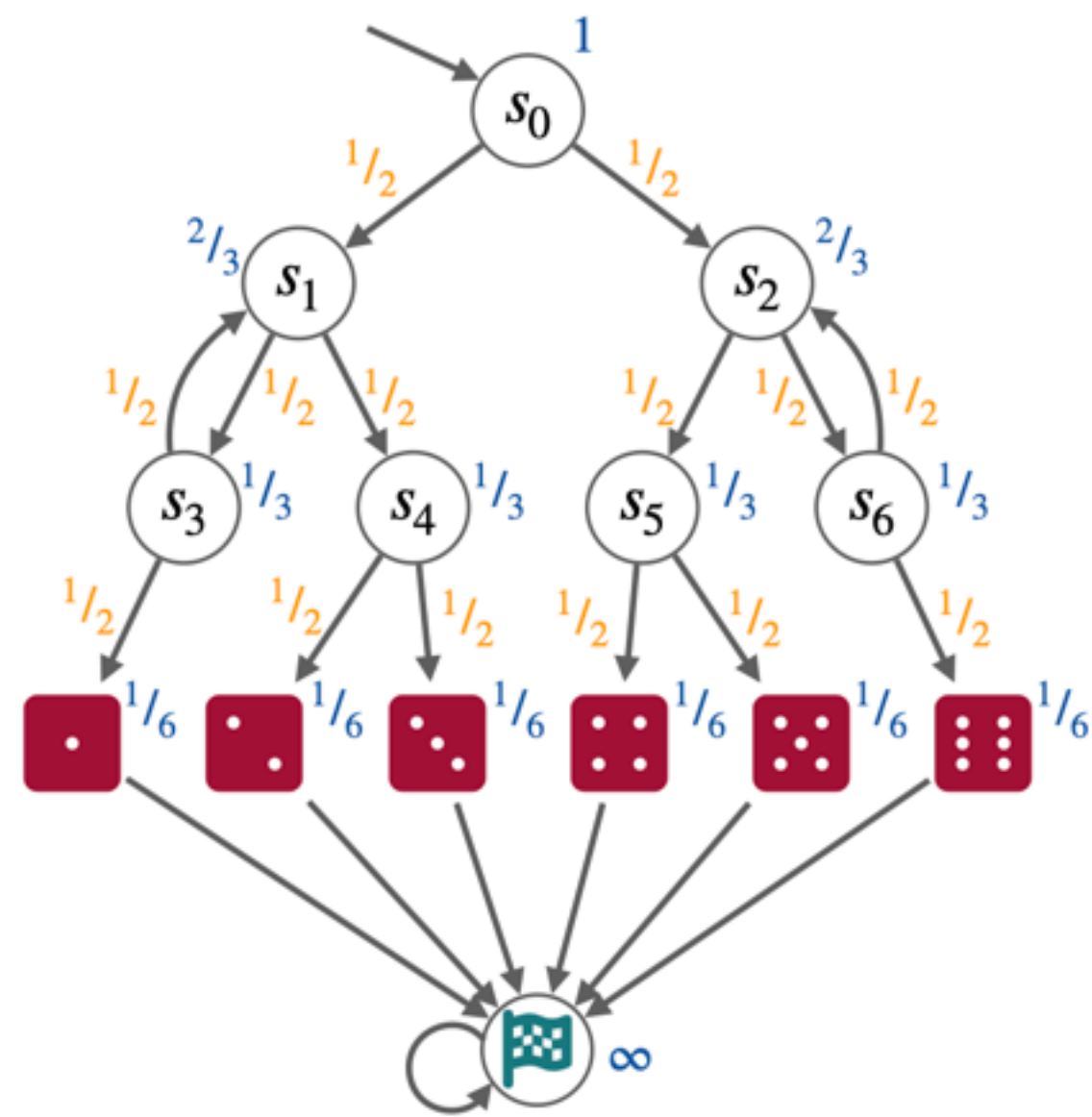
# Remedy: Certificates

Certificate	Condition(s)	Explanation
<b>Upper bounds on minimal</b>	<b>reachability probabilities:</b>	$\forall s \in S: \mathbb{P}_s^{\min}(\diamond T) \leq x(s)$ [Proposition 3]
$x \in [0, 1]^S$	$\mathcal{B}^{\min}(x) \leq x$	<i>min-Bellman operator <b>decreases</b> value of all states</i>

# Remedy: Certificates

Certificate	Condition(s)	Explanation
<b>Upper bounds on minimal</b> reachability probabilities:	$\forall s \in S: \mathbb{P}_s^{\min}(\diamond T) \leq x(s)$ [Proposition 3]	
$x \in [0, 1]^S$	$\mathcal{B}^{\min}(x) \leq x$	<i>min-Bellman operator <b>decreases</b> value of all states</i>
<b>Upper bounds on maximal</b> reachability probabilities:	$\forall s \in S: \mathbb{P}_s^{\max}(\diamond T) \leq x(s)$ [Proposition 3]	
$x \in [0, 1]^S$	$\mathcal{B}^{\max}(x) \leq x$	<i>max-Bellman operator <b>decreases</b> value of all states</i>
<b>Lower bounds on minimal</b> reachability probabilities:	$\forall s \in S: \mathbb{P}_s^{\min}(\diamond T) \geq x(s)$ [Proposition 4]	
$x \in [0, 1]^S$	$\mathcal{B}^{\min}(x) \geq x$	<i>min-Bellman operator <b>increases</b> value of all states</i>
$r \in \bar{\mathbb{N}}^S$	$\mathcal{D}^{\max}(r) \leq r$	<i>r upper bounds <b>maximal</b> distances to T</i>
	$x(s) > 0 \implies r(s) < \infty$	<i>positive reachability necessitates finite distance</i>
<b>Lower bounds on maximal</b> reachability probabilities:	$\forall s \in S: \mathbb{P}_s^{\max}(\diamond T) \geq x(s)$ [Proposition 6]	
$x \in [0, 1]^S$	$\mathcal{B}^{\max}(x) \geq x$	<i>max-Bellman operator <b>increases</b> value of all states</i>
$r \in \bar{\mathbb{N}}^S$	$\mathcal{D}_{x\uparrow}^{\min}(r) \leq r$	<i>r upper bounds <b>min.</b> distances to T via <b>x-incr. actions</b></i>
	$x(s) > 0 \implies r(s) < \infty$	<i>positive reachability necessitates finite distance</i>

# Current Topics at the MOVES Group



**Expected Visiting Times**

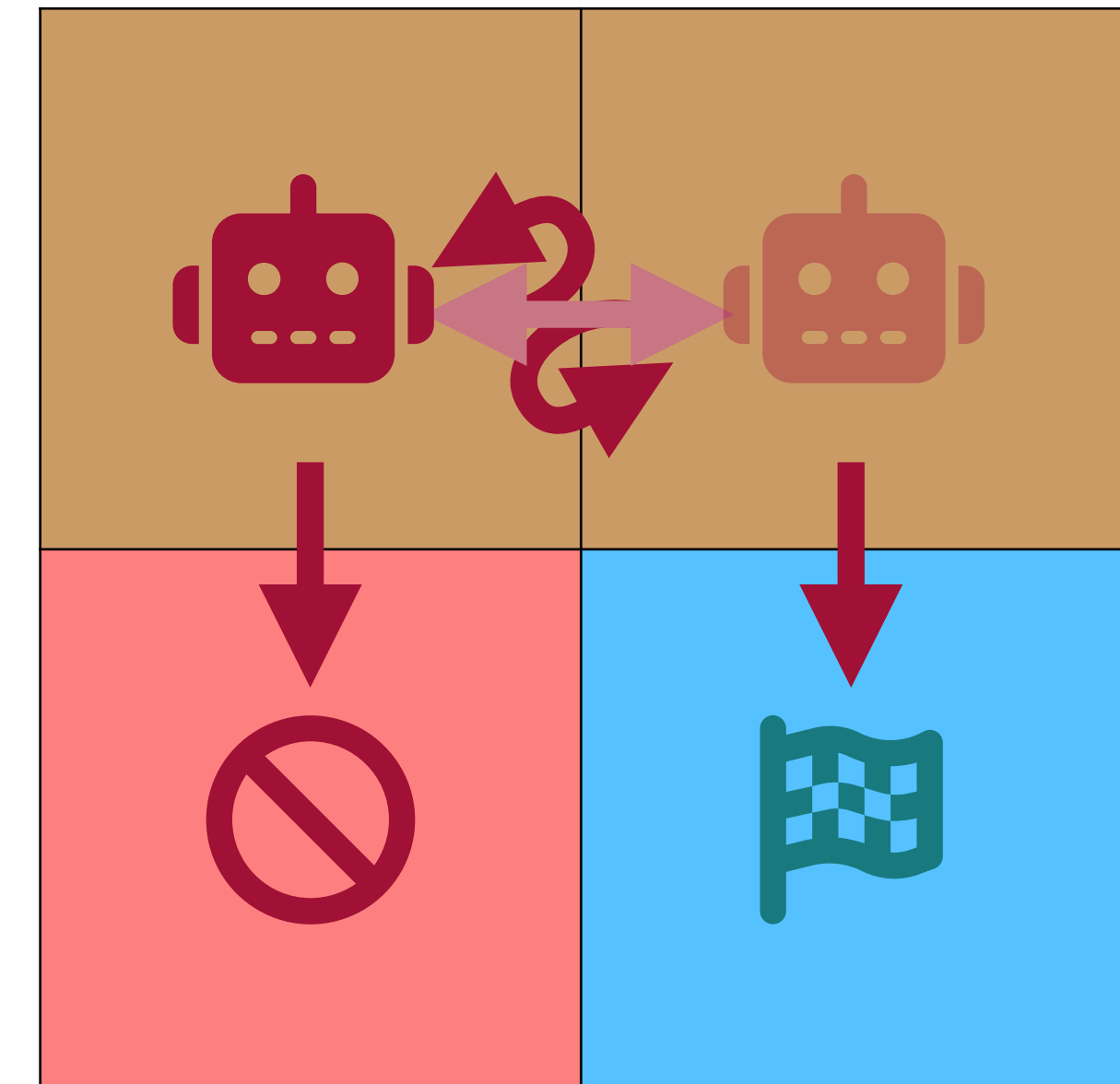
Upper bounds on minimal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\min}(x) \leq x$

Upper bounds on maximal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\max}(x) \leq x$

Lower bounds on minimal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\min}(x) \geq x$   
 $r \in \bar{\mathbb{N}}^S \quad \mathcal{D}^{\max}(r) \leq r$   
 $x(s) > 0 \implies r(s) < \infty$

