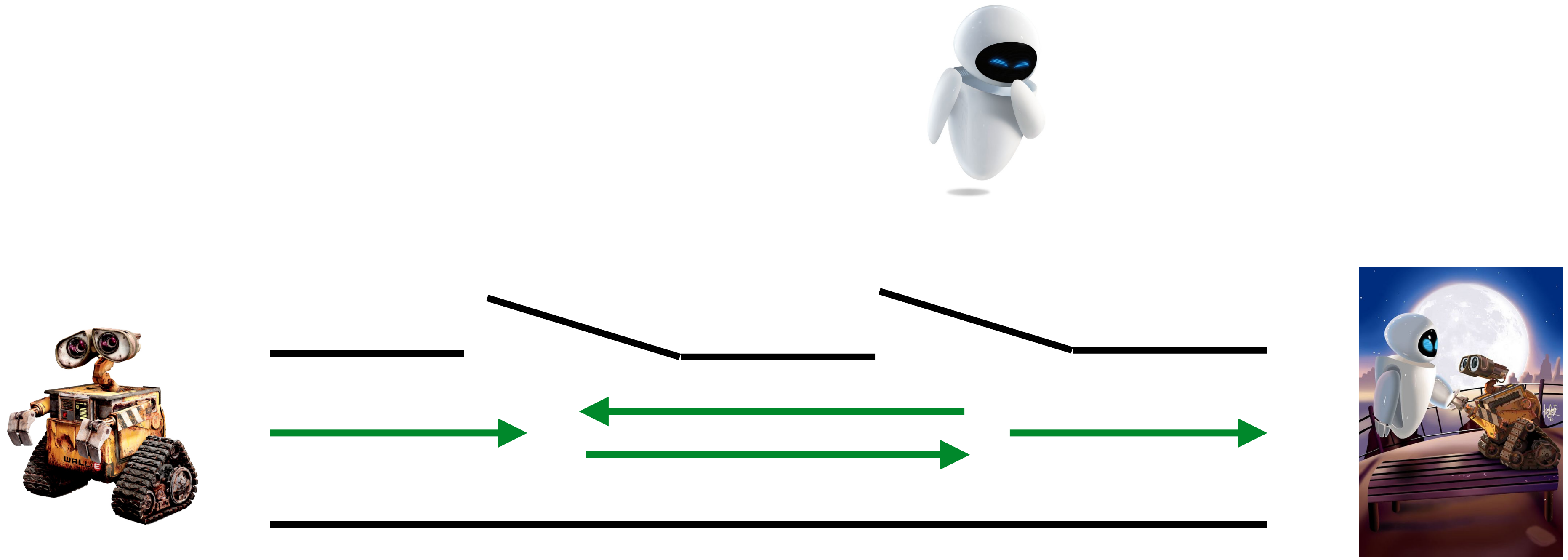
Tableaux for Policy Synthesis for MDPs with PCTL* Constraints

Peter Baumgartner, Sylvie Thiébaux, Felipe Trevizan

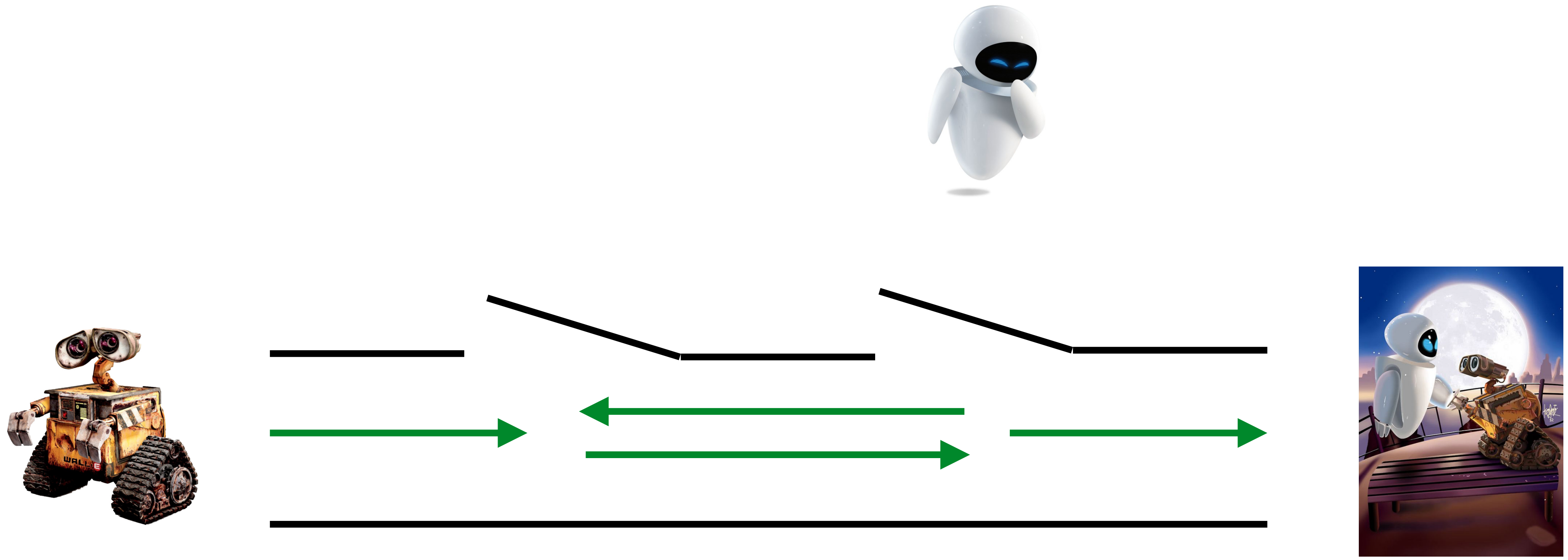
Data61/CSIRO and Research School of Computer Science, ANU
Australia

Markov Decision Processes (MDPs)



Actions: move left, move right, enter, get Eve, exit

Markov Decision Processes (MDPs)

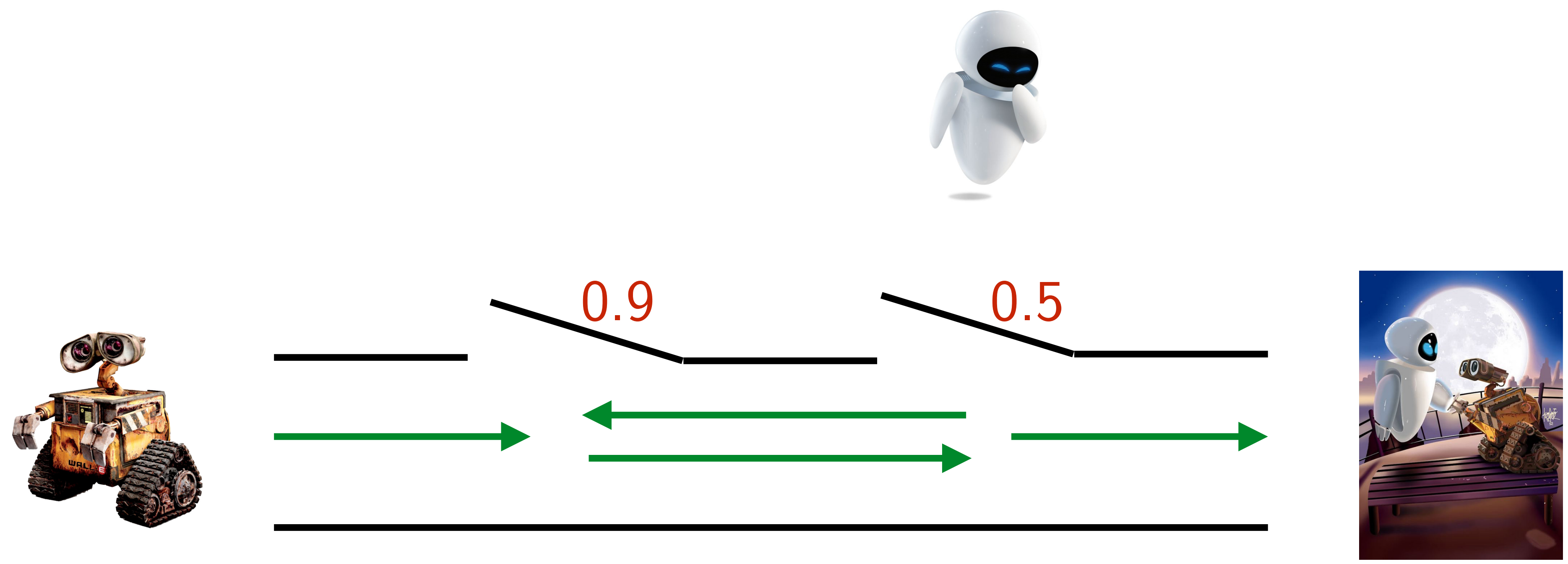


Nondeterministic action $\Longrightarrow$ stochastic environment response

Actions: move left, move right, enter, get Eve, exit

Environment: door possibly jams, location of Eve uncertain (10% - 90%)

Markov Decision Processes (MDPs)

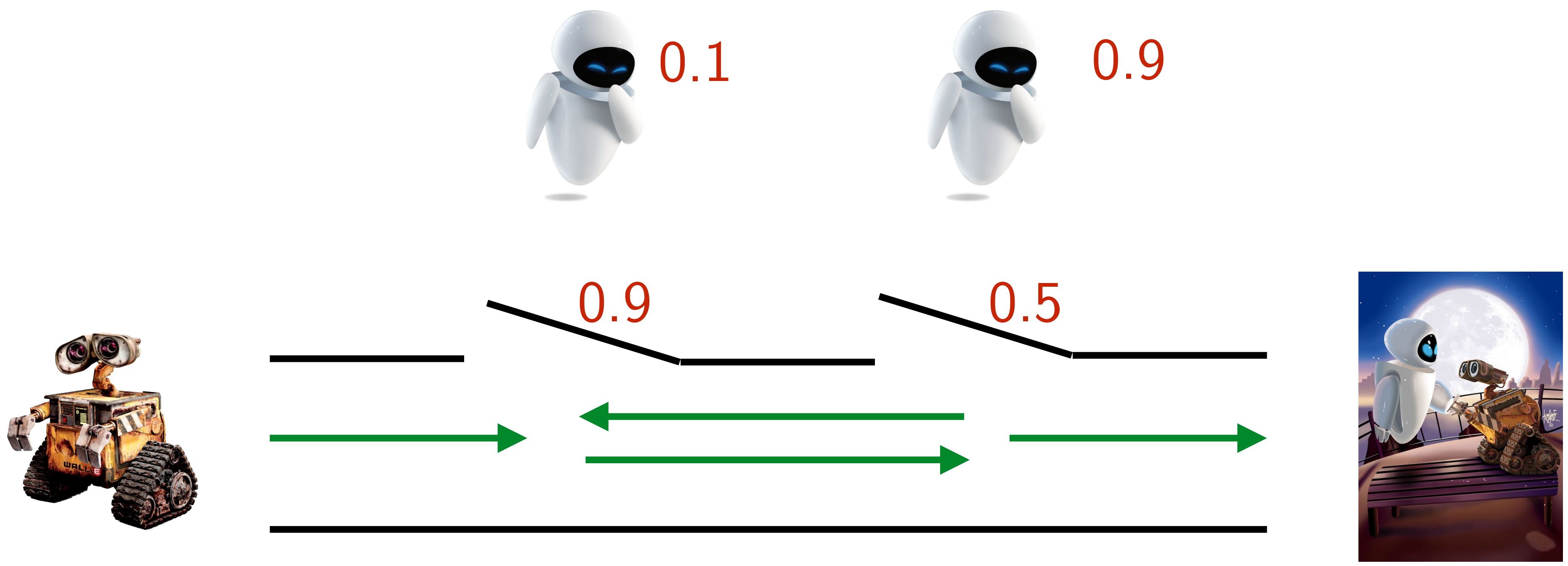


Nondeterministic action $\Longrightarrow$ stochastic environment response

Actions: move left, move right, enter, get Eve, exit

Environment: door possibly jams, location of Eve uncertain (10% - 90%)

Markov Decision Processes (MDPs)

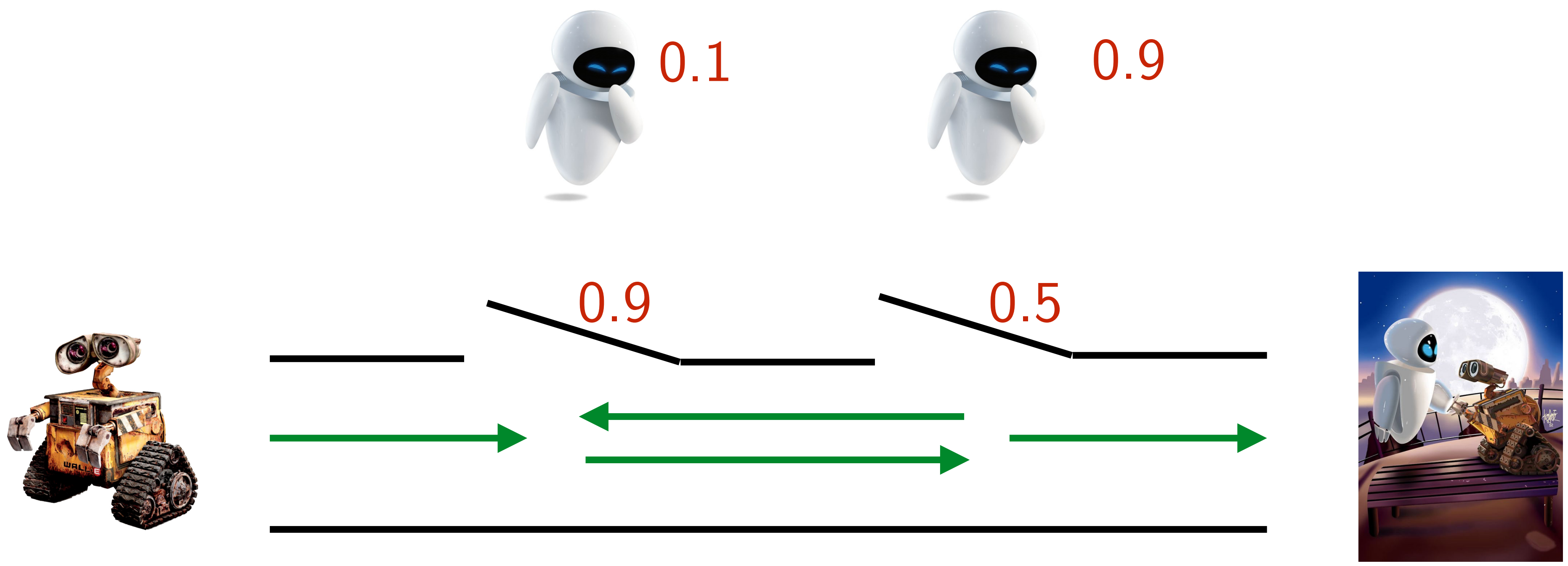


Nondeterministic action $\Longrightarrow$ stochastic environment response

Actions: move left, move right, enter, get Eve, exit

Environment: door possibly jams, location of Eve uncertain (10% - 90%)

Markov Decision Processes (MDPs)



Nondeterministic action $\Longrightarrow$ stochastic environment response

Actions: move left, move right, enter, get Eve, exit

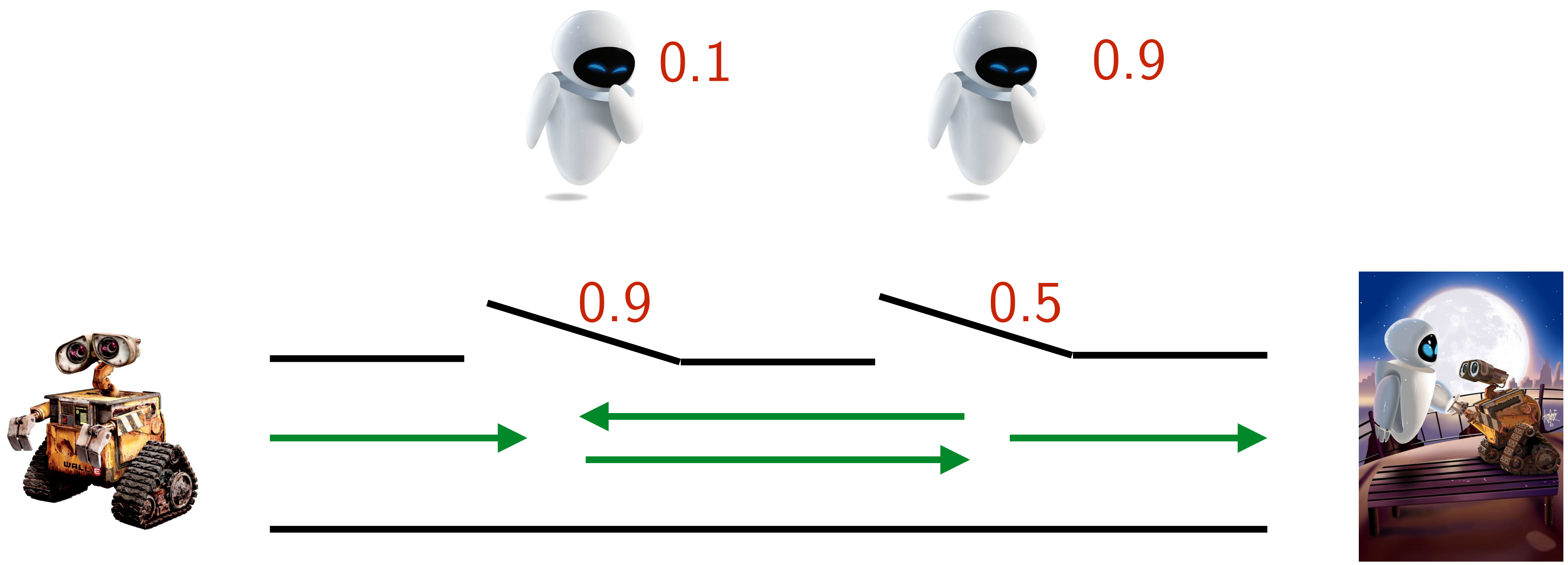
Environment: door possibly jams, location of Eve uncertain (10% - 90%)

Decision making:

What **action** to take in what **state** to achieve **objective**?