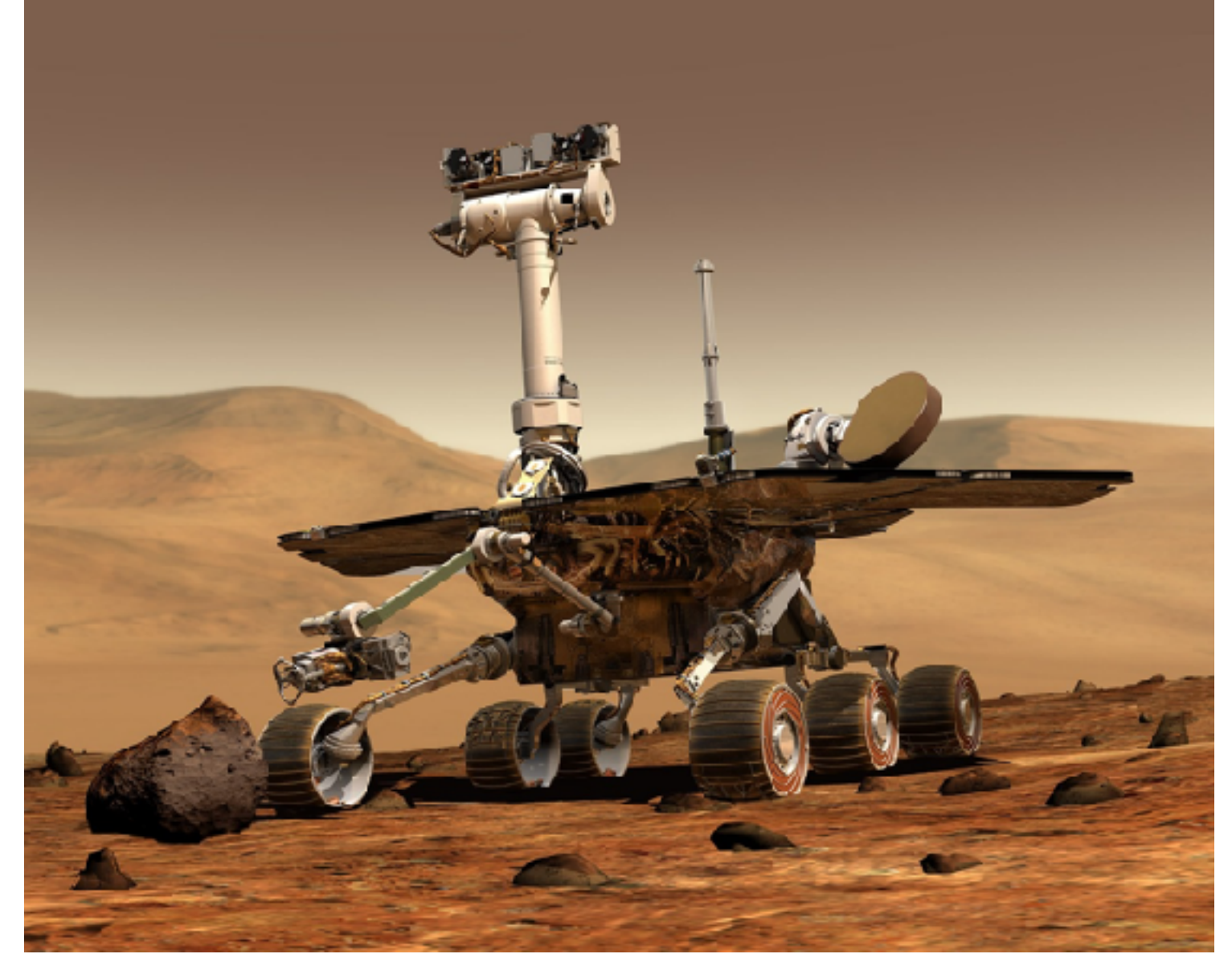
Lower bounds on maximal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\max}(x) \geq x$   
 $r \in \bar{\mathbb{N}}^S \quad \mathcal{D}_{x^\uparrow}^{\min}(r) \leq r$   
 $x(s) > 0 \implies r(s) < \infty$

**Certificates**



**Partially Observable MDPS**

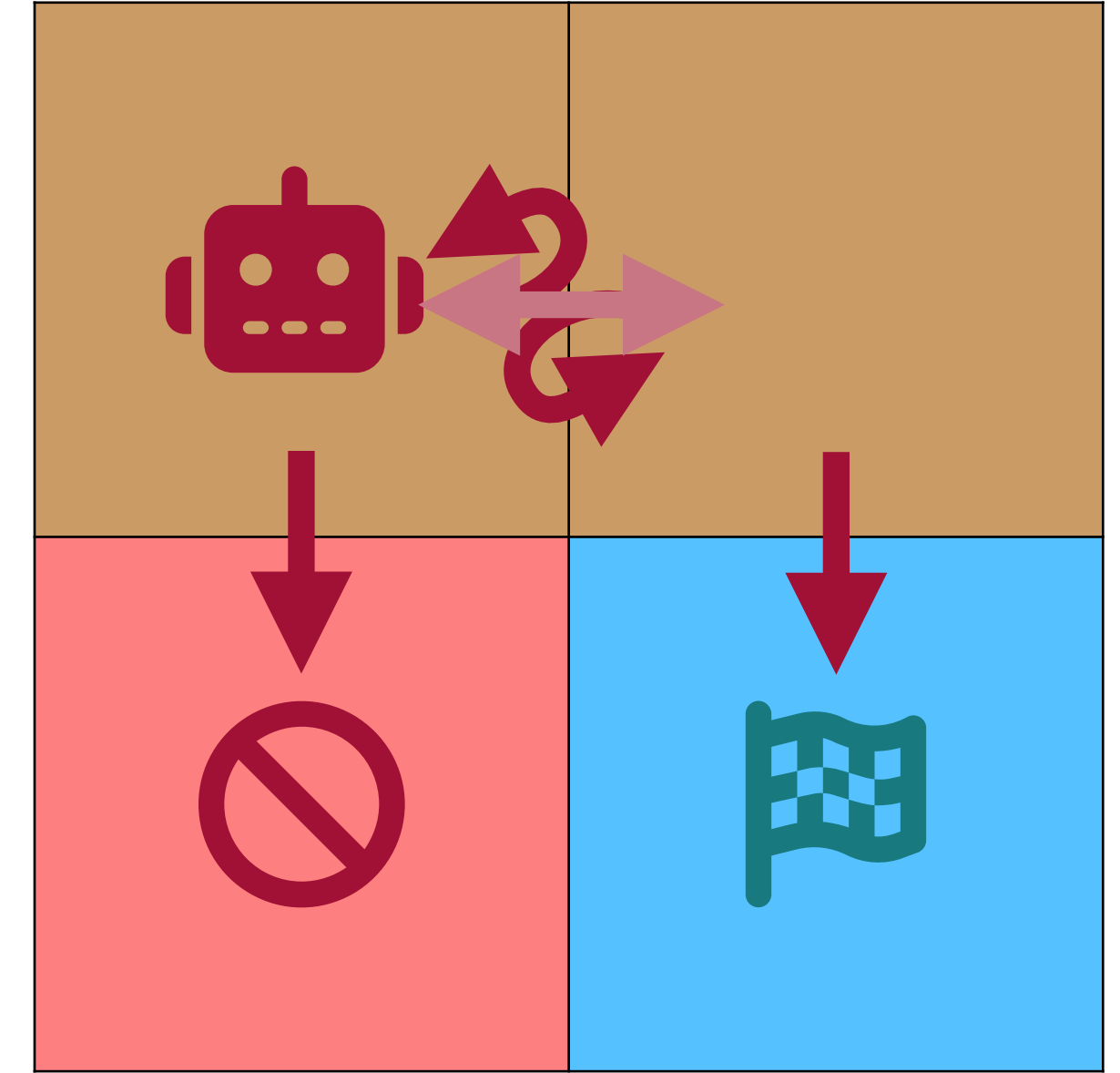
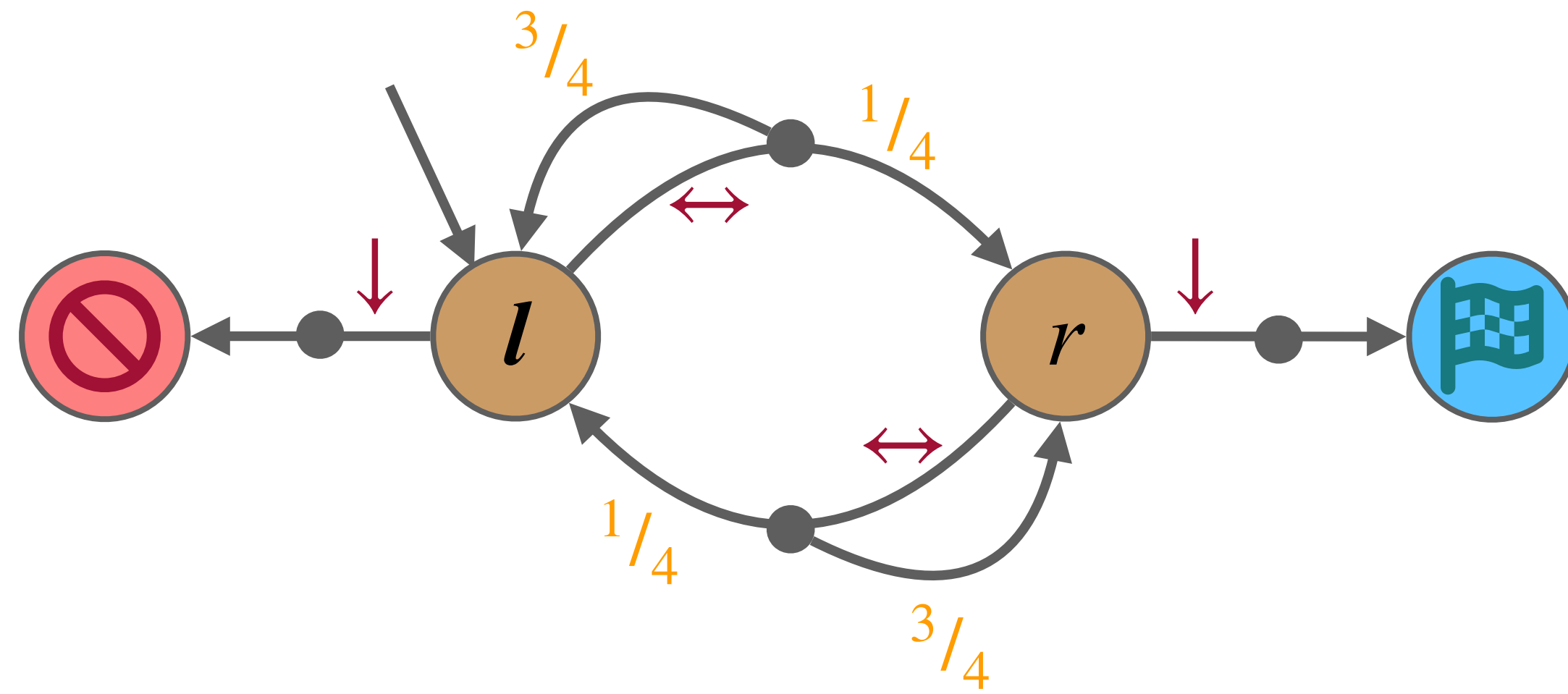
# Partially Observable MDPs





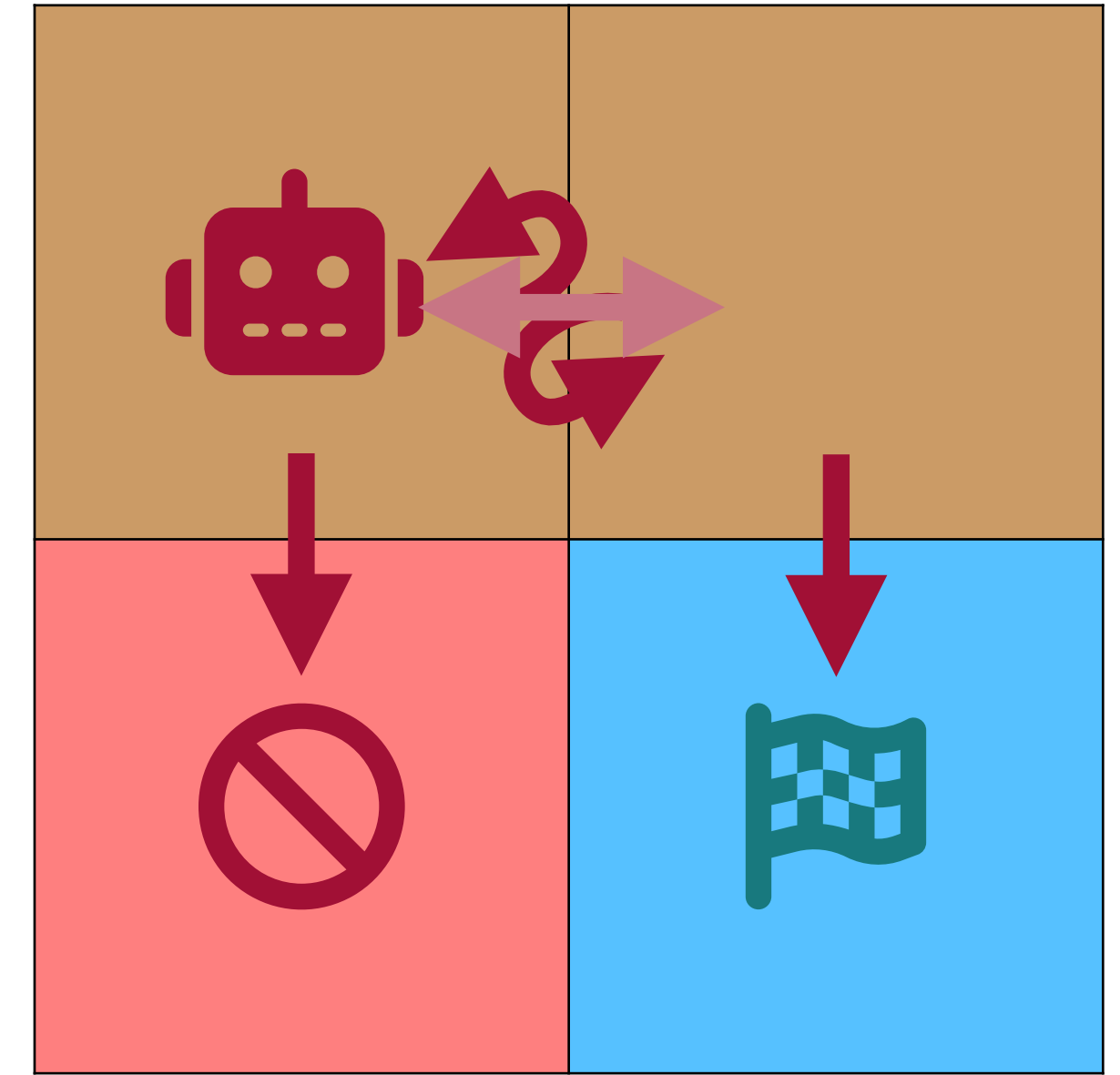
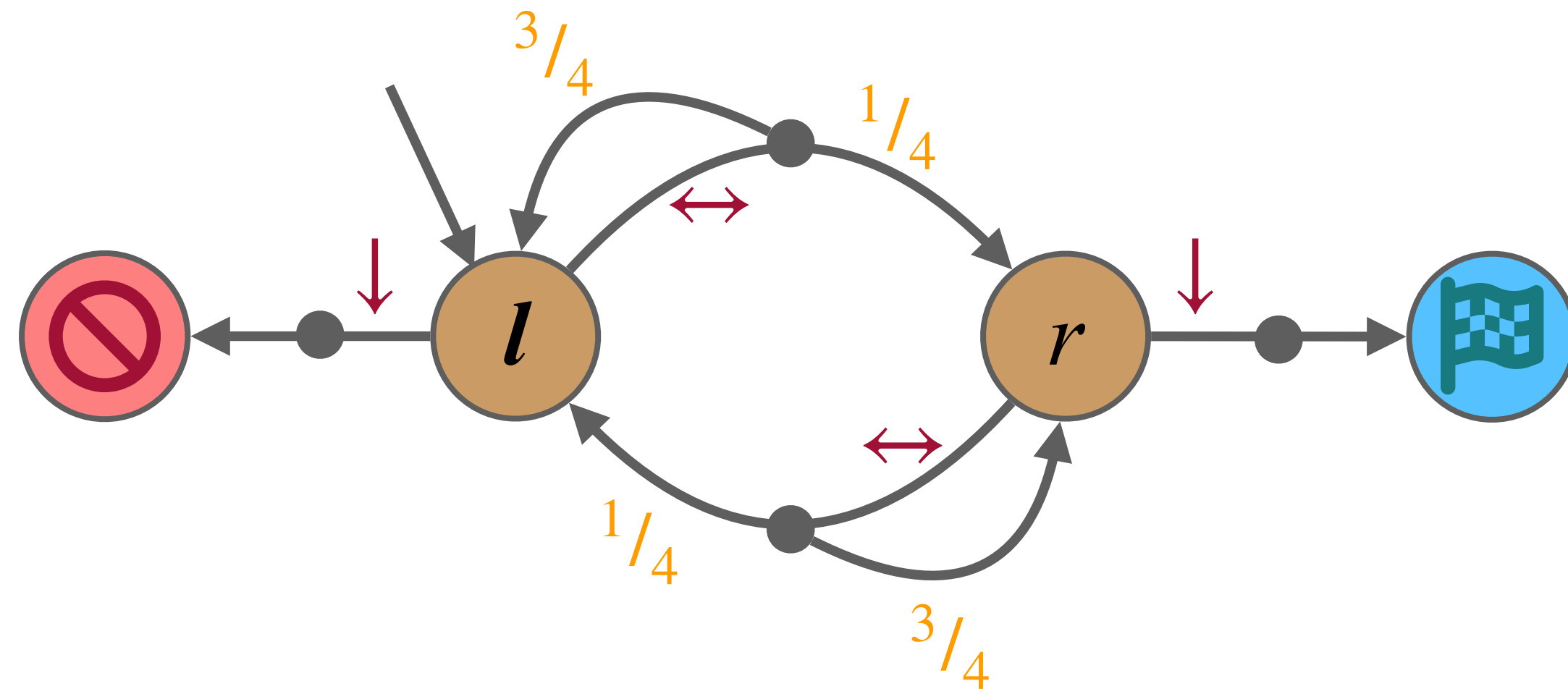
# Partially Observable MDPs

$\mathcal{P}$



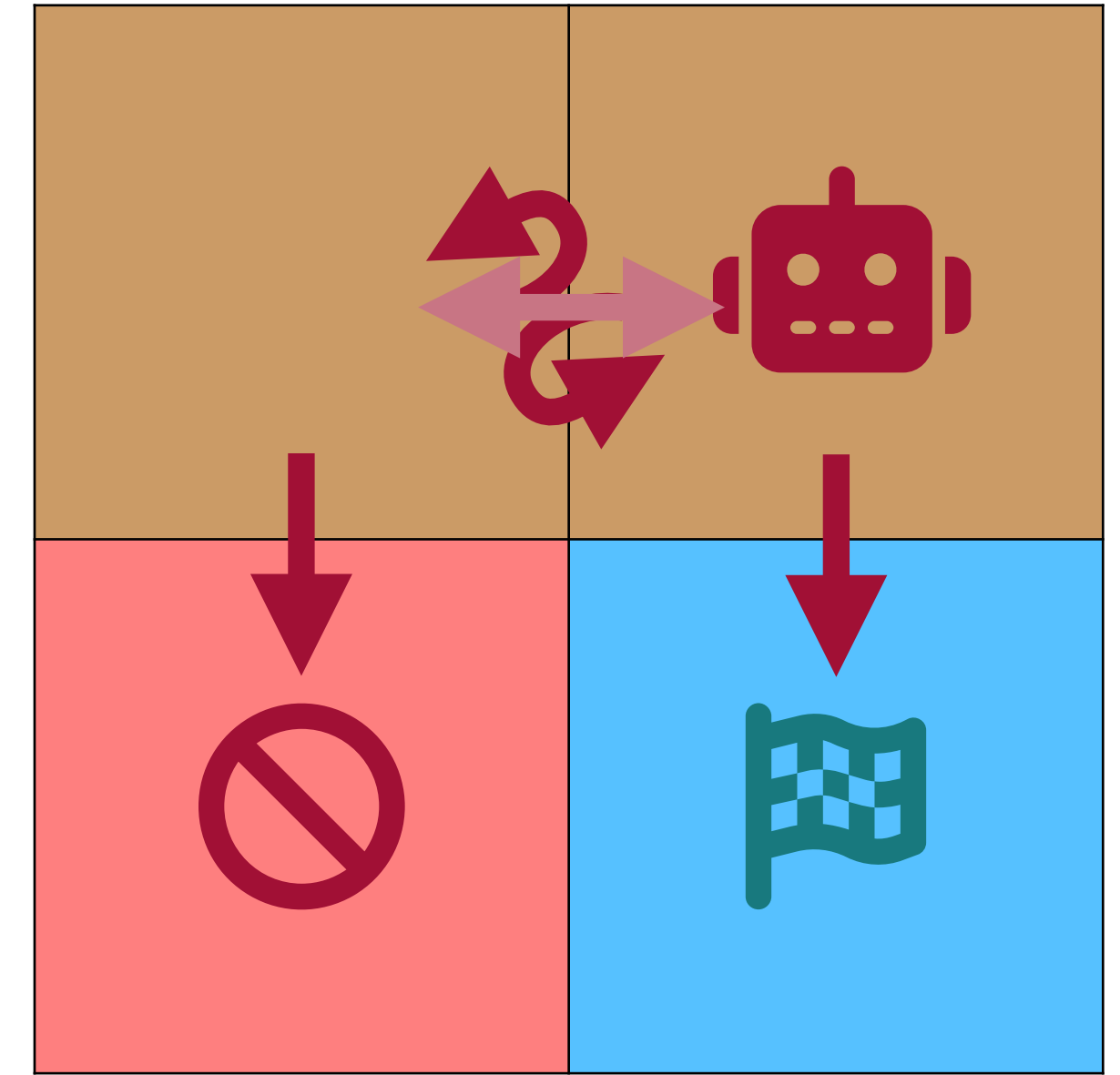
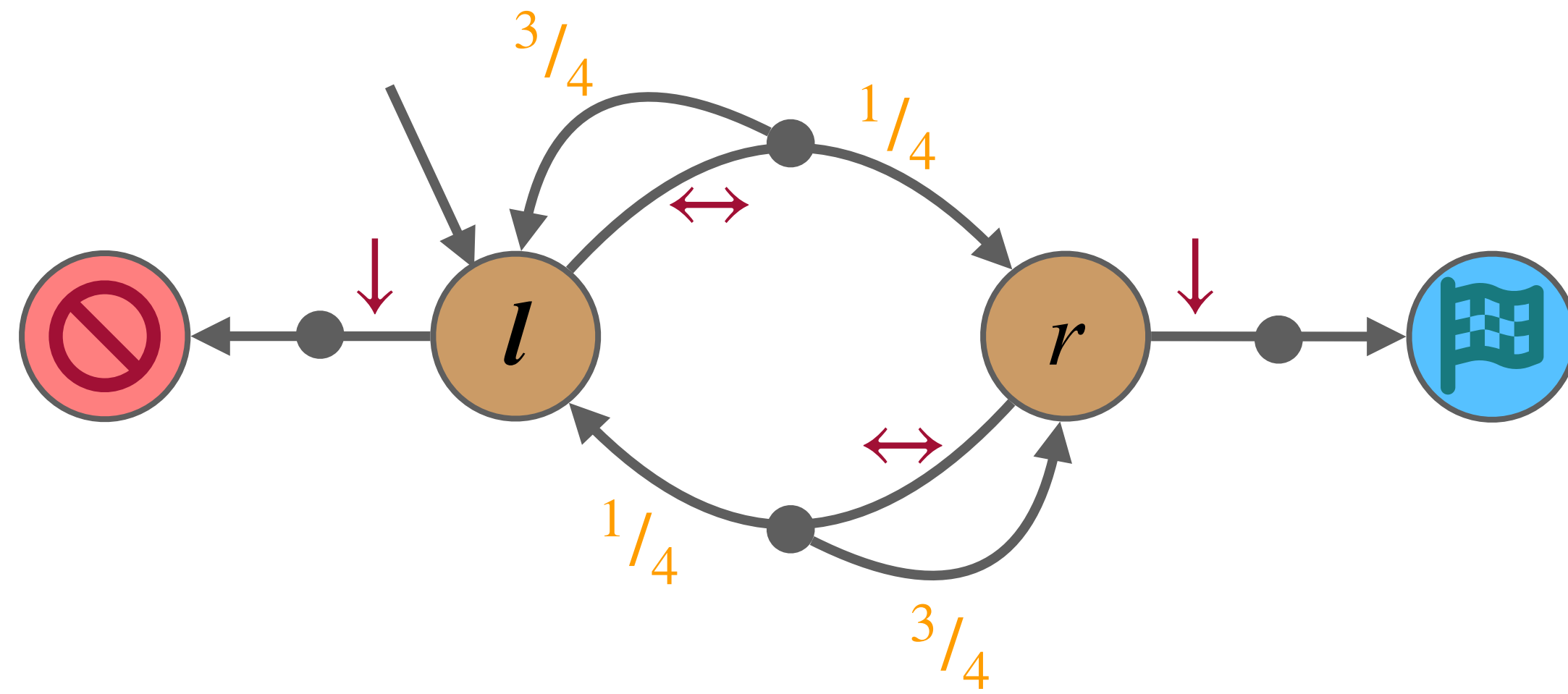
# Partially Observable MDPs