Objective: $\mathbf{P}_{>0.9}\ \mathbf{F}\ (\text{Eve} \wedge \mathbf{X}\ \mathbf{P}_{>0.8}\ \mathbf{F}\ \text{Done})$

Markov Decision Processes (MDPs)



Nondeterministic action $\Longrightarrow$ **stochastic environment response**

Actions: move left, move right, enter, get Eve, exit

Environment: door possibly jams, location of Eve uncertain (10% - 90%)

Decision making:

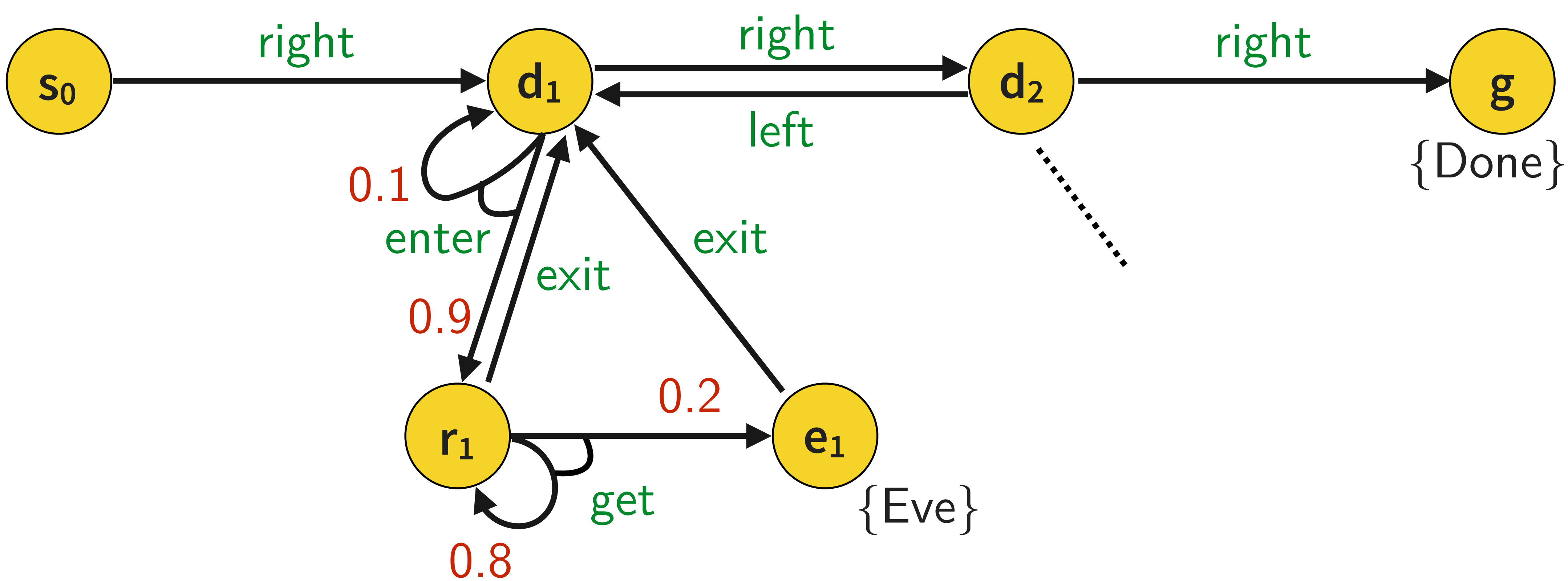
What **action** to take in what **state** to achieve **objective**?

Objective: $\mathbf{P}_{>0.9}\ \mathbf{F}\ (\text{Eve} \wedge \mathbf{X}\ \mathbf{P}_{>0.8}\ \mathbf{F}\ \text{Done})$

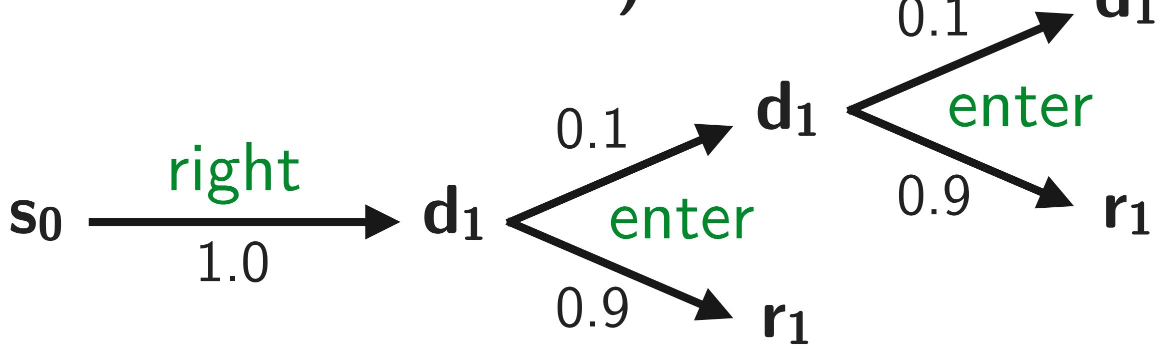
$\rightsquigarrow$ **MDP formalism**

MDPs, Execution Paths and Probabilities

Nondeterministic action $\Longrightarrow$ stochastic environment response

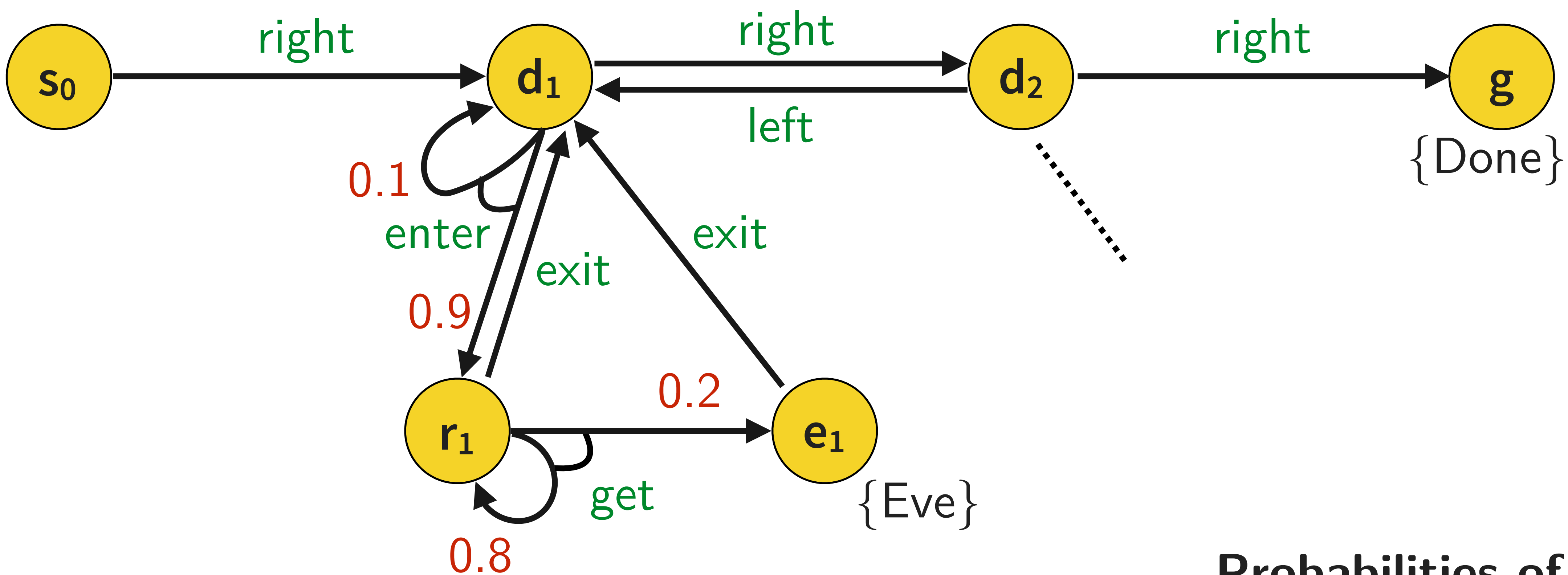


Paths (actions have been resolved)



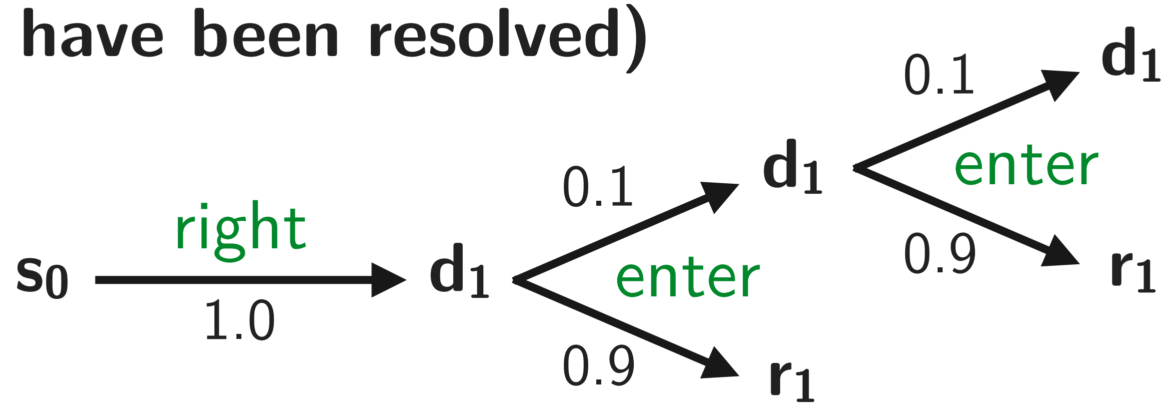
MDPs, Execution Paths and Probabilities

Nondeterministic action $\Longrightarrow$ stochastic environment response



Paths (actions have been resolved)

Probabilities of paths



0.01

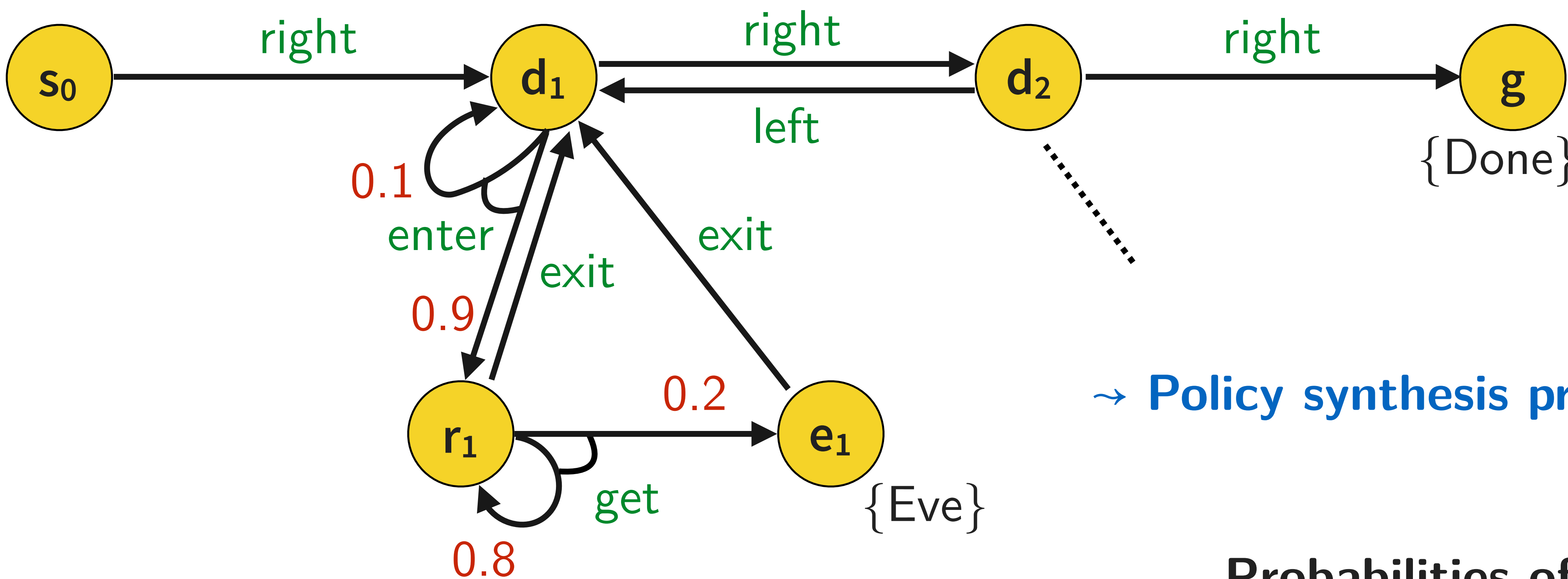
0.09

0.9 $(\Sigma = 1.0)$

"The probability of reaching $\mathbf{r_1}$ *after at most two enter steps is* 0.99*"*

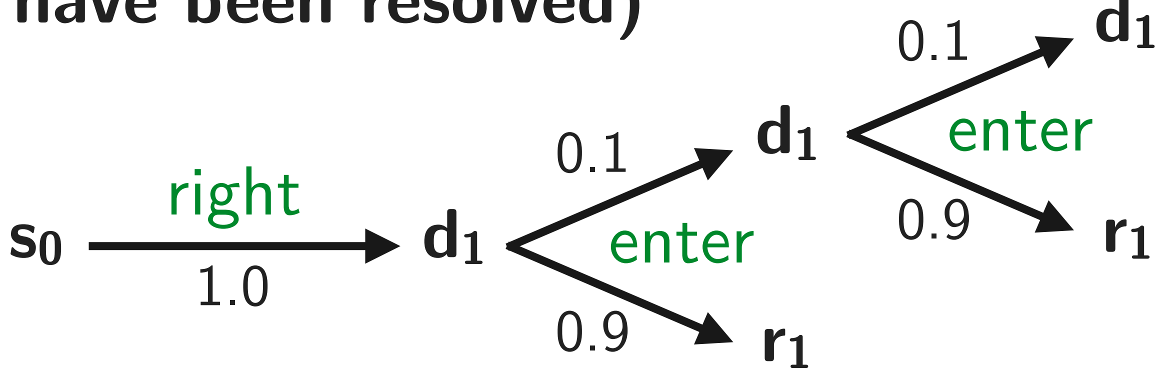
MDPs, Execution Paths and Probabilities

Nondeterministic action $\Longrightarrow$ stochastic environment response



$\rightsquigarrow$ **Policy synthesis problem**

Paths (actions have been resolved)



Probabilities of paths

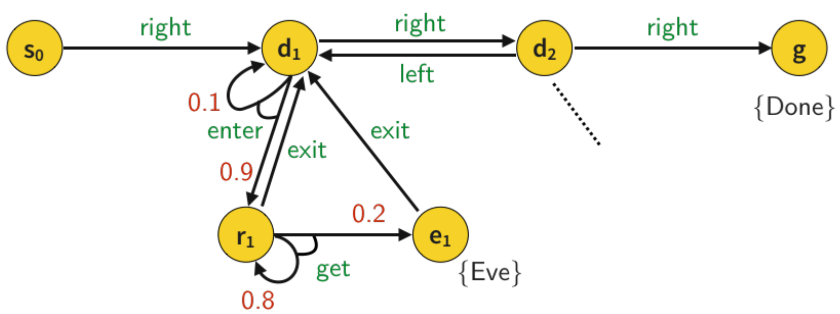
0.01

0.09

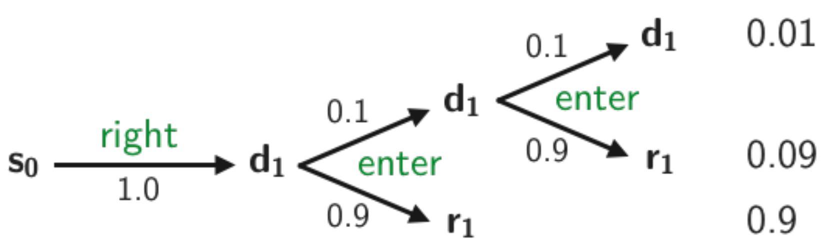
0.9 $(\Sigma = 1.0)$

"The probability of reaching $\mathbf{r_1}$ *after at most two* enter *steps is* 0.99*"*

Policy Synthesis Problem



- **Static**: MDP



- **Dynamics**: paths and probabilities of paths
- Induced by actions chosen

$s_0 \models \mathbf{P}_{>0.9}\ \mathbf{F}\ (\mathrm{Eve} \wedge \mathbf{X}\ \mathbf{P}_{>0.8}\ \mathbf{F}\ \mathrm{Done})$

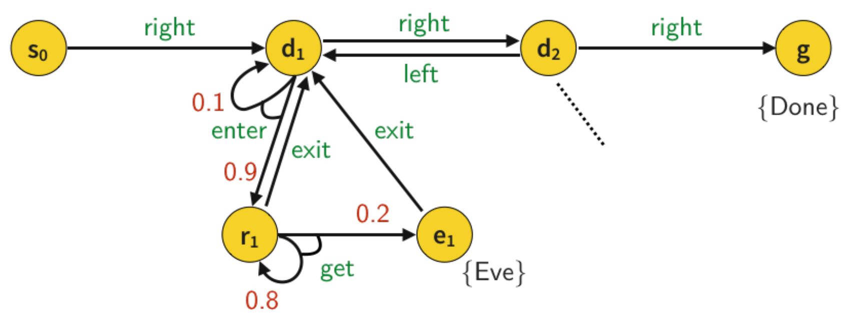
- **Logic**: specification of target property (see below)
- Constraints on probabilities of these paths

Policy synthesis problem

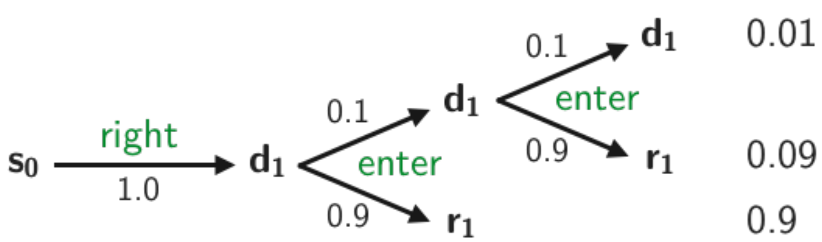
Policy σ: what actions to chose in what state

Synthesis problem: determine σ such that target property is satisfied

Policy Synthesis Problem



- **Static**: MDP



- **Dynamics**: paths and probabilities of paths
- Induced by actions chosen

$s_0 \models \mathbf{P}_{>0.9}\ \mathbf{F}\ (\text{Eve} \wedge \mathbf{X}\ \mathbf{P}_{>0.8}\ \mathbf{F}\ \text{Done})$

- **Logic**: specification of target property (see below)
- Constraints on probabilities of these paths

Policy synthesis problem

Policy σ: what actions to chose in what state → **Different kinds of policies**

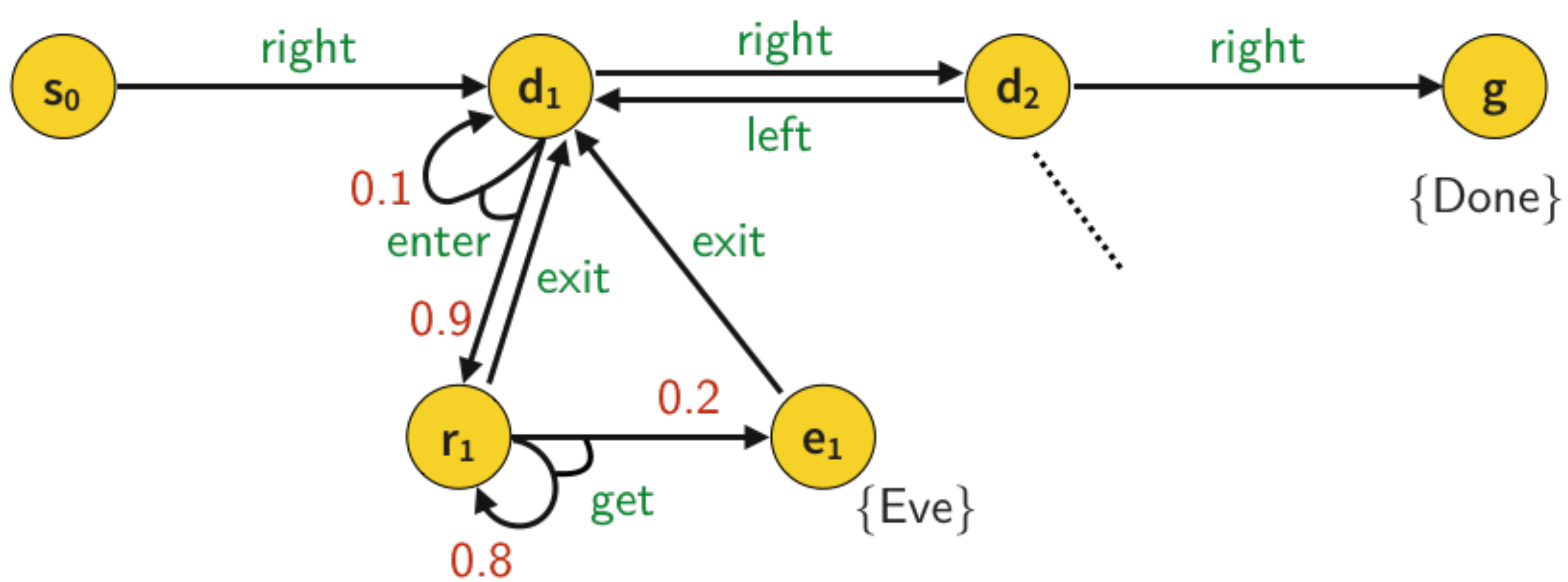
Synthesis problem: determine σ such that target property is satisfied

Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\ \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case M: History-independent policy

Attempt 1



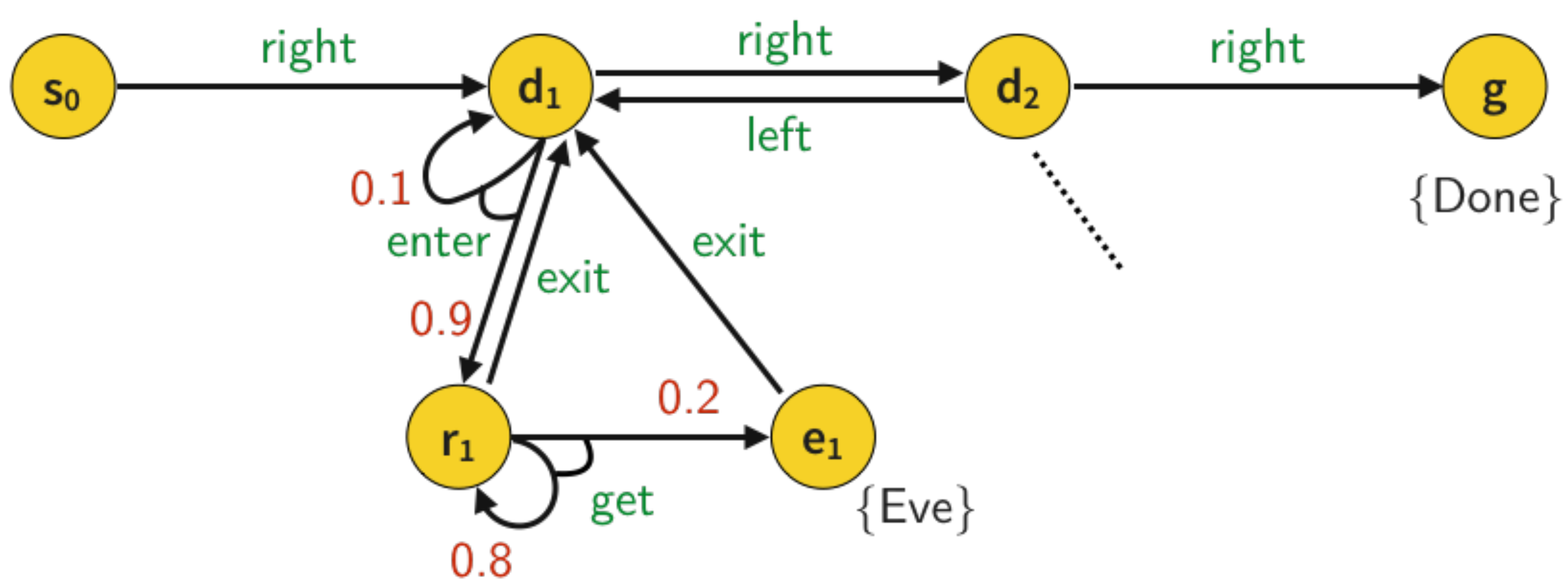
Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\ \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case M: History-independent policy

Attempt 1

$\mathbf{s_0}$: right



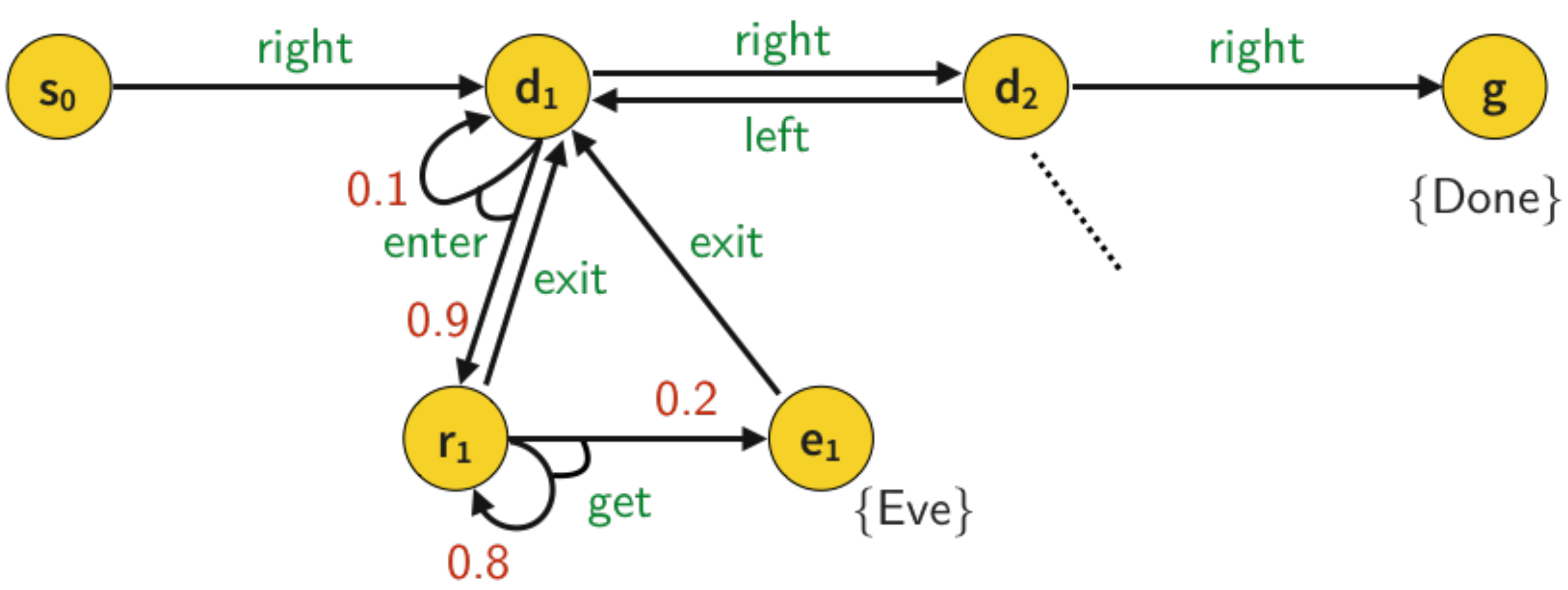
Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\ \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case M: History-independent policy

Attempt 1

$\mathbf{s_0}$: right $\mathbf{d_1}$: enter



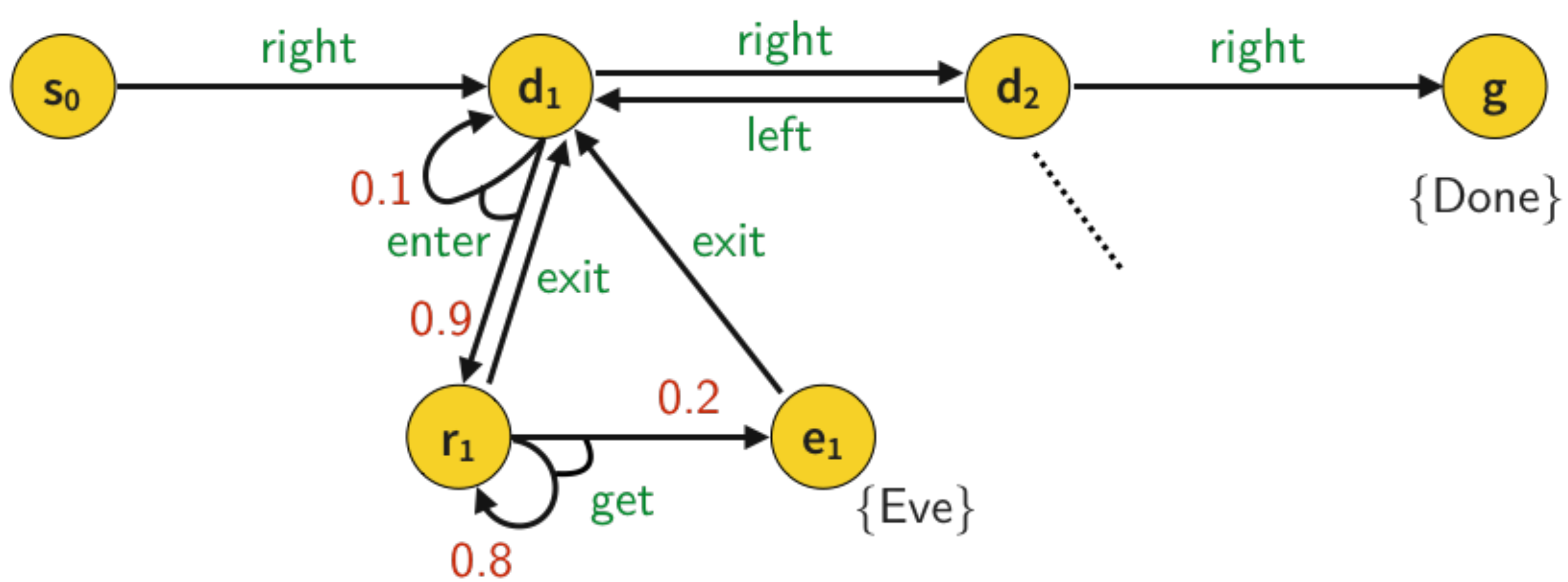
Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \vDash \mathbf{P}_{>0}\ \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case M: History-independent policy

Attempt 1

$\mathbf{s_0}$: right $\quad$ $\mathbf{d_1}$: enter $\quad$ $\mathbf{r_1}$: get



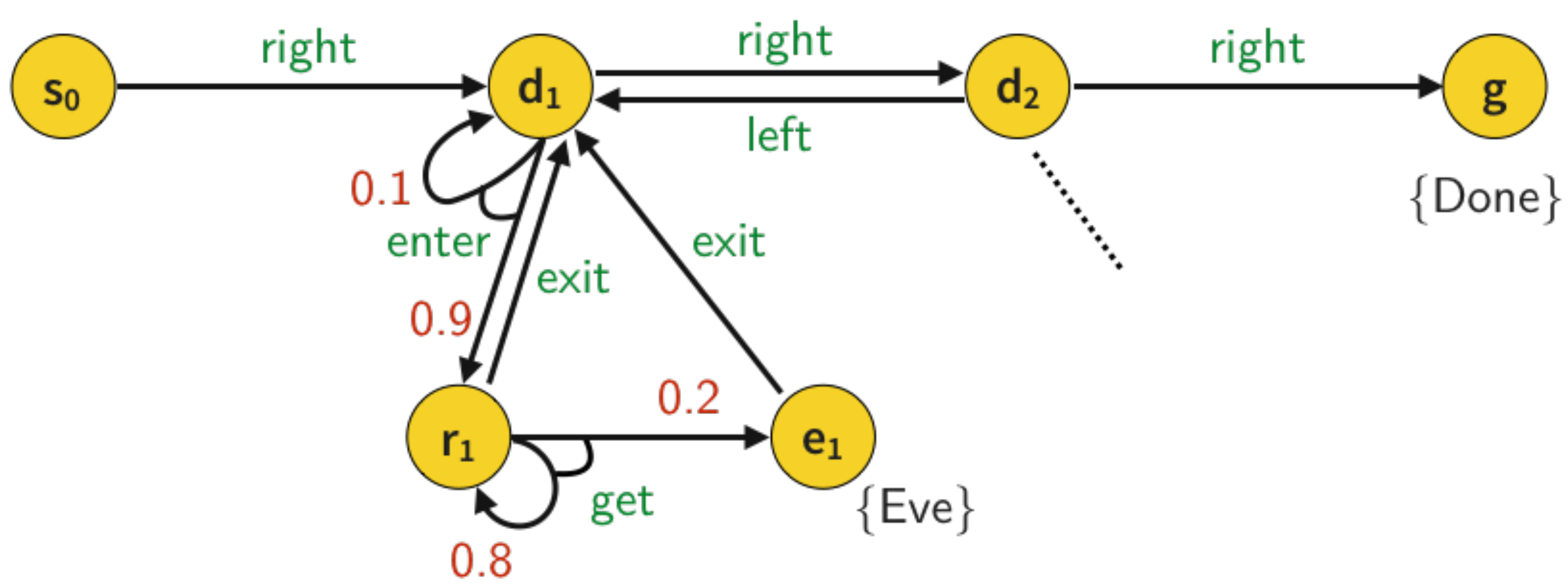
Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\ \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case M: History-independent policy

Attempt 1

$\mathbf{s_0}$: right $\quad$ $\mathbf{d_1}$: enter $\quad$ $\mathbf{r_1}$: get $\quad$ $\mathbf{e_1}$: exit



Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\ \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

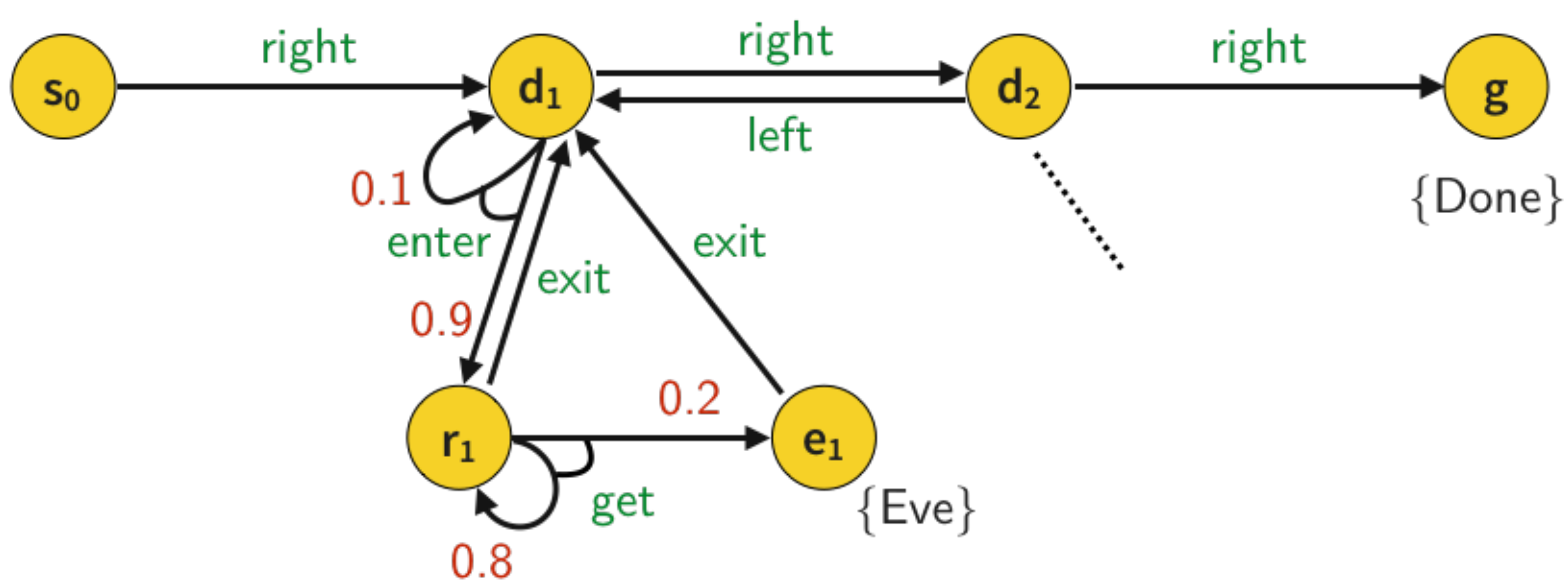
Case M: History-independent policy

Attempt 1

$\mathbf{s_0}$: right $\quad$ $\mathbf{d_1}$: enter $\quad$ $\mathbf{r_1}$: get $\quad$ $\mathbf{e_1}$: exit