$\mathcal{P}$



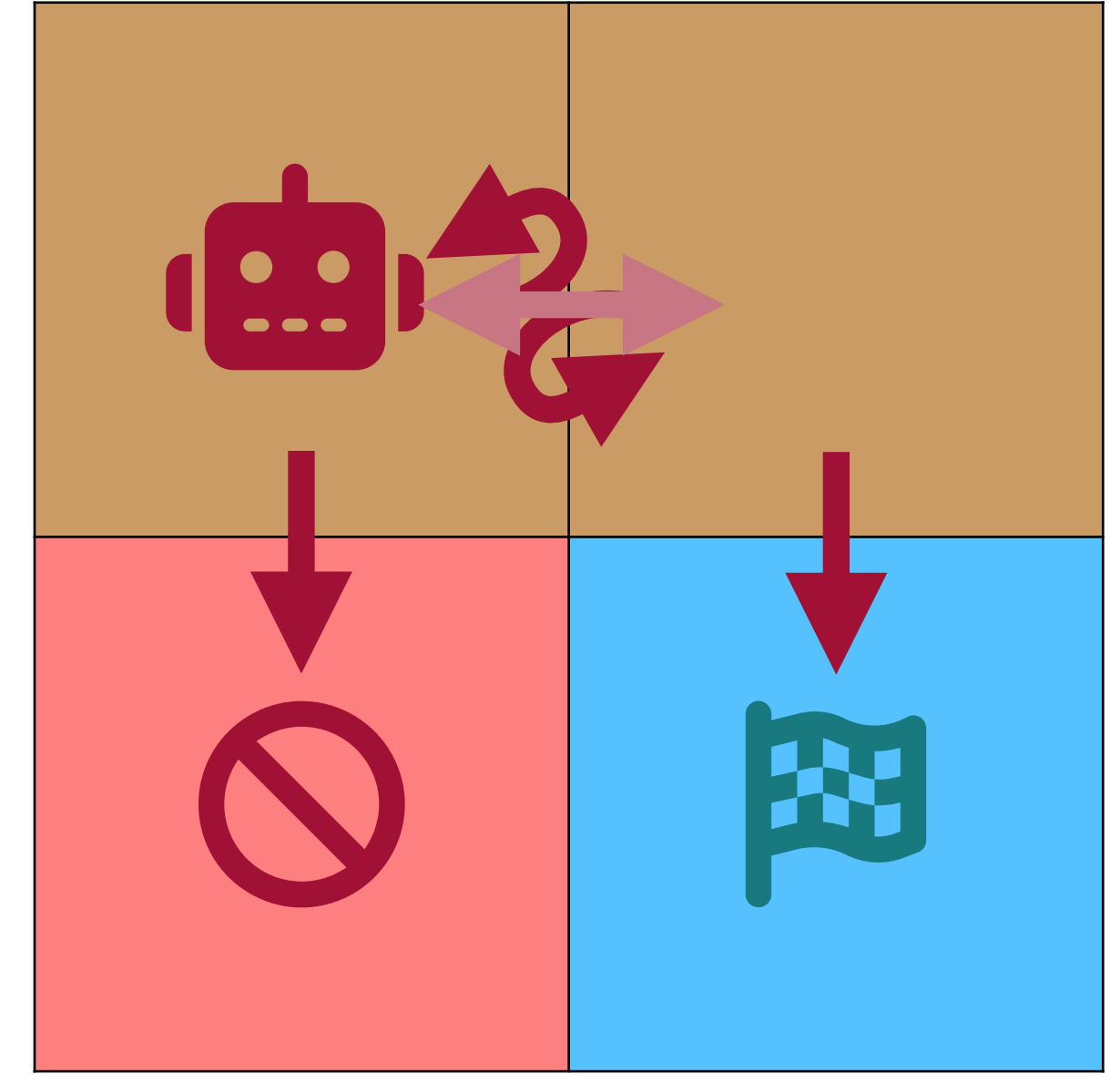
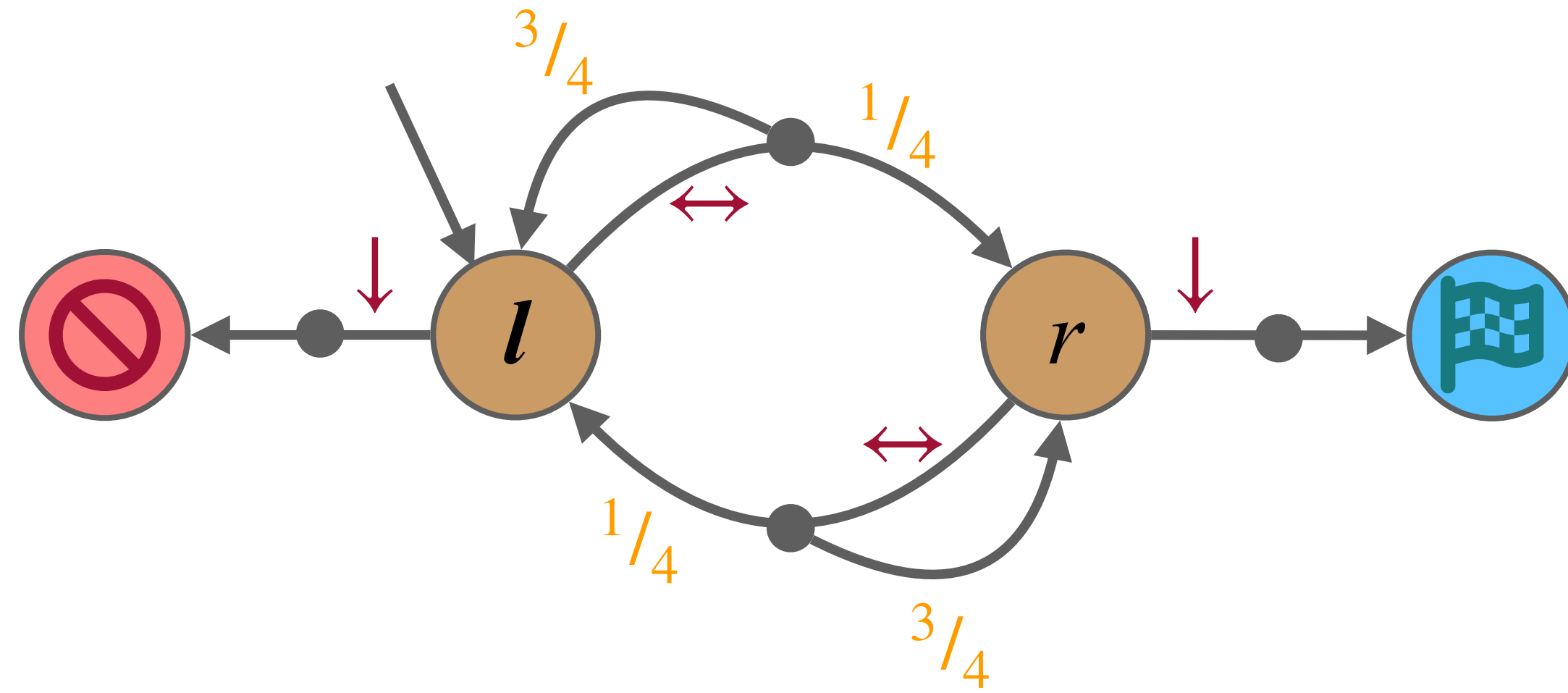
# Partially Observable MDPs

$\mathcal{P}$



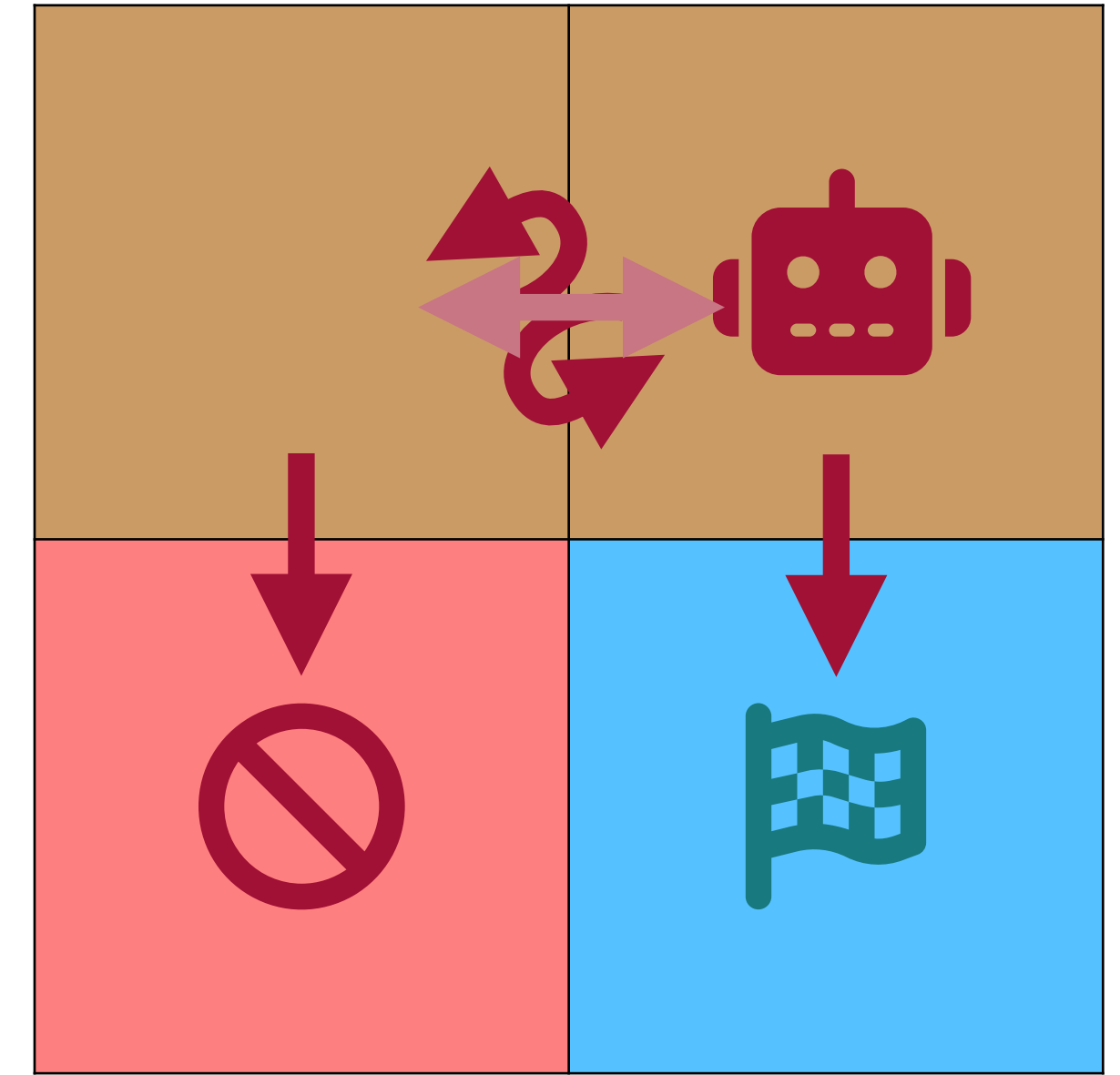
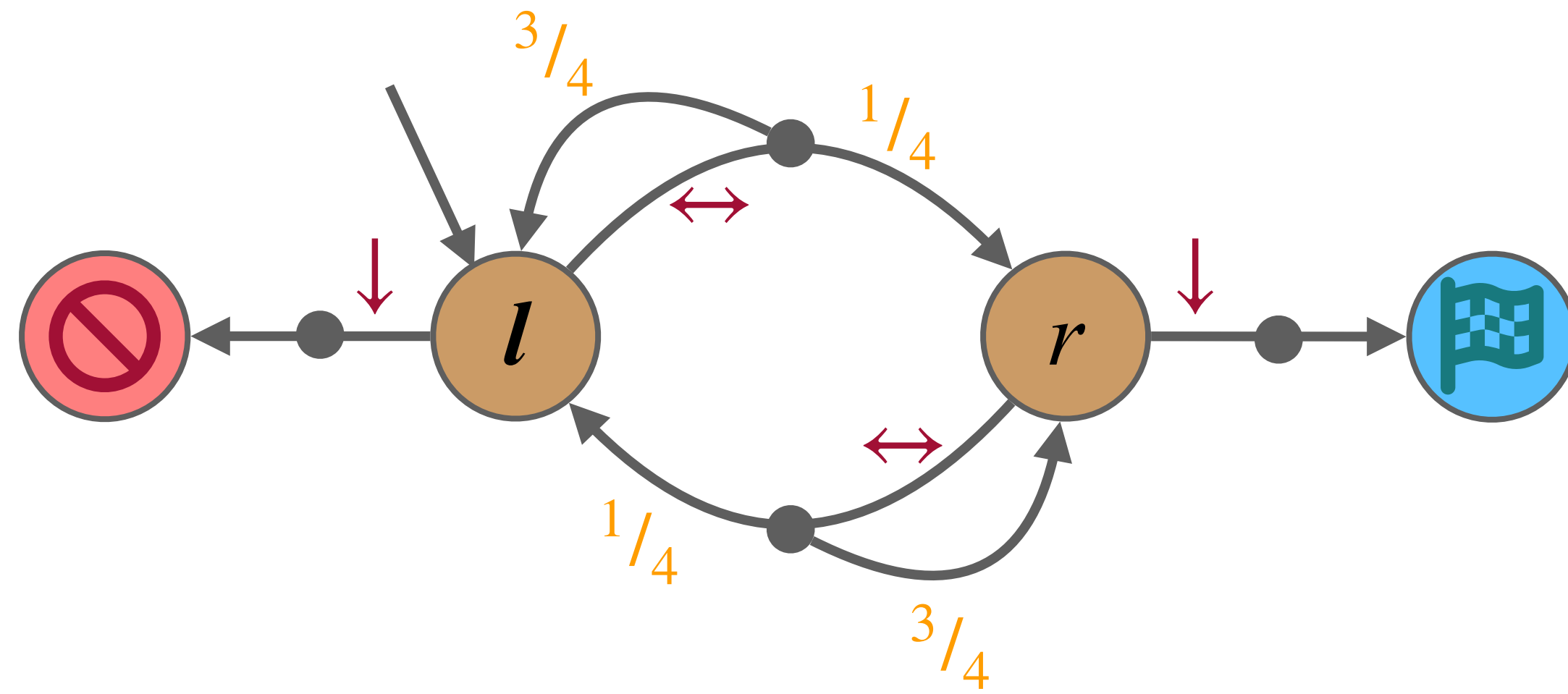
# Partially Observable MDPs

$\mathcal{P}$



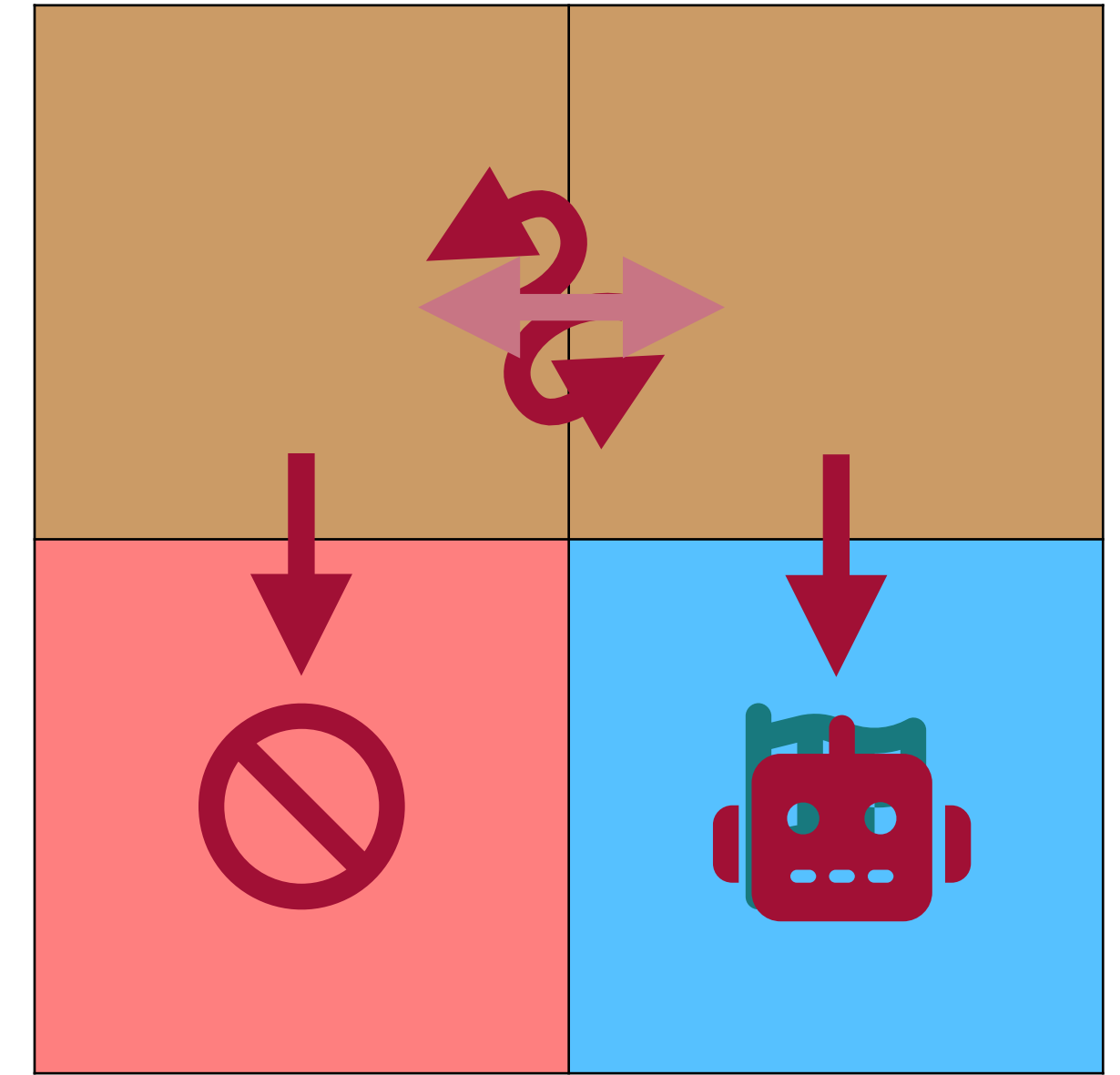
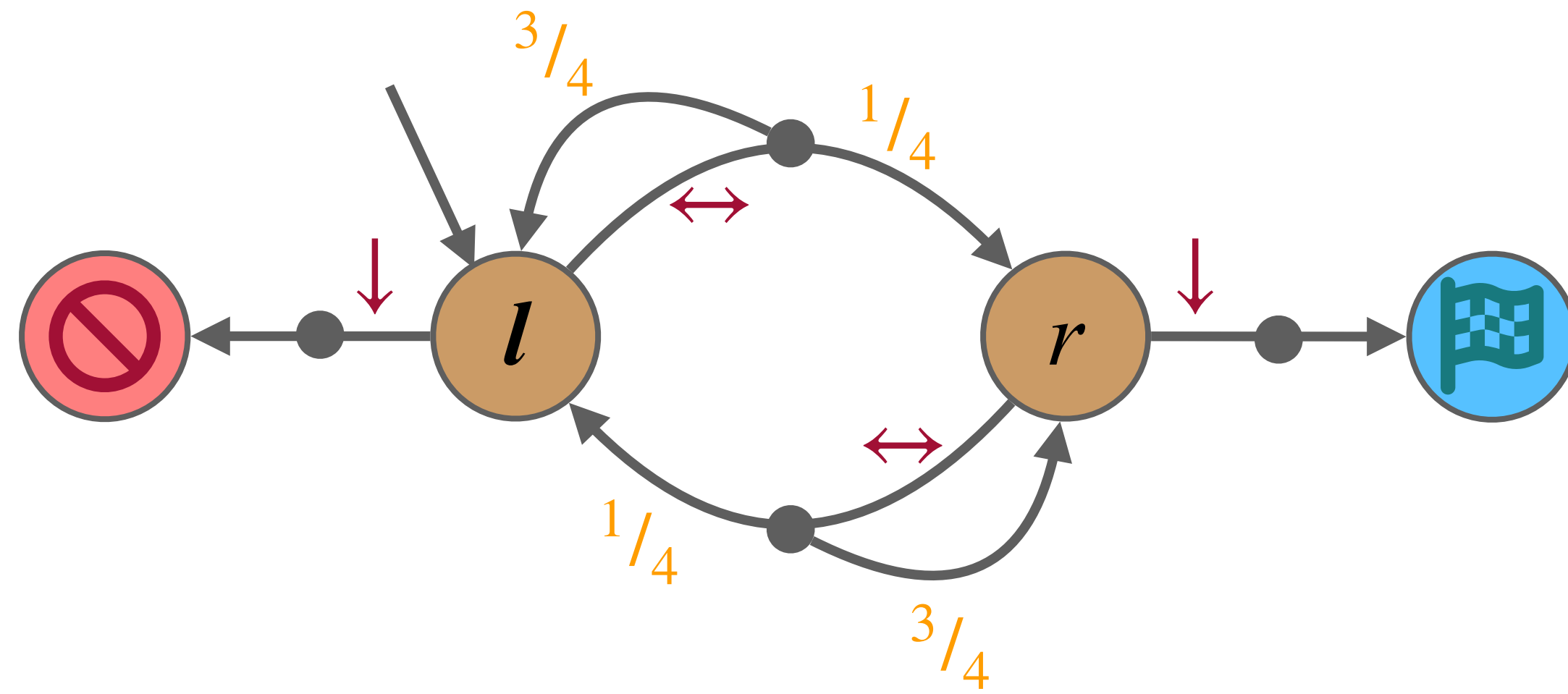
# Partially Observable MDPs

$\mathcal{P}$



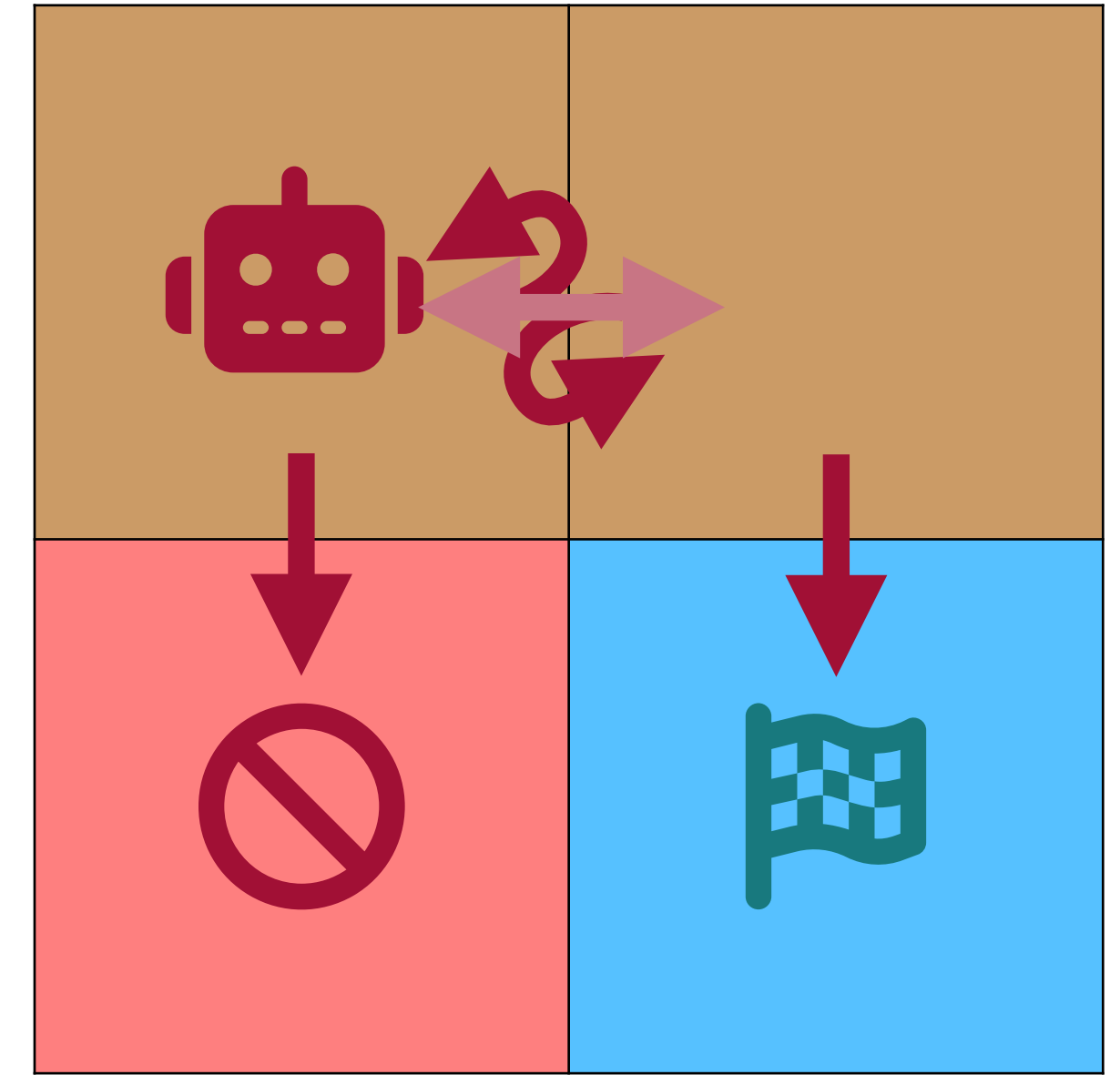
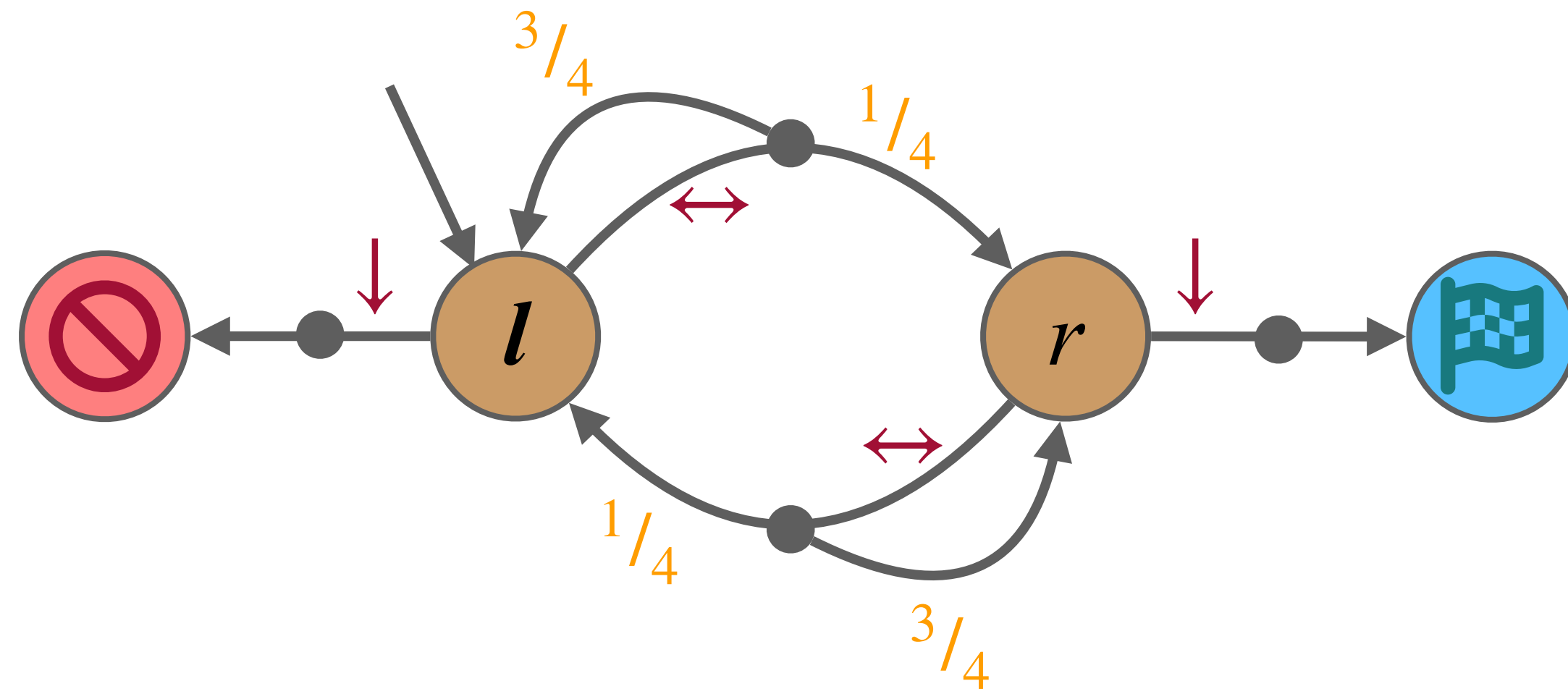
# Partially Observable MDPs