✓ eventually Eve

✗ never Done



Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \vDash \mathbf{P}_{>0}\ \mathbf{F}\ (\mathrm{Eve} \wedge \mathbf{F}\ \mathrm{Done})$

Case M: History-independent policy

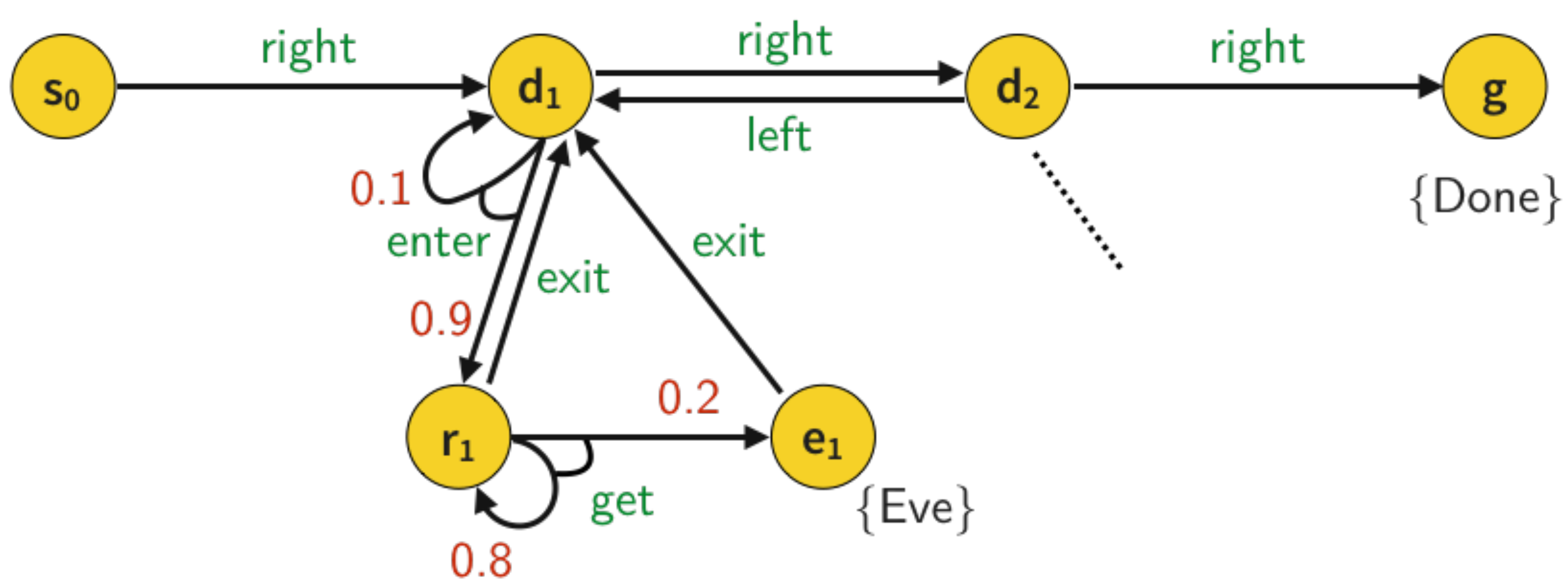
Attempt 1

$\mathbf{s_0}$: right $\mathbf{d_1}$: enter $\mathbf{r_1}$: get $\mathbf{e_1}$: exit

✓ eventually Eve

✗ never Done

Attempt 2



Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \vDash \mathbf{P}_{>0}\ \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case M: History-independent policy

Attempt 1

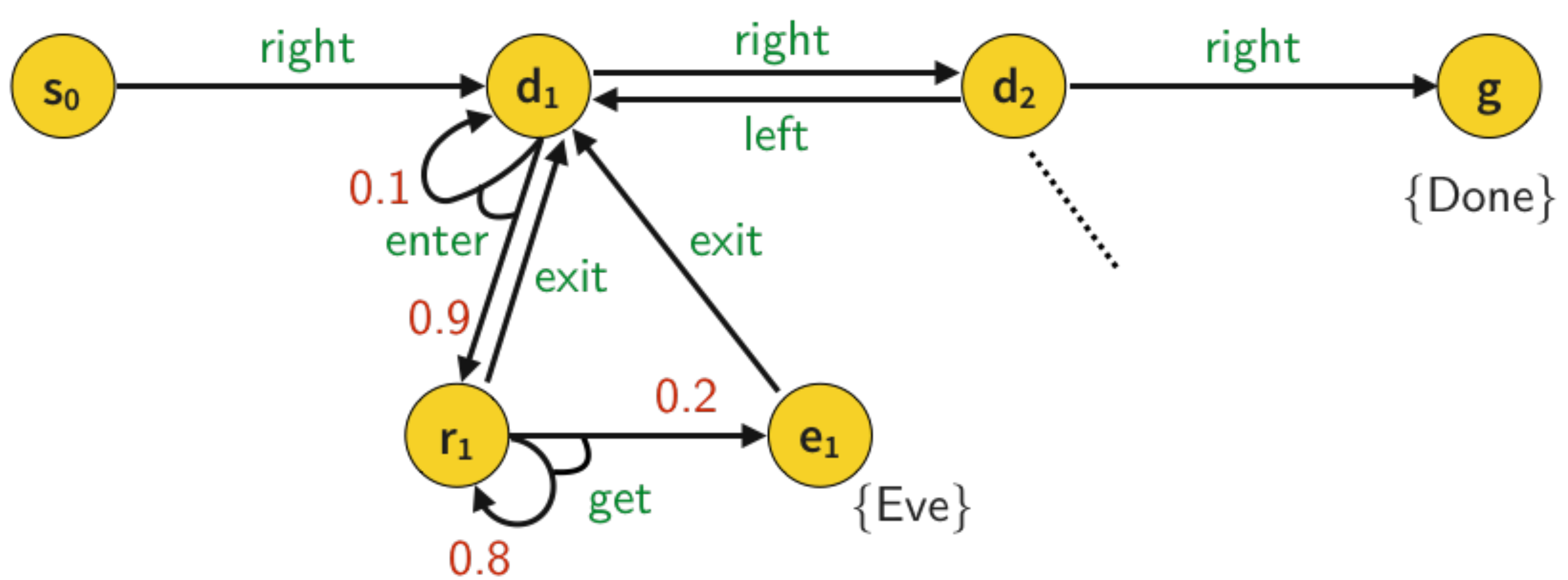
$\mathbf{s_0}$: right $\mathbf{d_1}$: enter $\mathbf{r_1}$: get $\mathbf{e_1}$: exit

✓ eventually Eve

✗ never Done

Attempt 2

$\mathbf{s_0}$: right



Policies - History Dependance and Randomization

Target property: $s_0 \models \mathbf{P}_{>0}\ \mathbf{F}\ (\mathrm{Eve} \wedge \mathbf{F}\ \mathrm{Done})$

Case M: History-independent policy

Attempt 1

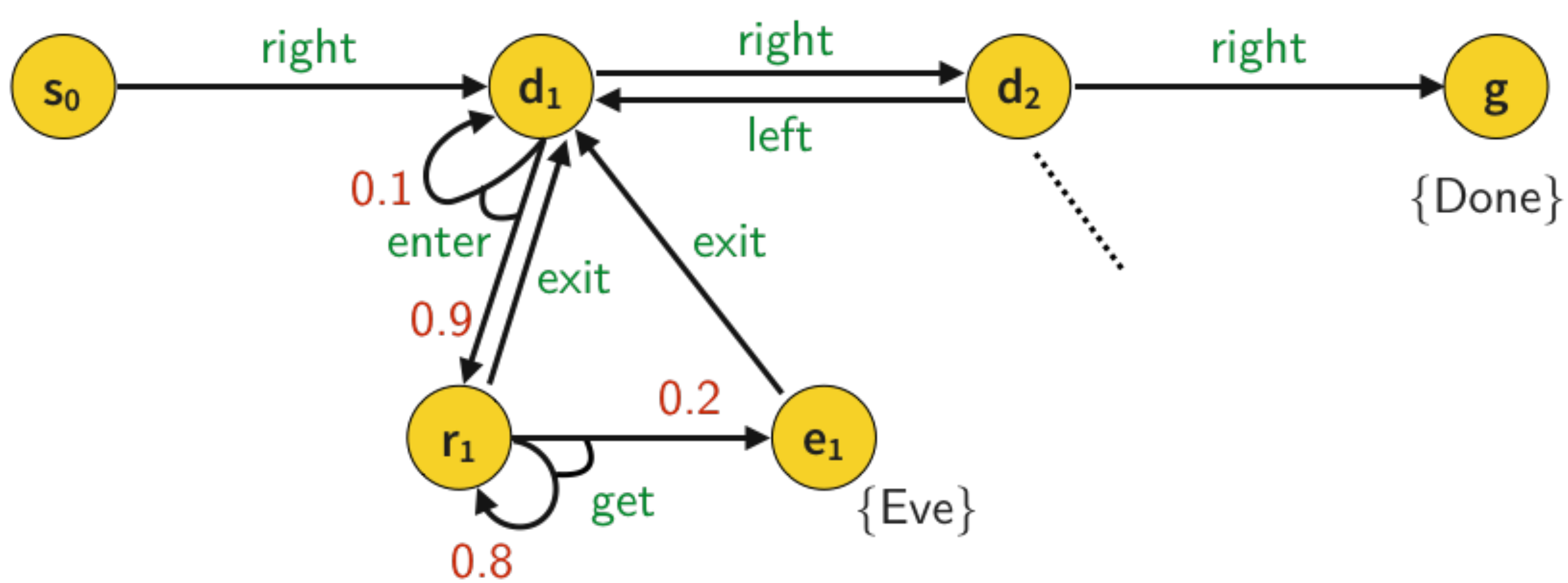
$\mathbf{s_0}$: right $\mathbf{d_1}$: enter $\mathbf{r_1}$: get $\mathbf{e_1}$: exit

✓ eventually Eve

✗ never Done

Attempt 2

$\mathbf{s_0}$: right $\mathbf{d_1}$: right



Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\ \mathbf{F}\ (\mathsf{Eve} \wedge \mathbf{F}\ \mathsf{Done})$

Case M: History-independent policy

Attempt 1

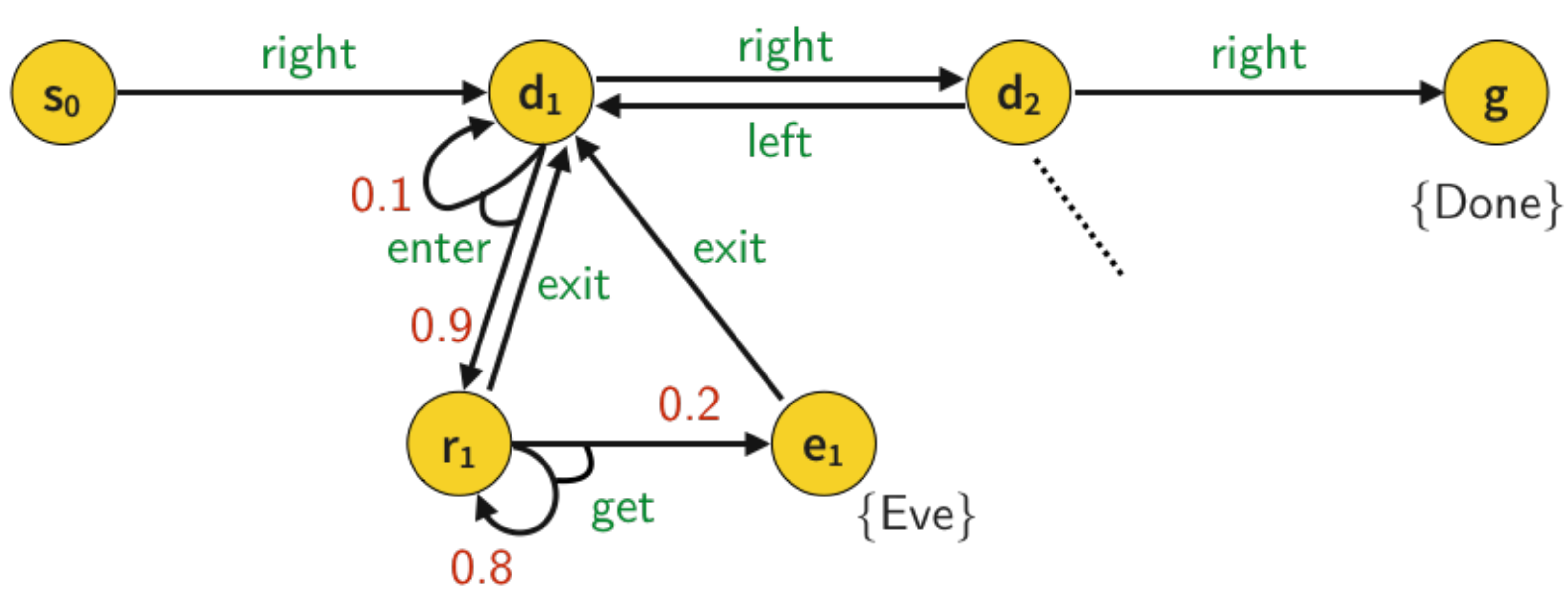
$\mathbf{s_0}$: right $\mathbf{d_1}$: enter $\mathbf{r_1}$: get $\mathbf{e_1}$: exit

✓ eventually Eve

✗ never Done

Attempt 2

$\mathbf{s_0}$: right $\mathbf{d_1}$: right $\mathbf{d_2}$: right



Policies - History Dependance and Randomization

Target property: $s_0 \models \mathbf{P}_{>0}\ \mathbf{F}\ (\mathrm{Eve} \wedge \mathbf{F}\ \mathrm{Done})$

Case M: History-independent policy

Attempt 1

$\mathbf{s_0}$: right $\mathbf{d_1}$: enter $\mathbf{r_1}$: get $\mathbf{e_1}$: exit

✓ eventually Eve

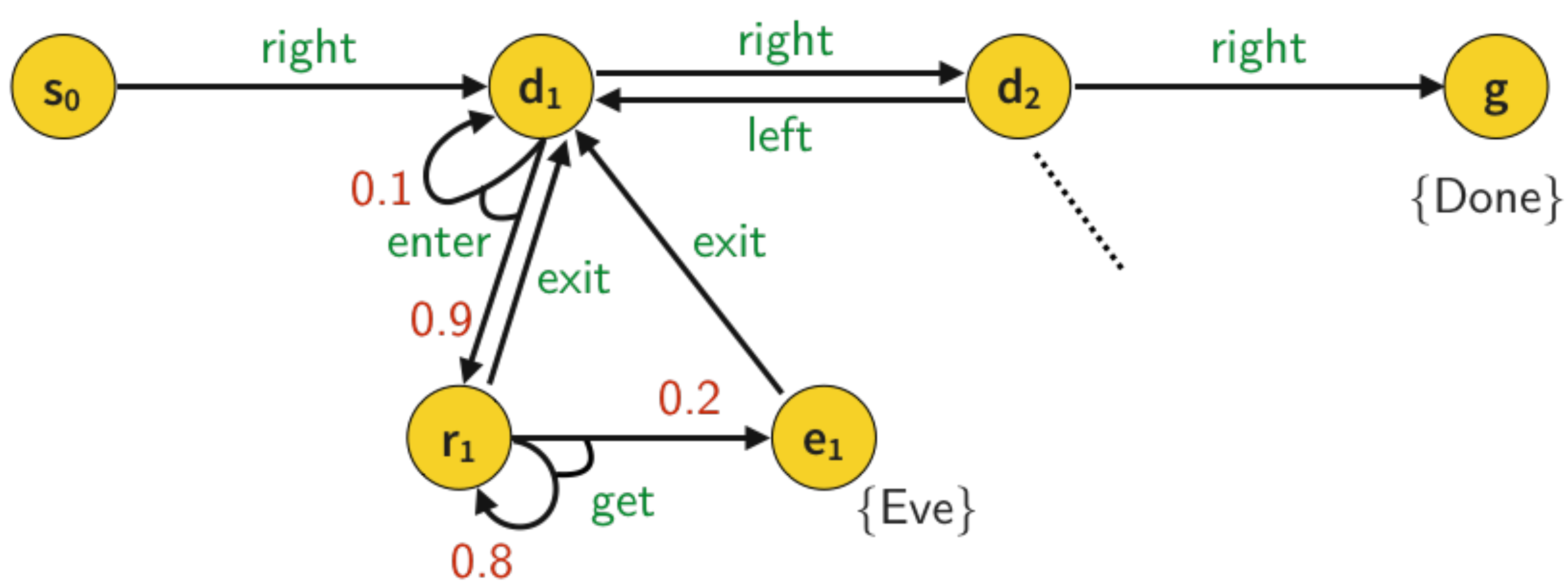
✗ never Done

Attempt 2

$\mathbf{s_0}$: right $\mathbf{d_1}$: right $\mathbf{d_2}$: right

✓ eventually Done

✗ never Eve



Policies - History Dependance and Randomization

Target property: $s_0 \models \mathbf{P}_{>0}\ \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case M: History-independent policy

Attempt 1

$\mathbf{s_0}$: right $\mathbf{d_1}$: enter $\mathbf{r_1}$: get $\mathbf{e_1}$: exit

✓ eventually Eve

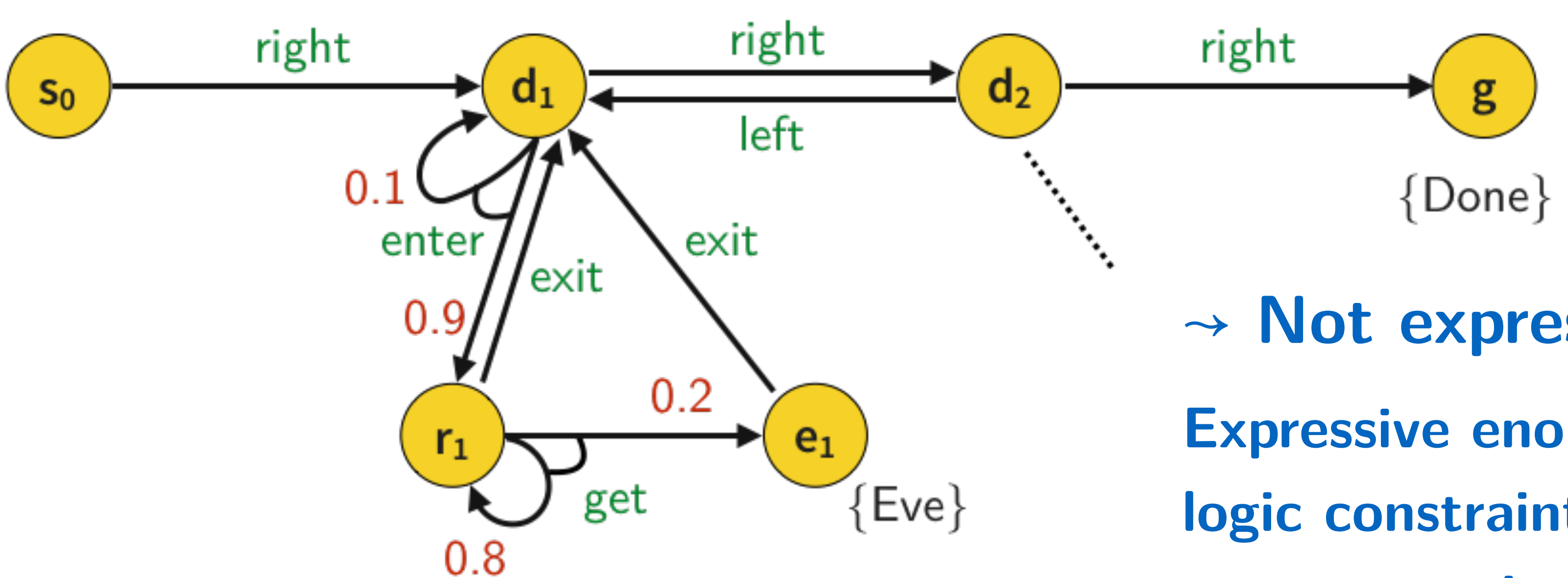
✗ never Done

Attempt 2

$\mathbf{s_0}$: right $\mathbf{d_1}$: right $\mathbf{d_2}$: right

✓ eventually Done

✗ never Eve



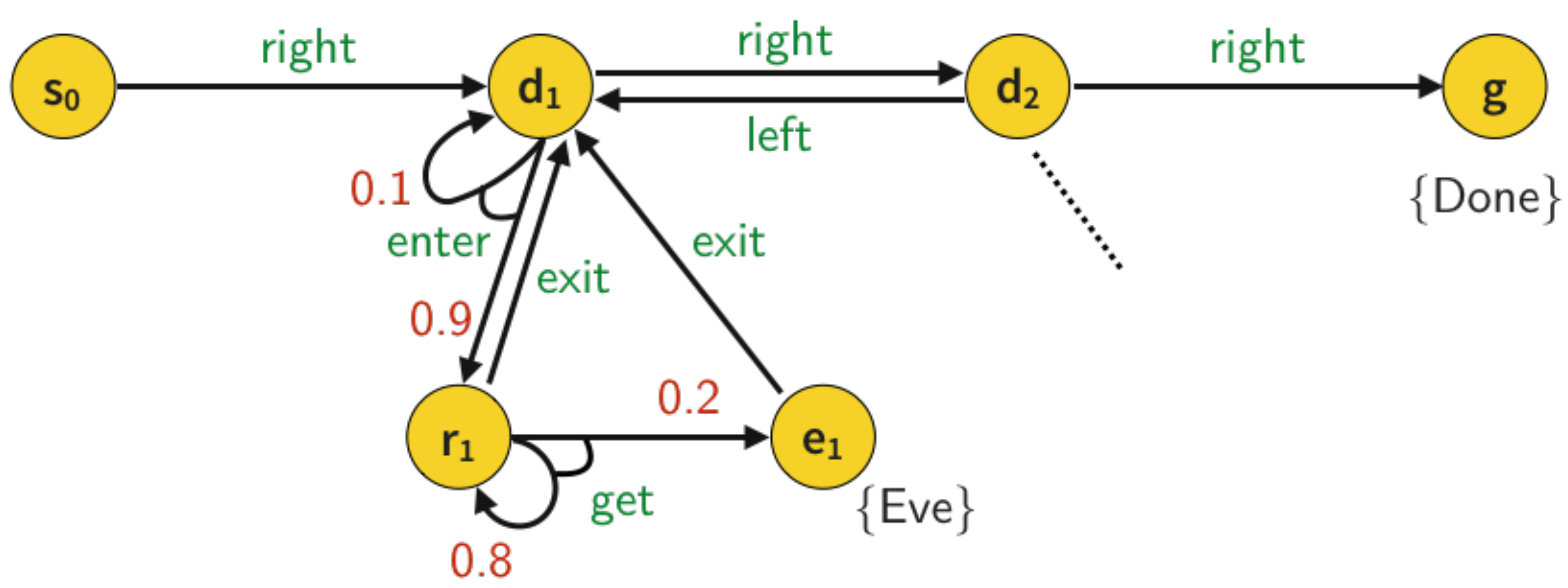
→ **Not expressive enough**

Expressive enough without logic constraints, e.g. cost constraints only

Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \vDash \mathbf{P}_{>0}\, \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case H: History-dependent policy

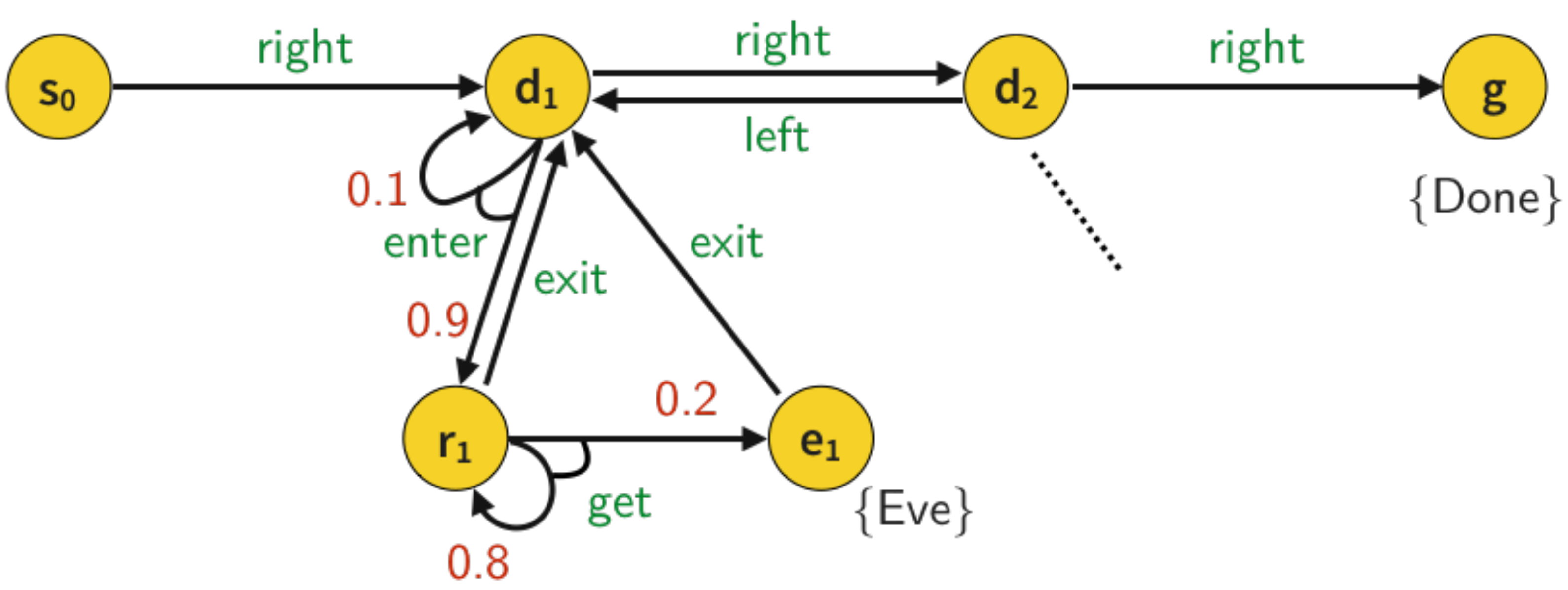


Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\, \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case H: History-dependent policy

$\mathbf{s_0}$: right

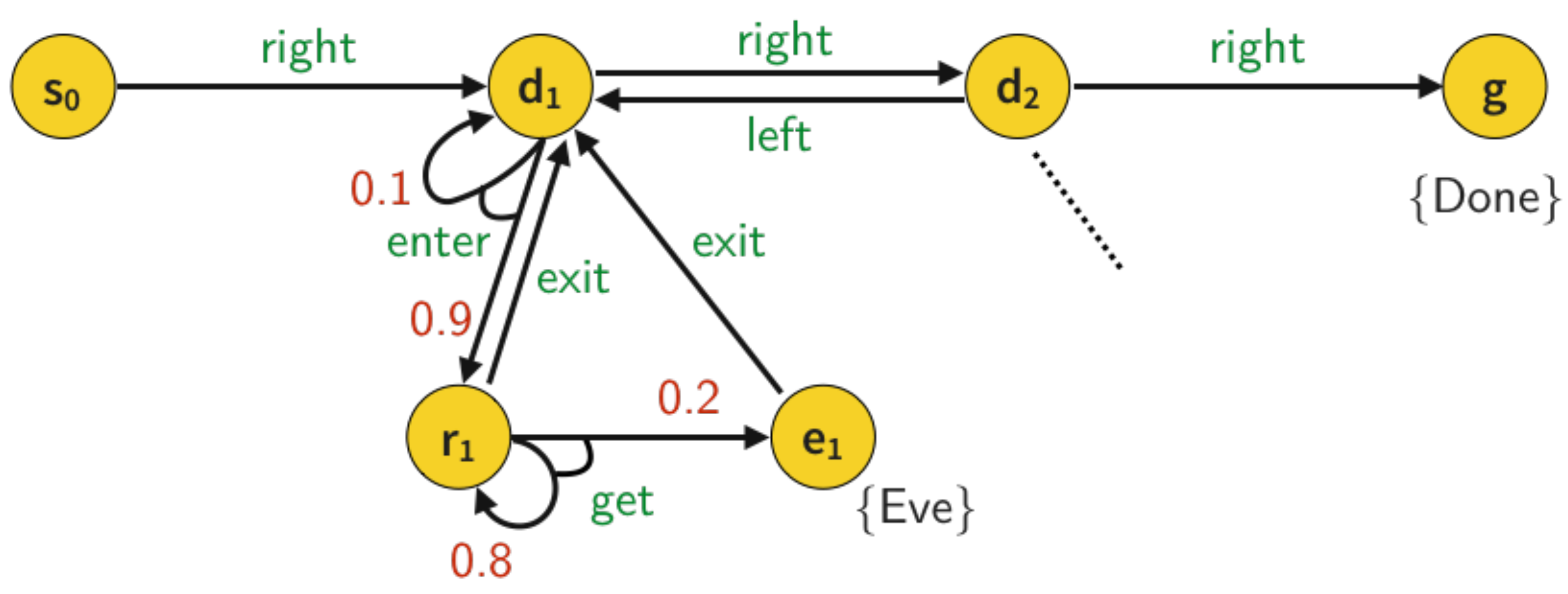


Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\, \mathbf{F}\, (\text{Eve} \wedge \mathbf{F}\, \text{Done})$

Case H: History-dependent policy

$\mathbf{s_0}$: right $\mathbf{s_0}\ \mathbf{d_1}\ \dots\ \mathbf{d_1}\ \dots\ \mathbf{d_1}$: enter

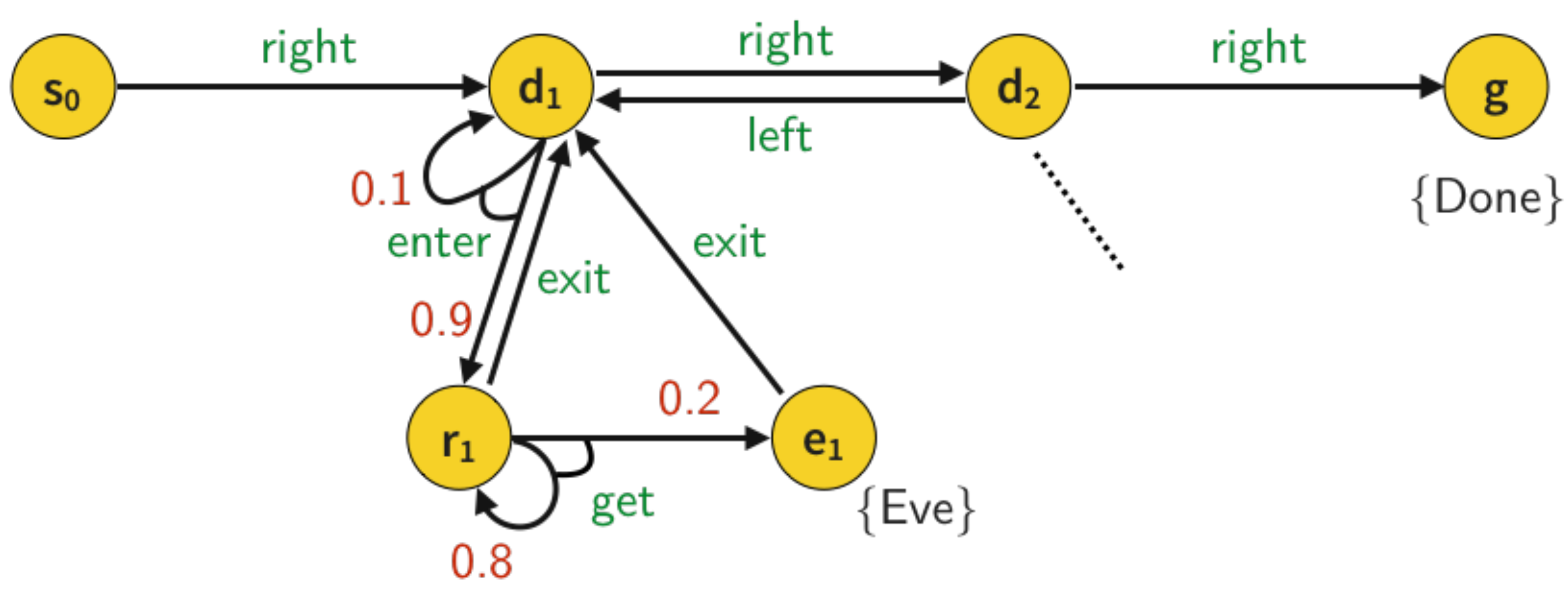


Policies - History Dependance and Randomization

Target property: $s_0 \models \mathbf{P}_{>0}\, \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case H: History-dependent policy

$\mathbf{s_0}$: right $\mathbf{s_0\ d_1\ \dots\ d_1\ \dots\ d_1}$: enter $\mathbf{s_0\ \dots\ r_1}$: get

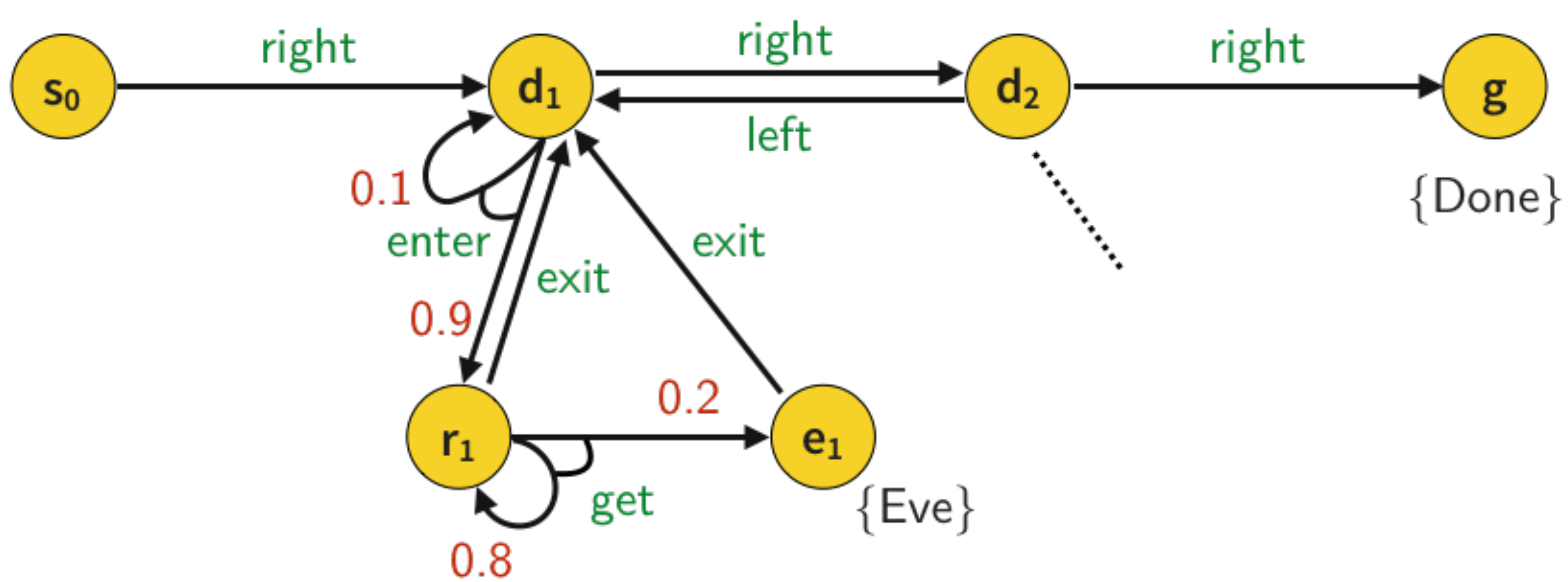


Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\ \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case H: History-dependent policy

$\mathbf{s_0}$: right $\mathbf{s_0\ d_1\ \ldots\ d_1\ \ldots\ d_1}$: enter $\mathbf{s_0\ \ldots\ r_1}$: get $\mathbf{s_0\ \ldots\ e_1}$: exit