$\mathcal{P}$



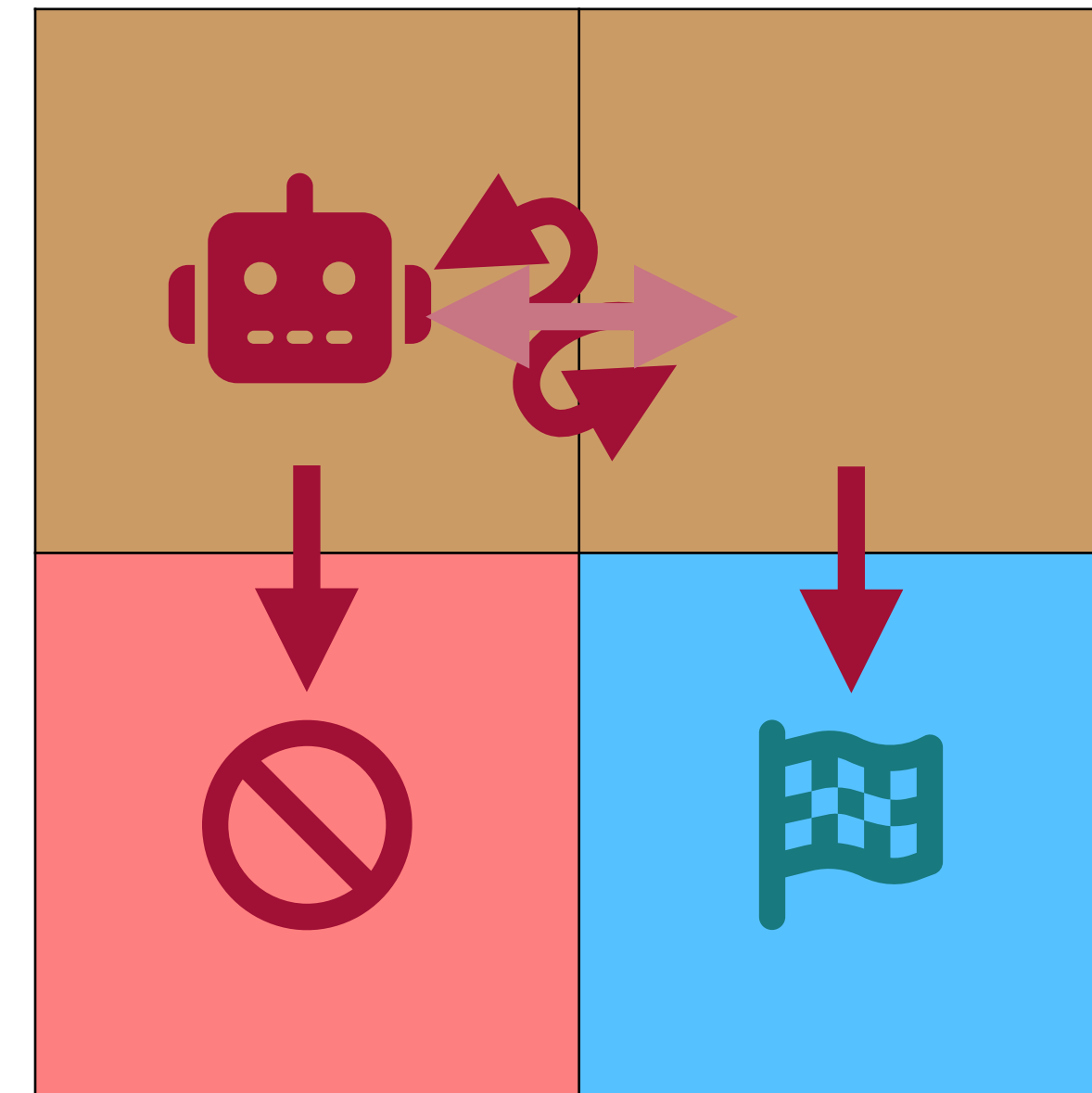
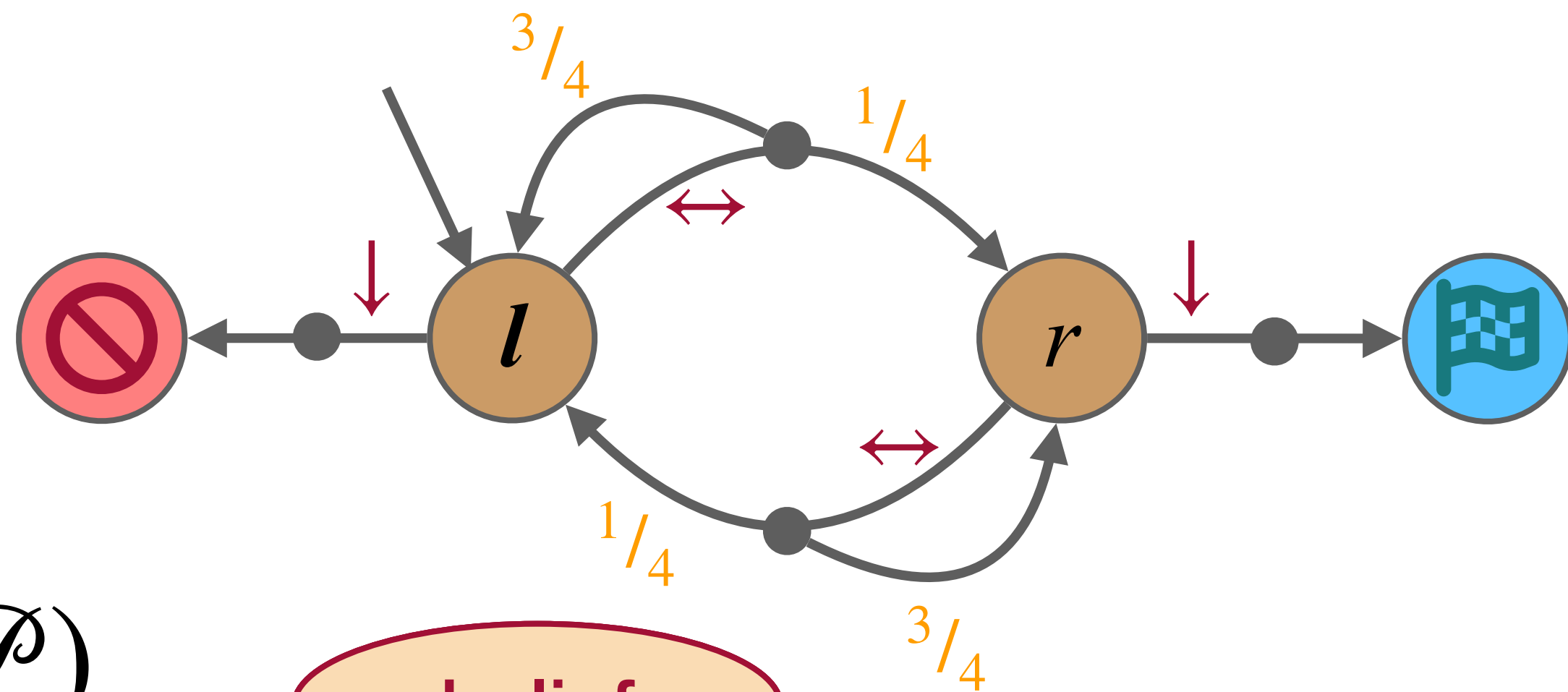
# Partially Observable MDPs