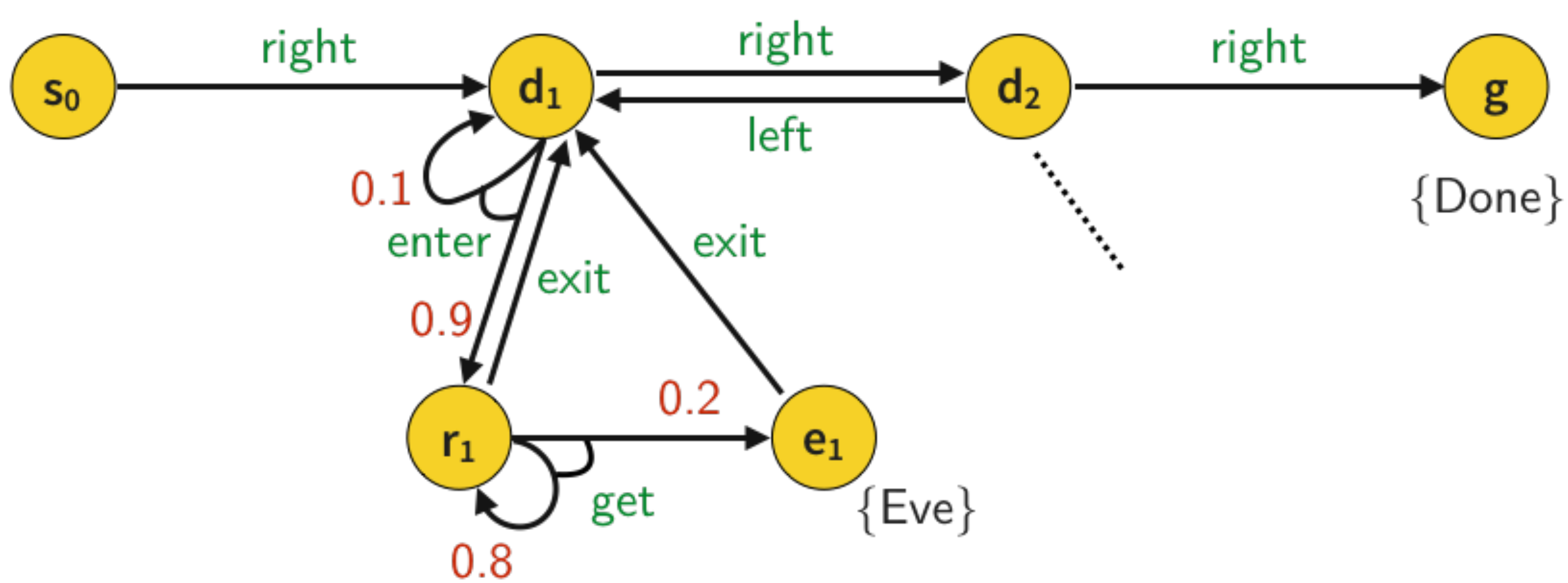
Policies - History Dependance and Randomization

Target property: $s_0 \models \mathbf{P}_{>0}\, \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case H: History-dependent policy

$\mathbf{s_0}$: right $\quad$ $\mathbf{s_0\ d_1\ \ldots\ d_1\ \ldots\ d_1}$: enter $\quad$ $\mathbf{s_0\ \ldots\ r_1}$: get $\quad$ $\mathbf{s_0\ \ldots\ e_1}$: exit

$\mathbf{s_0\ d_1\ \ldots\ e_1\ \ldots\ d_1}$: right



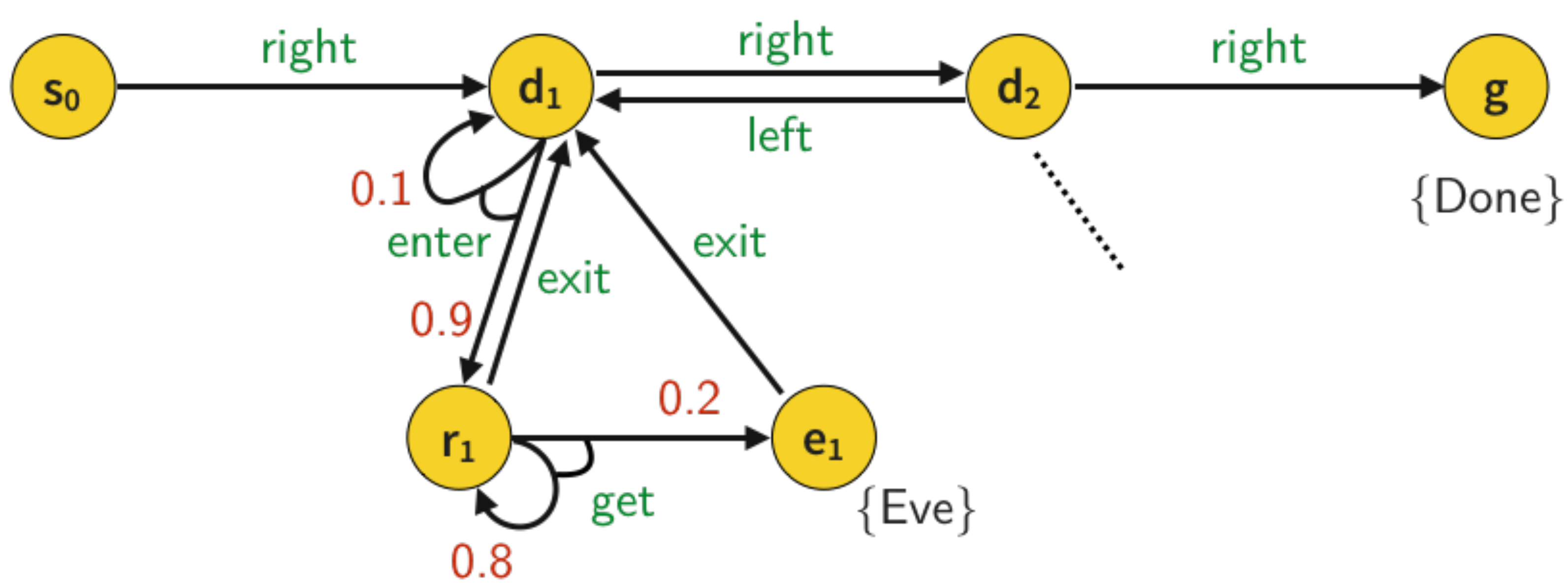
Policies - History Dependance and Randomization

Target property: $s_0 \models \mathbf{P}_{>0}\, \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case H: History-dependent policy

$\mathbf{s}_0$: right $\mathbf{s}_0\ \mathbf{d}_1\ \ldots\ \mathbf{d}_1\ \ldots\ \mathbf{d}_1$: enter $\mathbf{s}_0\ \ldots\ \mathbf{r}_1$: get $\mathbf{s}_0\ \ldots\ \mathbf{e}_1$: exit

$\mathbf{s}_0\ \mathbf{d}_1\ \ldots\ \mathbf{e}_1\ \ldots\ \mathbf{d}_1$: right $\mathbf{s}_0\ \ldots\ \mathbf{d}_2$: right



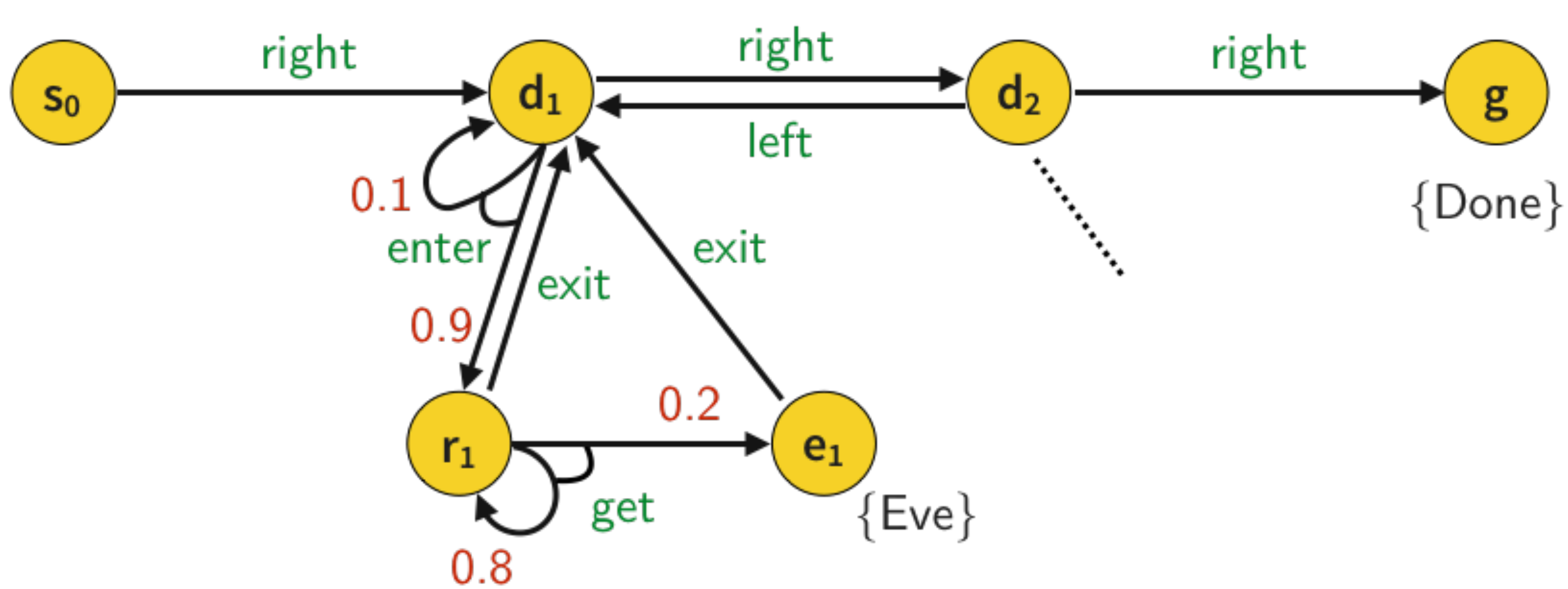
Policies - History Dependance and Randomization

Target property: $s_0 \models \mathbf{P}_{>0}\, \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case H: History-dependent policy

s_0: right $\quad$ $s_0\ d_1\ \ldots\ d_1\ \ldots\ d_1$: enter $\quad$ $s_0\ \ldots\ r_1$: get $\quad$ $s_0\ \ldots\ e_1$: exit $\quad$ ✓ eventually Eve

$s_0\ d_1\ \ldots\ e_1\ \ldots\ d_1$: right $\quad$ $s_0\ \ldots\ d_2$: right $\quad$ ✓ eventually Done



Policies - History Dependance and Randomization

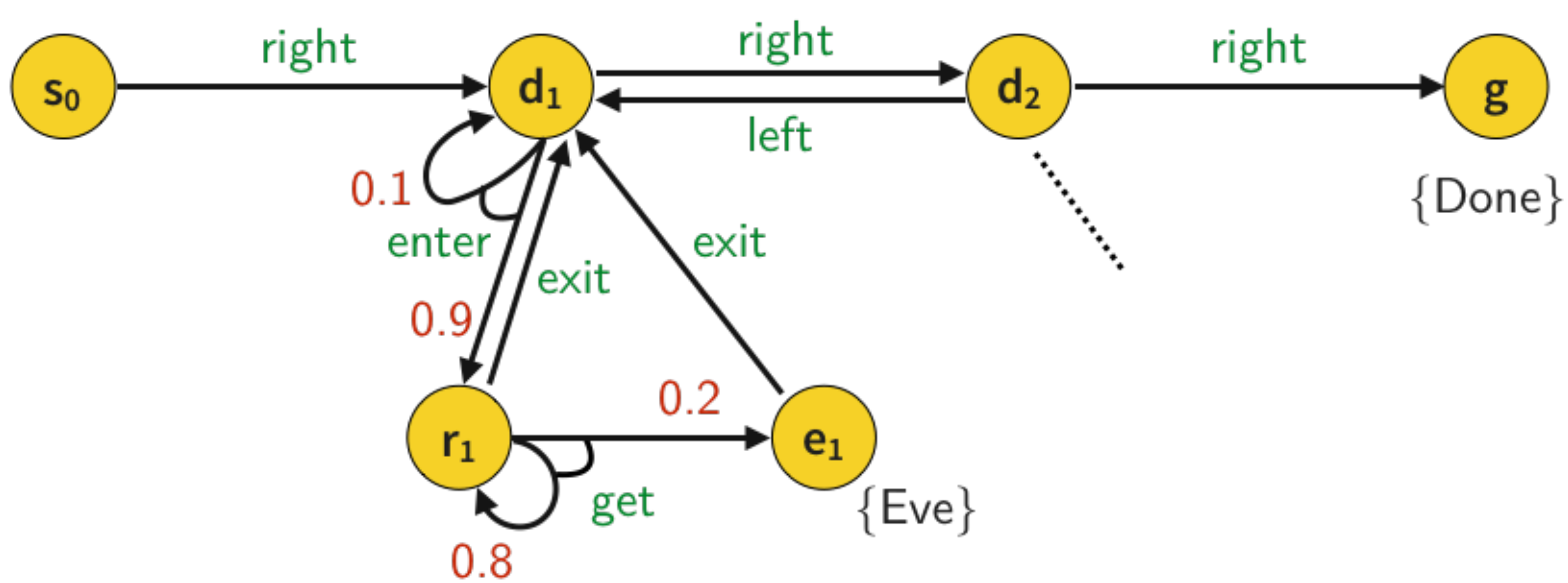
Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\, \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case H: History-dependent policy

$\mathbf{s_0}$: right　$\mathbf{s_0\ d_1\ \ldots\ d_1\ \ldots\ d_1}$: enter　$\mathbf{s_0\ \ldots\ r_1}$: get　$\mathbf{s_0\ \ldots\ e_1}$: exit　✓ eventually Eve

$\mathbf{s_0\ d_1\ \ldots\ e_1\ \ldots\ d_1}$: right　$\mathbf{s_0\ \ldots\ d_2}$: right　✓ eventually Done

✗ unbounded history length - highly undecidable



Policies - History Dependance and Randomization

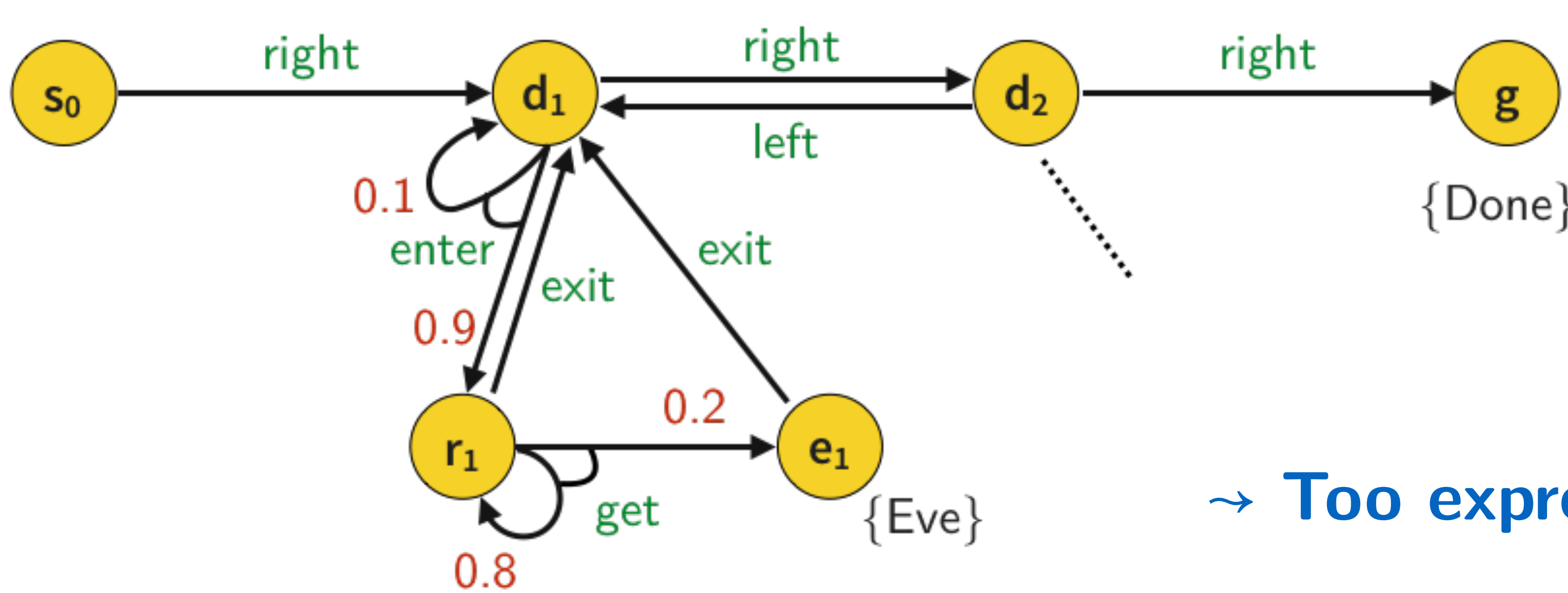
Target property: $s_0 \models \mathbf{P}_{>0}\,\mathbf{F}\,(\text{Eve} \wedge \mathbf{F}\,\text{Done})$

Case H: History-dependent policy

s_0: right $s_0\ d_1\ \ldots\ d_1\ \ldots\ d_1$: enter $s_0\ \ldots\ r_1$: get $s_0\ \ldots\ e_1$: exit ✓ eventually Eve

$s_0\ d_1\ \ldots\ e_1\ \ldots\ d_1$: right $s_0\ \ldots\ d_2$: right ✓ eventually Done

✗ unbounded history length - highly undecidable

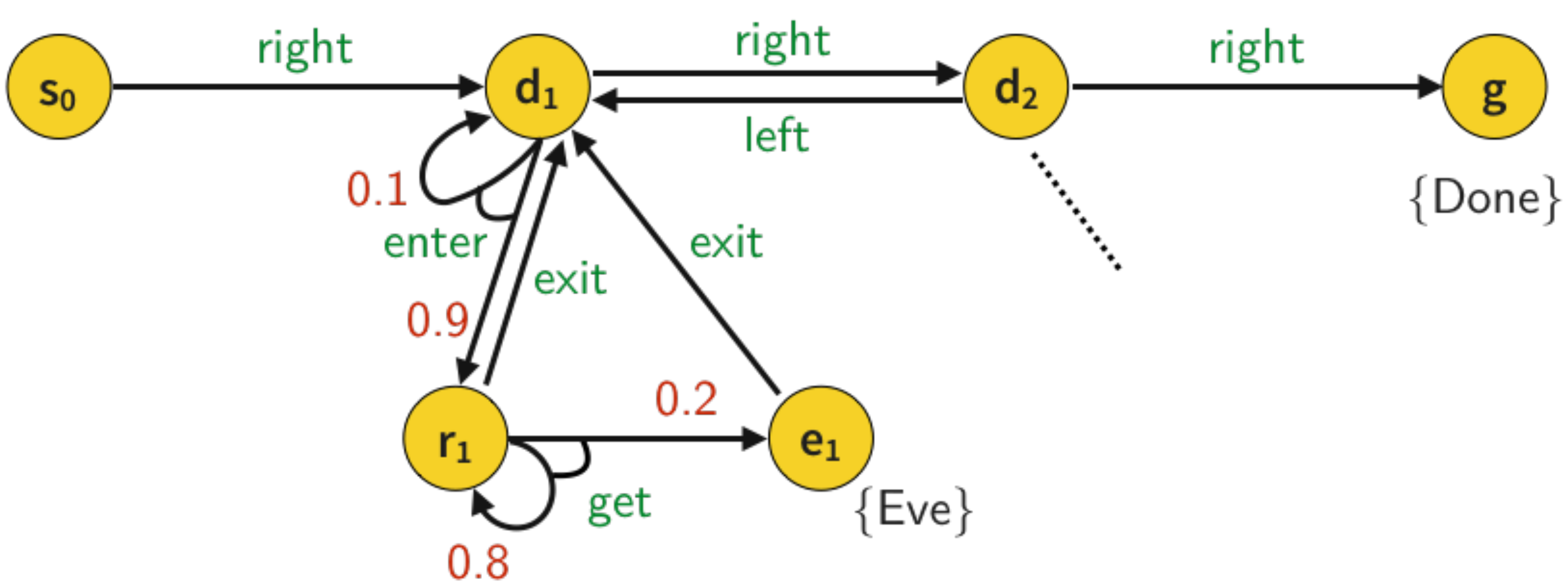


→ **Too expressive**

Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \vDash \mathbf{P}_{>0}\, \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case F: Finite history-dependent policy

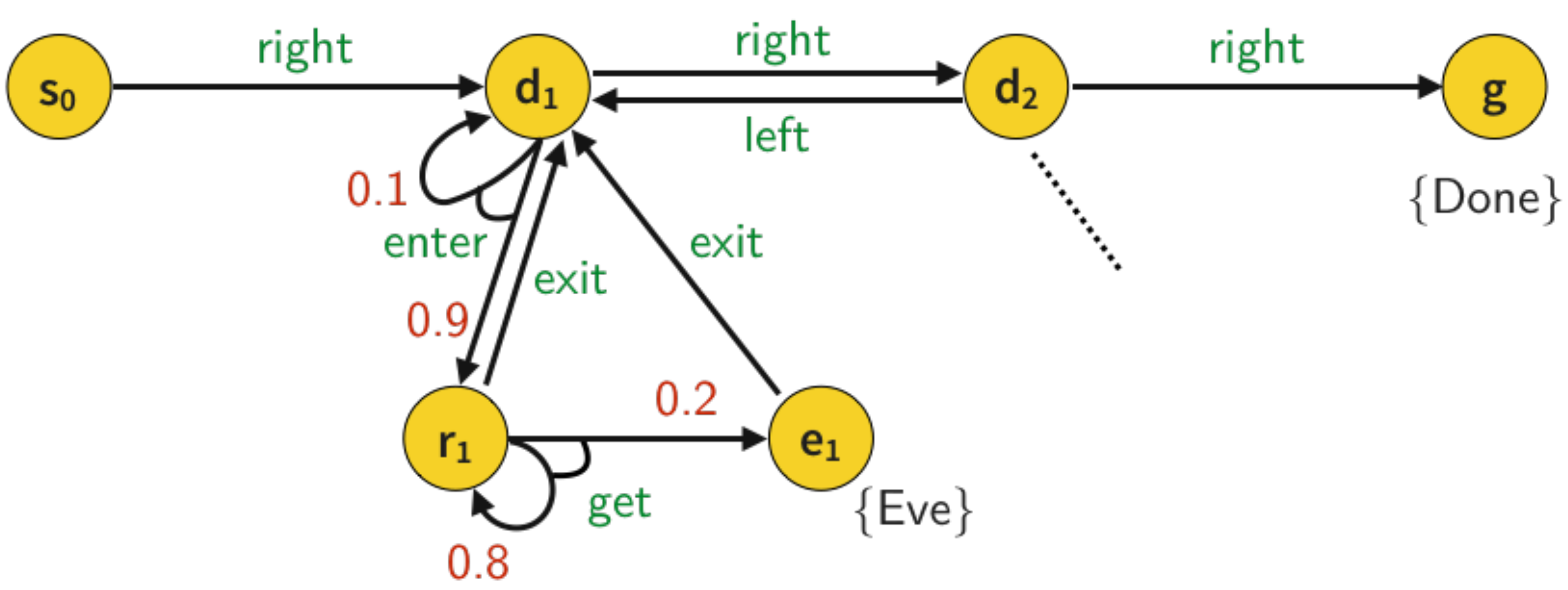


Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\, \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case F: Finite history-dependent policy

$\mathbf{s_0}$: right

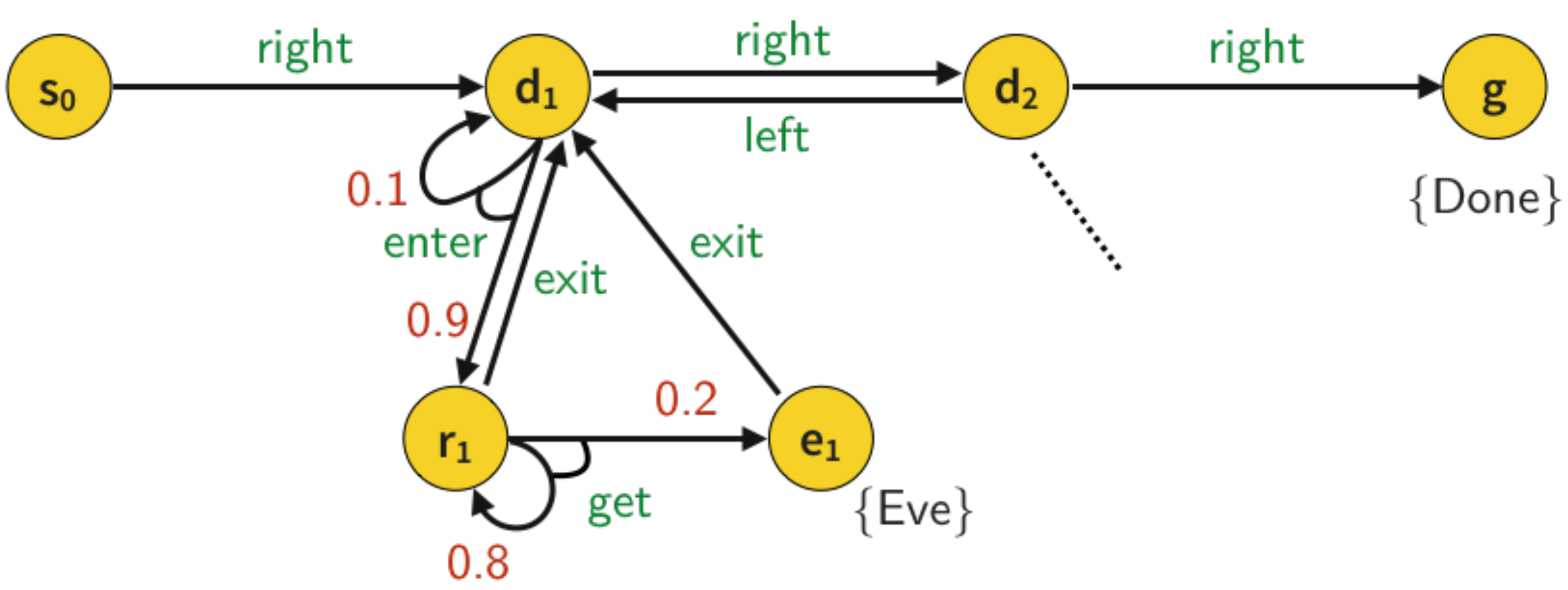


Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\, \mathbf{F}\, (\mathrm{Eve} \wedge \mathbf{F}\ \mathrm{Done})$

Case F: Finite history-dependent policy

$\mathbf{s_0}$: right $\quad$ $\mathbf{s_0 d_1}$: enter



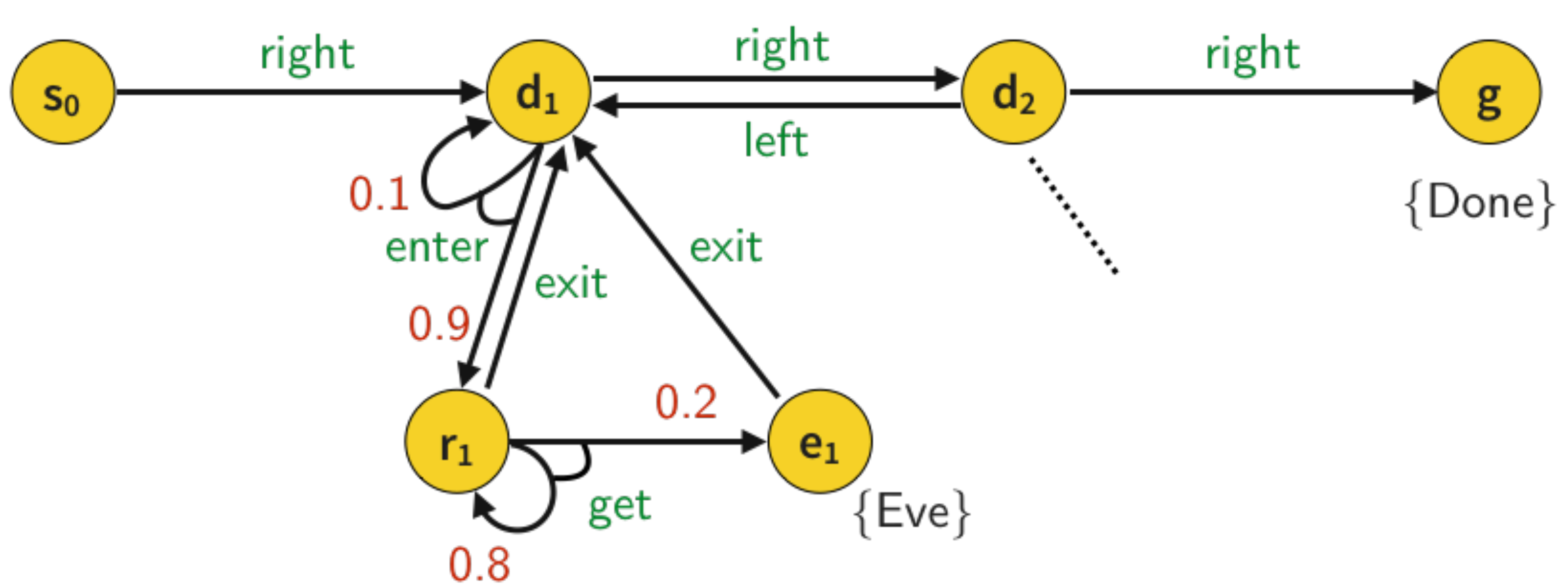
Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\, \mathbf{F}\, (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case F: Finite history-dependent policy

$\mathbf{s_0}$: right $\quad \mathbf{s_0 d_1}$: enter

$\mathbf{d_1 d_1}$: enter



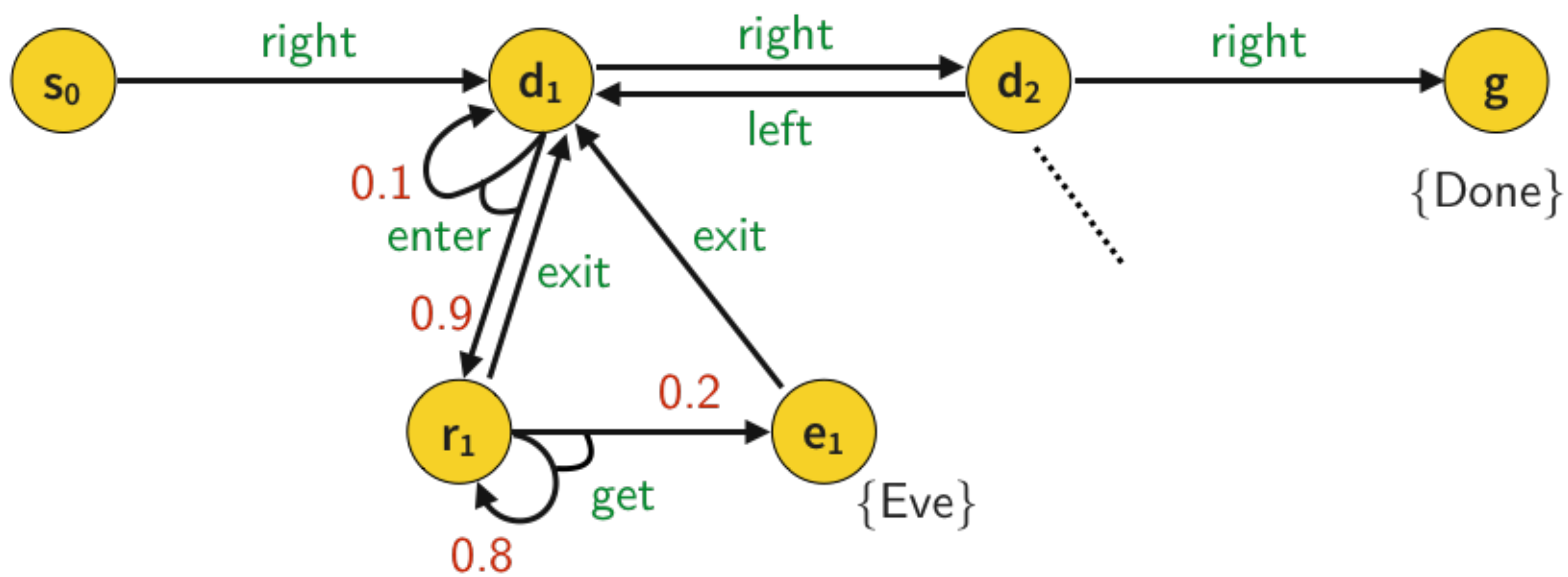
Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\, \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case F: Finite history-dependent policy

$\mathbf{s_0}$: right $\mathbf{s_0 d_1}$: enter $\mathbf{d_1 r_1}$: get

$\mathbf{d_1 d_1}$: enter



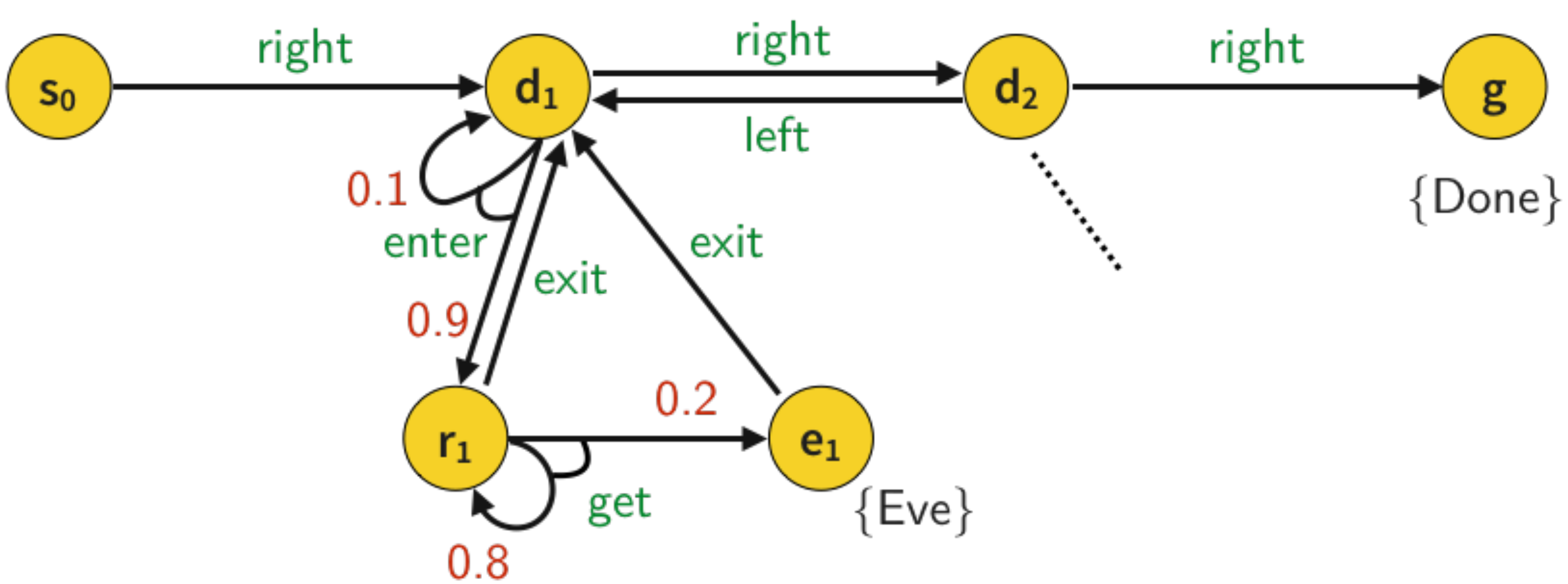
Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\,\mathbf{F}\,(\text{Eve} \wedge \mathbf{F}\,\text{Done})$

Case F: Finite history-dependent policy

$\mathbf{s_0}$: right $\quad$ $\mathbf{s_0 d_1}$: enter $\quad$ $\mathbf{d_1 r_1}$: get