$\mathcal{P}$

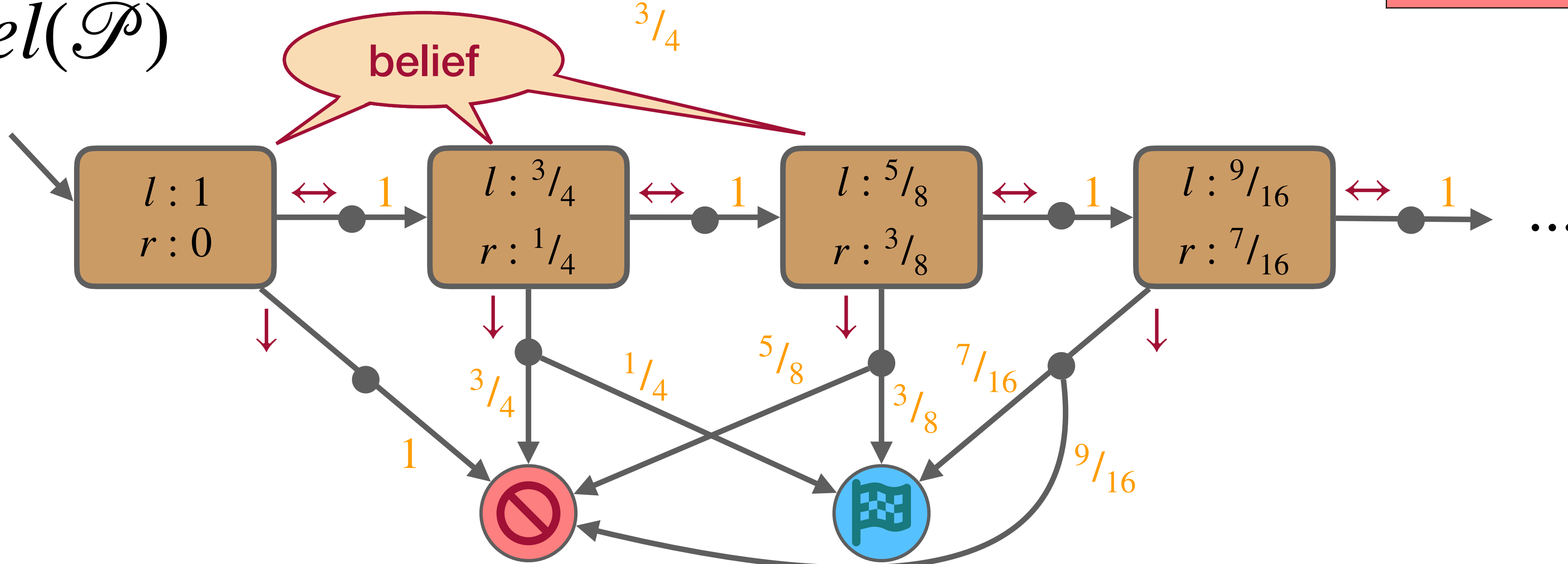


# Partially Observable MDPs

$\mathcal{P}$



$bel(\mathcal{P})$





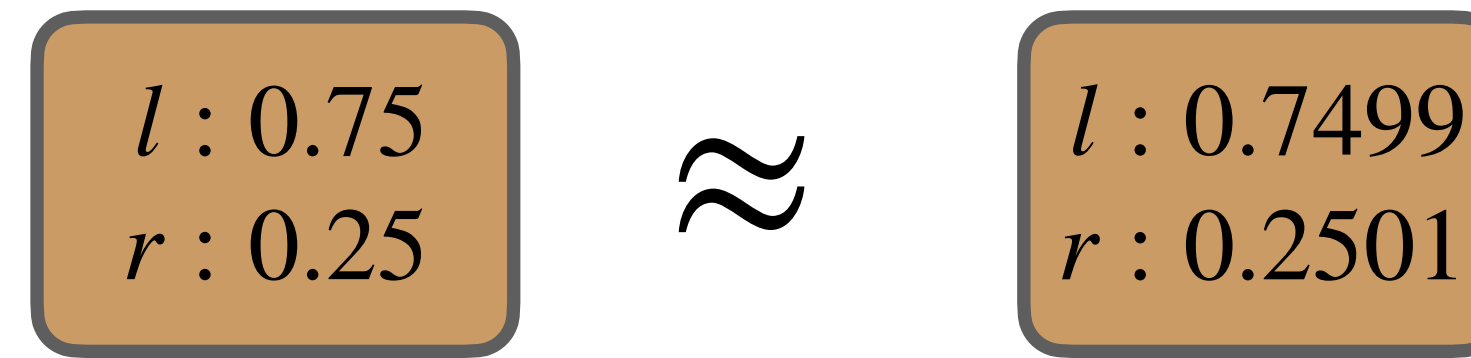
# Current Developments @i2

- **Cost-bounded reachability** for POMDPs
  - Probability to reach  within a given time and energy budget

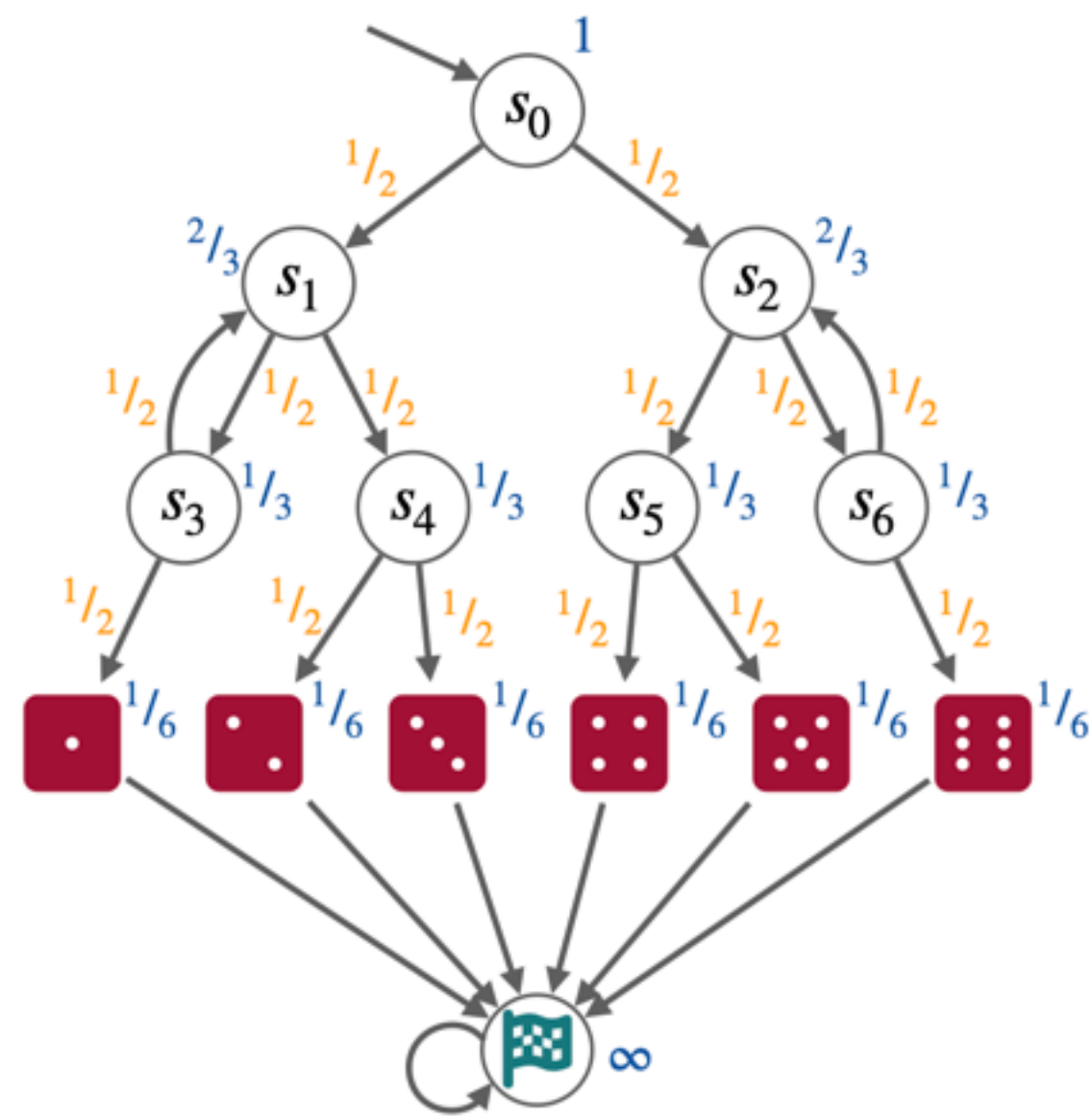
# Current Developments @i2

- **Cost-bounded reachability** for POMDPs
  - Probability to reach  within a given time and energy budget

- Investigate properties of **similar beliefs**



# Current Topics at the MOVES Group



**Expected Visiting Times**

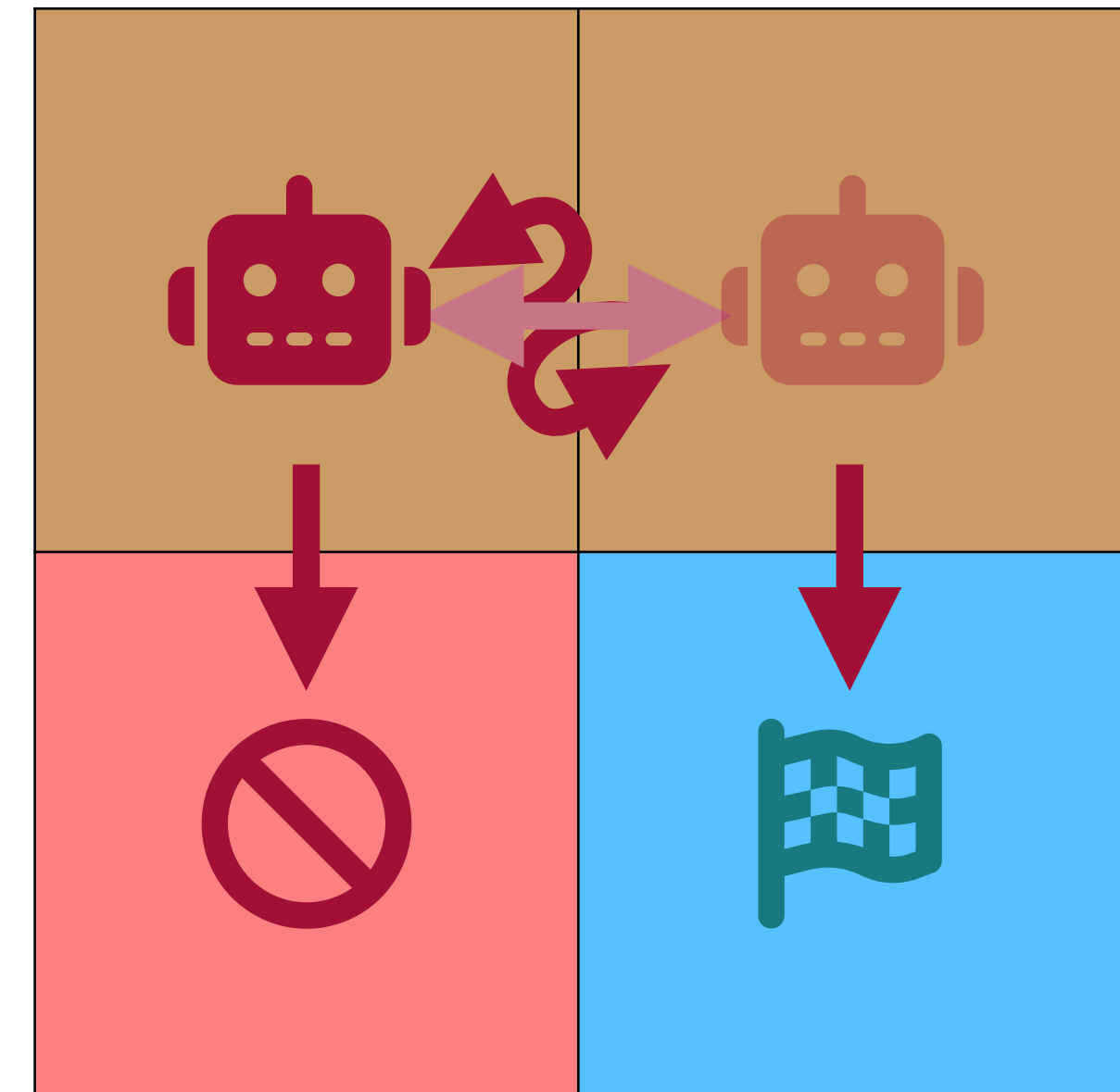
Upper bounds on minimal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\min}(x) \leq x$

Upper bounds on maximal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\max}(x) \leq x$

Lower bounds on minimal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\min}(x) \geq x$   
 $r \in \bar{\mathbb{N}}^S \quad \mathcal{D}^{\max}(r) \leq r$   
 $x(s) > 0 \implies r(s) < \infty$

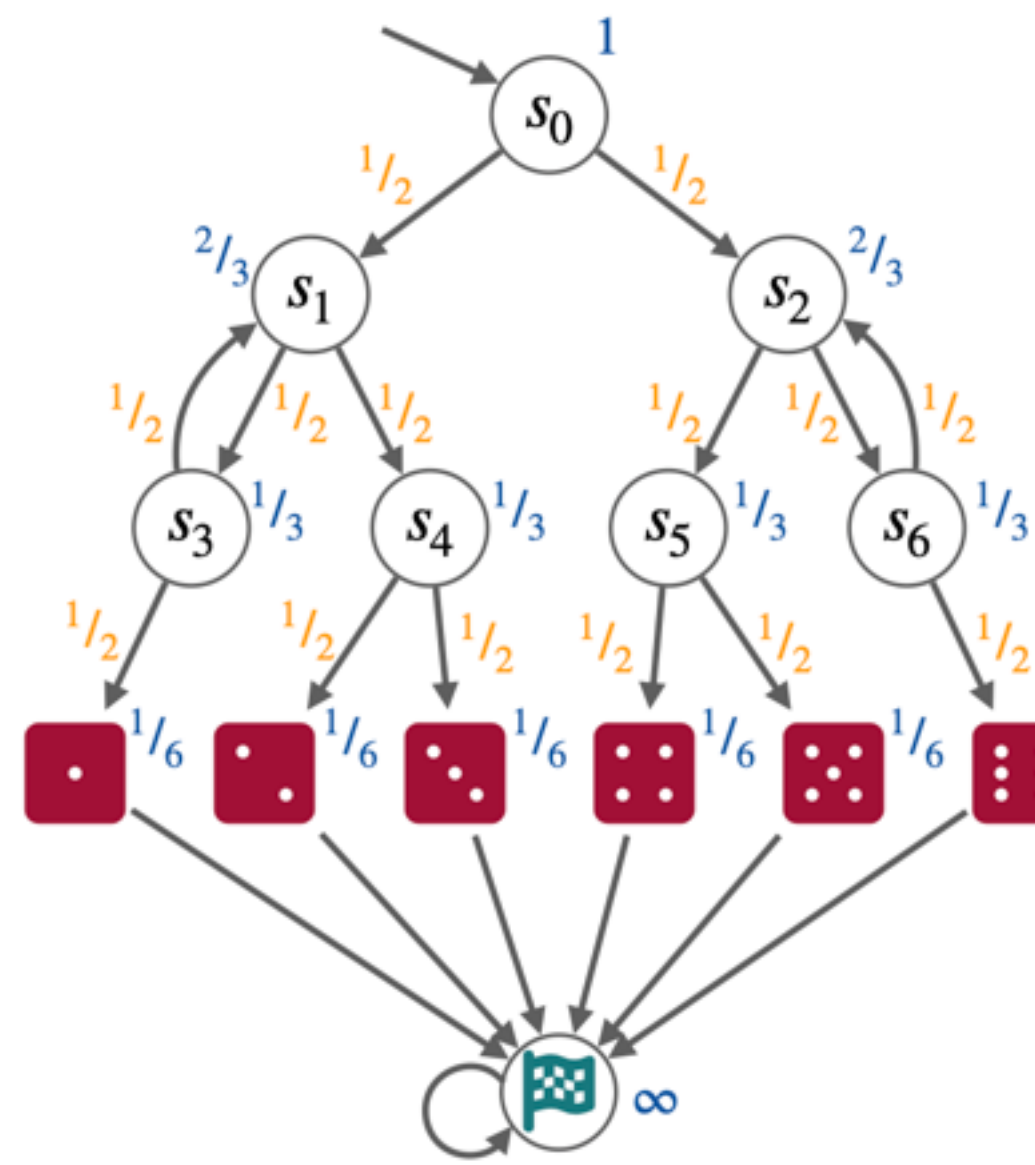
Lower bounds on maximal reachability  
 $x \in [0, 1]^S \quad \mathcal{B}^{\max}(x) \geq x$   
 $r \in \bar{\mathbb{N}}^S \quad \mathcal{D}_{x^\uparrow}^{\min}(r) \leq r$   
 $x(s) > 0 \implies r(s) < \infty$

**Certificates**

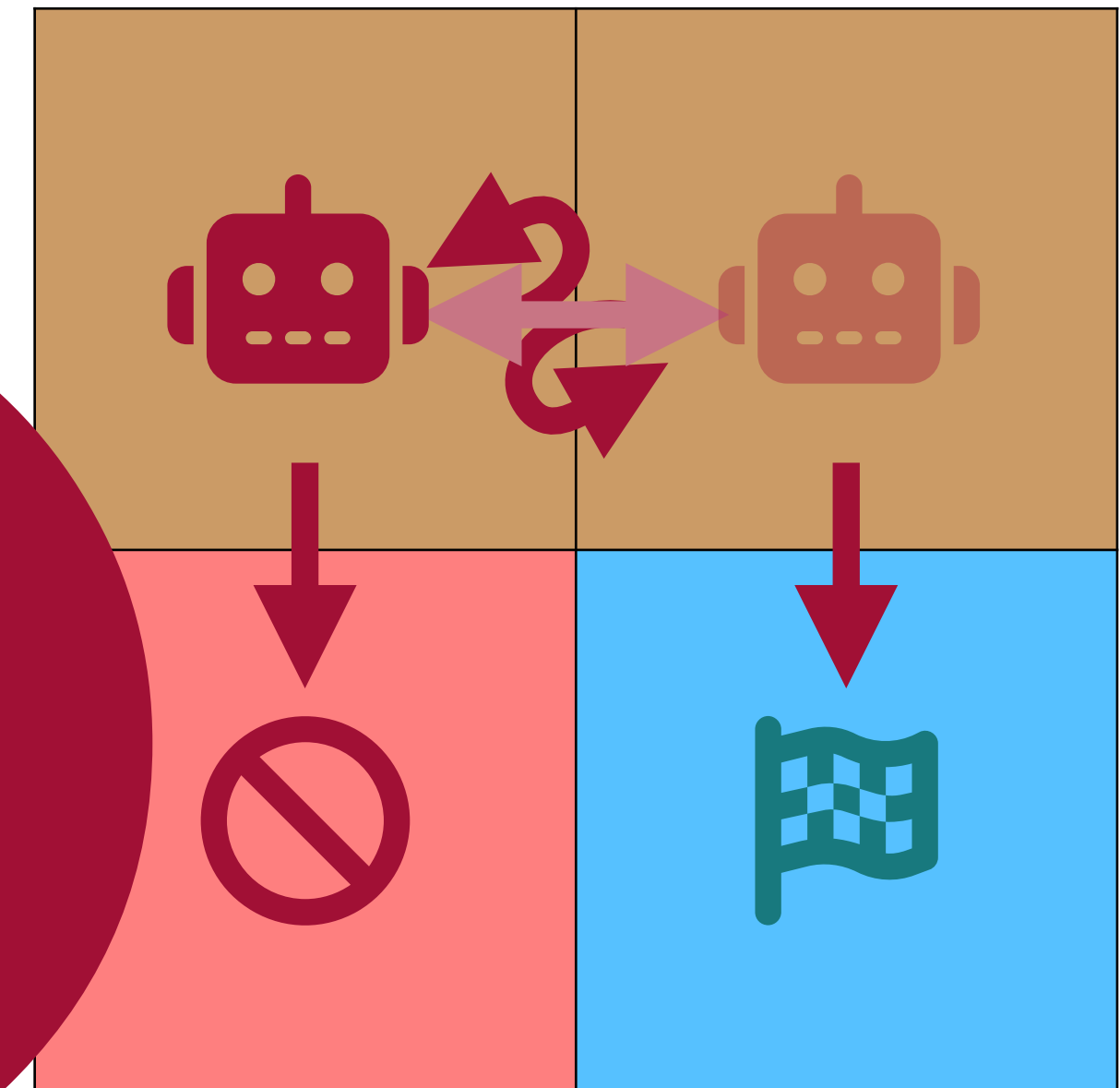


**Partially Observable MDPS**

# Current Topics at the MOVES Group

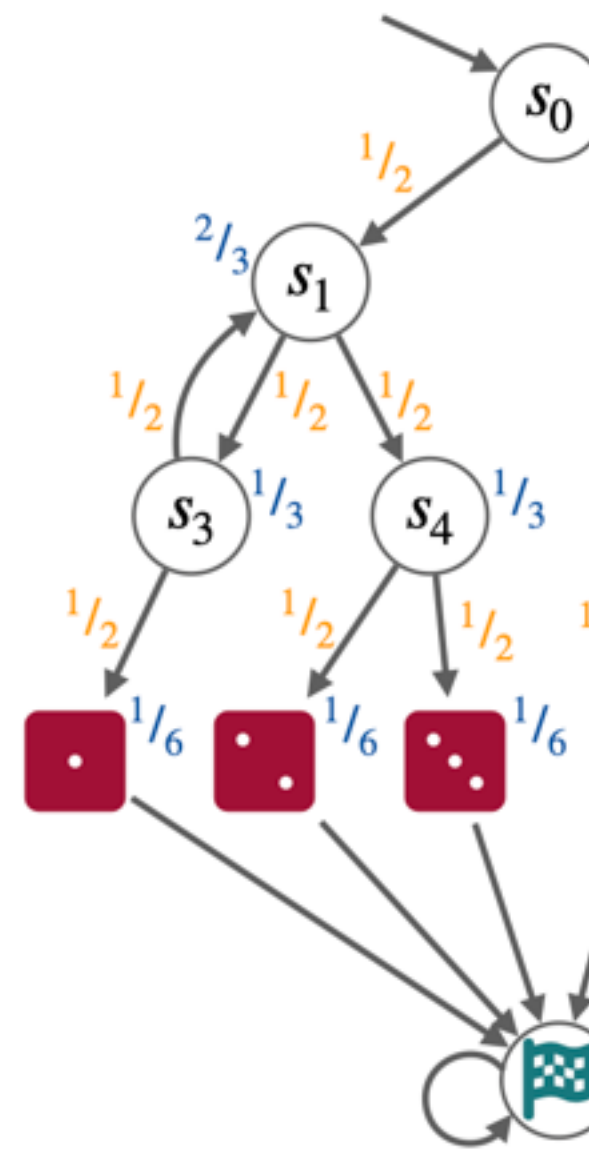


**Expected Visiting Times**






**Partially Observable MDPS**

# Current Topics at the MOVES Group



## Riding the Storm in a Probabilistic Model Checking Landscape\*

Christian Hensel, Sebastian Junges<sup>1</sup> ,  
Tim Quatmann<sup>2</sup> , and Matthias Volk<sup>3</sup> 

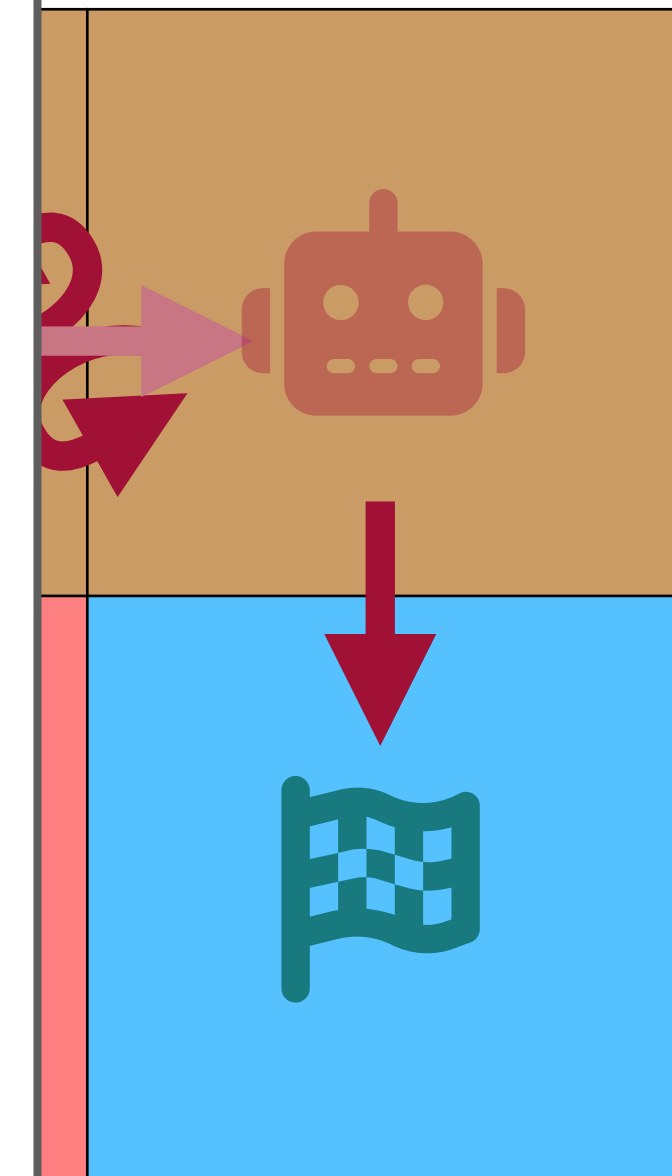
<sup>1</sup> Radboud University, Nijmegen, the Netherlands  
sebastian.junges@ru.nl

<sup>2</sup> RWTH Aachen University, Aachen, Germany

<sup>3</sup> Eindhoven University of Technology, Eindhoven, the Netherlands

Expect  
Visiting

**Abstract.** Probabilistic model checking is a formal verification technique to check whether stochastic models satisfy properties of interest. Along with a rich theory, the community has developed mature tool support, which in turn has been applied to a set of industrial case studies. This paper demonstrates various abilities of the probabilistic model checker Storm by a set of simple and more accessible examples.



tially  
ervable  
DPS