$\mathbf{d_1 d_1}$: enter $\quad$ $\mathbf{r_1 r_1}$: get



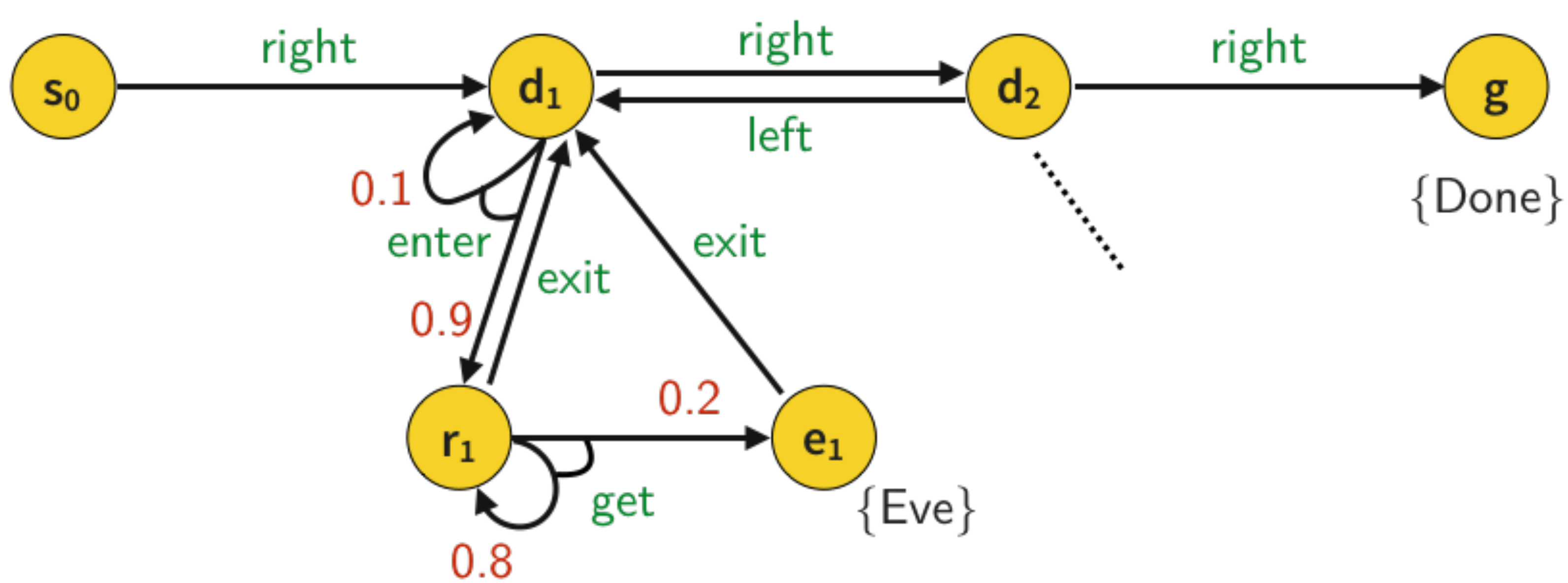
Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\, \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case F: Finite history-dependent policy

$\mathbf{s_0}$: right $\quad$ $\mathbf{s_0 d_1}$: enter $\quad$ $\mathbf{d_1 r_1}$: get $\quad$ $\mathbf{r_1 e_1}$: exit

$\mathbf{d_1 d_1}$: enter $\quad$ $\mathbf{r_1 r_1}$: get

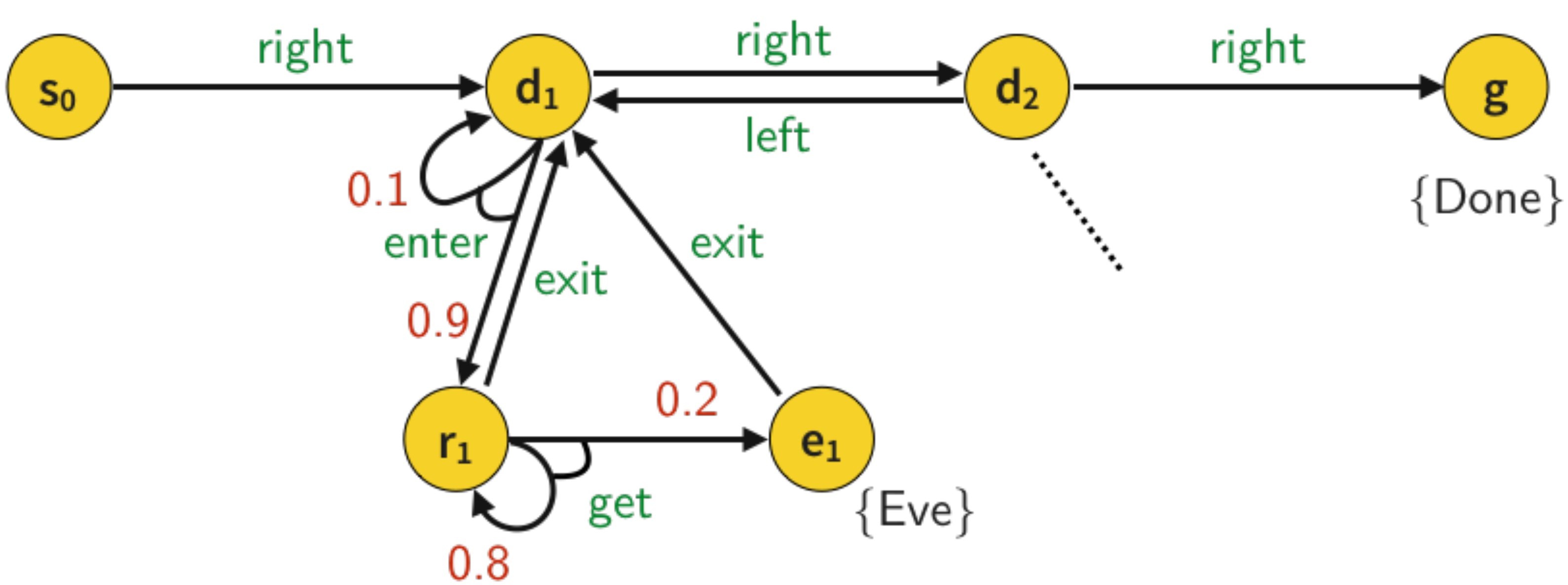


Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\, \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case F: Finite history-dependent policy

$\mathbf{s_0}$: right	$\mathbf{s_0 d_1}$: enter	$\mathbf{d_1 r_1}$: get	$\mathbf{r_1 e_1}$: exit	$\mathbf{e_1 d_1}$: right
	$\mathbf{d_1 d_1}$: enter	$\mathbf{r_1 r_1}$: get		



Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\, \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

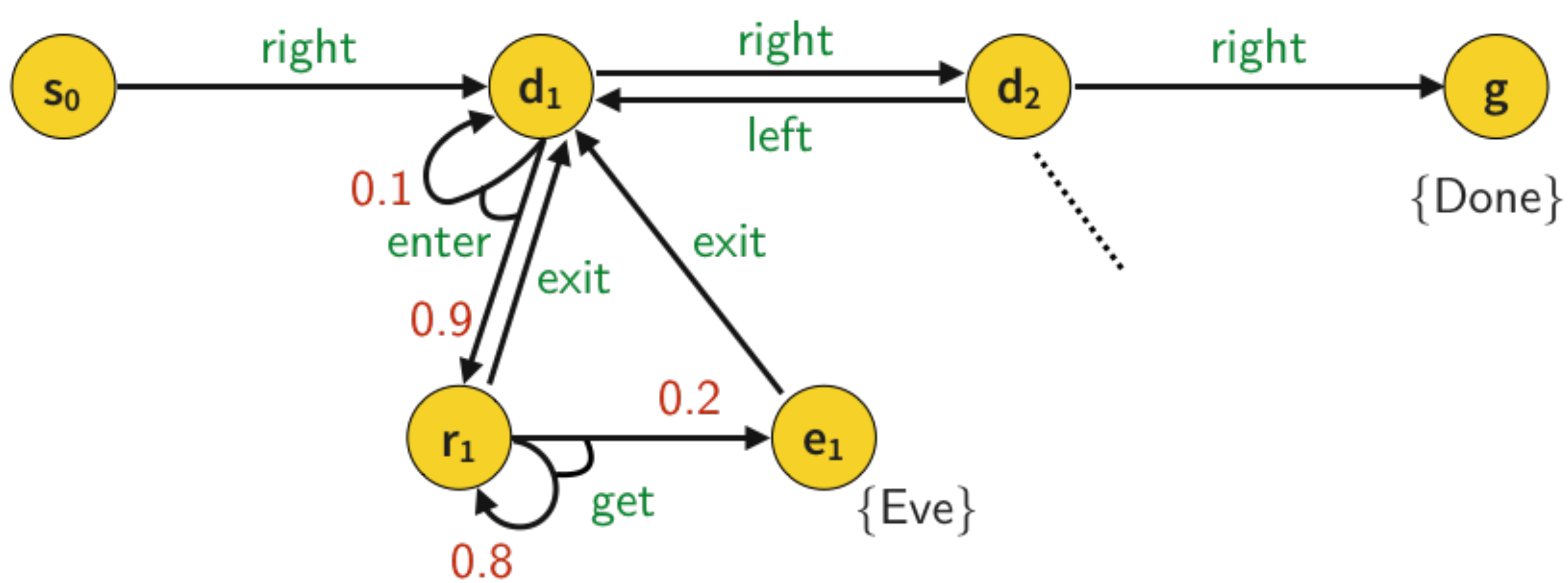
Case F: Finite history-dependent policy

$\mathbf{s_0}$: right $\mathbf{s_0 d_1}$: enter $\mathbf{d_1 r_1}$: get $\mathbf{r_1 e_1}$: exit $\mathbf{e_1 d_1}$: right

$\mathbf{d_1 d_1}$: enter $\mathbf{r_1 r_1}$: get

✓ eventually Eve

✓ eventually Done



Policies - History Dependance and Randomization

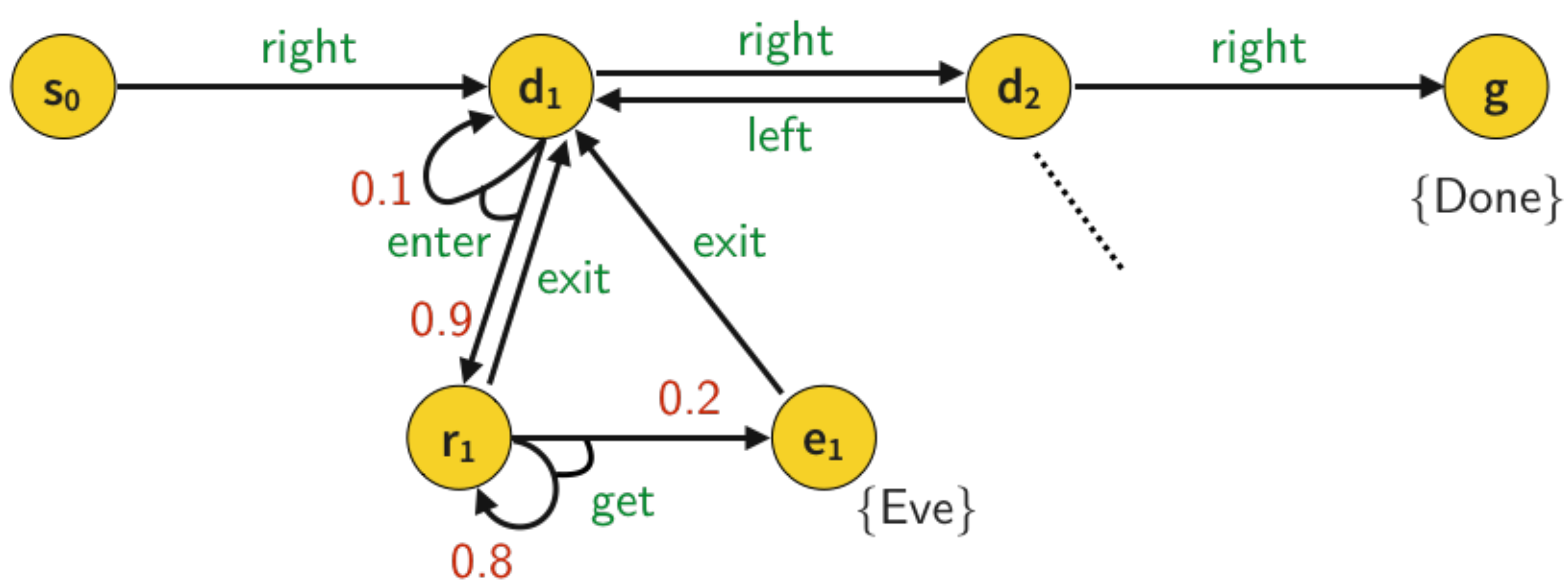
Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\, \mathbf{F}\ (\text{Eve} \wedge \mathbf{F}\ \text{Done})$

Case F: Finite history-dependent policy

$\mathbf{s_0}$: right	$\mathbf{s_0 d_1}$: enter	$\mathbf{d_1 r_1}$: get	$\mathbf{r_1 e_1}$: exit	$\mathbf{e_1 d_1}$: right	✓ eventually Eve
	$\mathbf{d_1 d_1}$: enter	$\mathbf{r_1 r_1}$: get			✓ eventually Done

Our approach

A priori finitely bounded history length - decidable (our main result)



Policies - History Dependance and Randomization

Target property: $s_0 \models \mathbf{P}_{>0}\, \mathbf{F}\,(\mathrm{Eve} \wedge \mathbf{F}\ \mathrm{Done})$

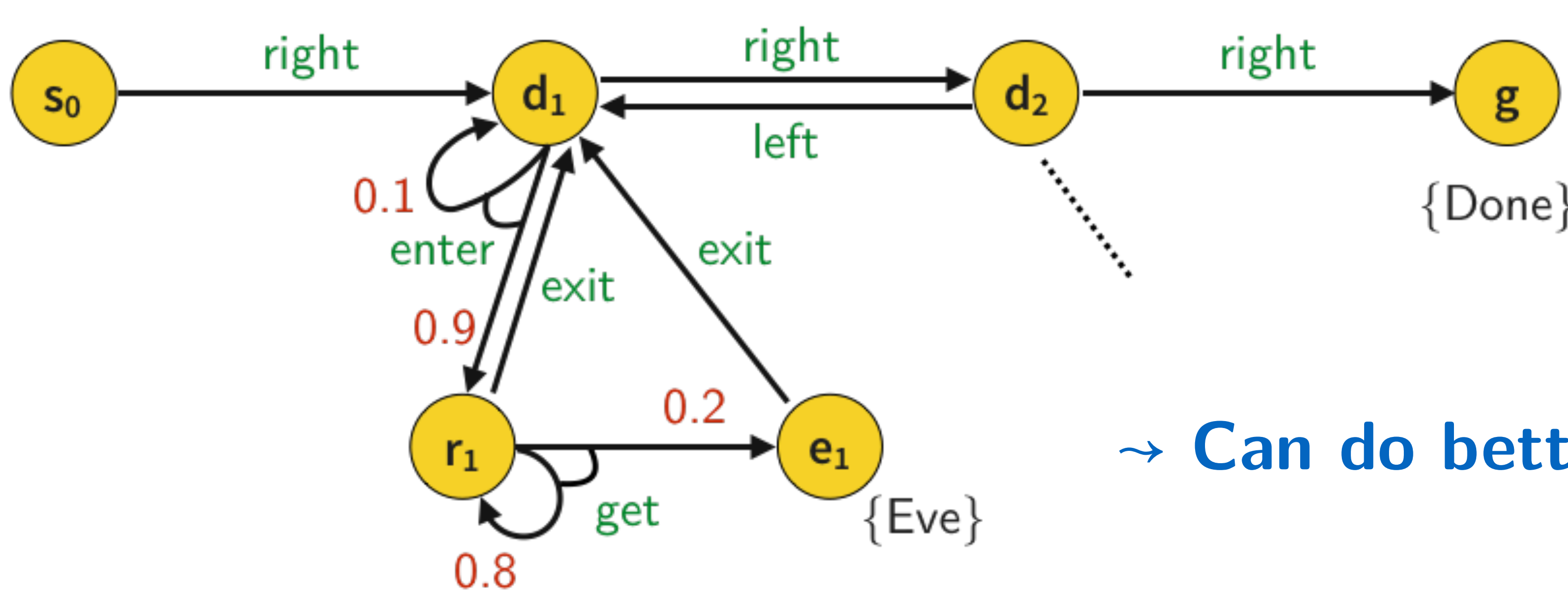
Case F: Finite history-dependent policy

s_0: right s_0d_1: enter d_1r_1: get r_1e_1: exit e_1d_1: right ✓ eventually Eve

d_1d_1: enter r_1r_1: get ✓ eventually Done

Our approach

A priori finitely bounded history length - decidable (our main result)

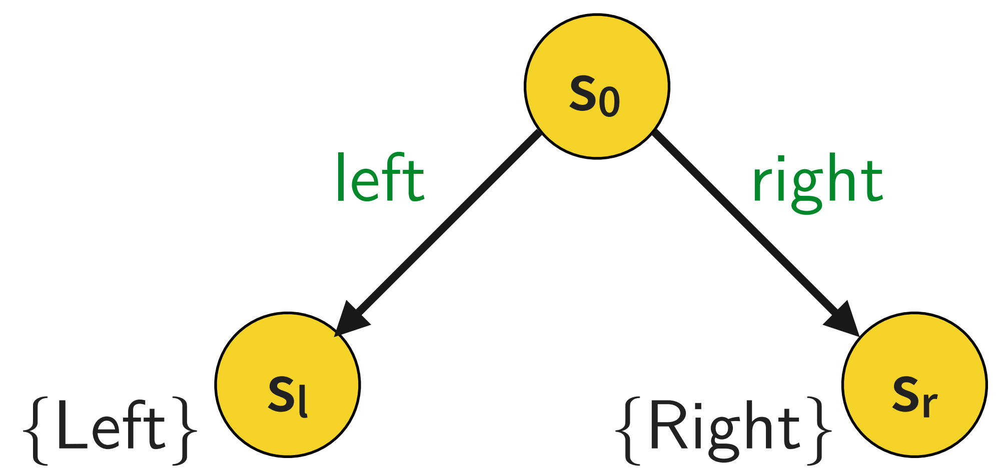


→ **Can do better (more expressive)**

Policies - History Dependance and Randomization

Target property: $\mathbf{P}_{>0}\ \mathbf{F}\ \text{Left} \wedge \mathbf{P}_{>0}\ \mathbf{F}\ \text{Right}$

Case D: Deterministic policy



Policies - History Dependance and Randomization

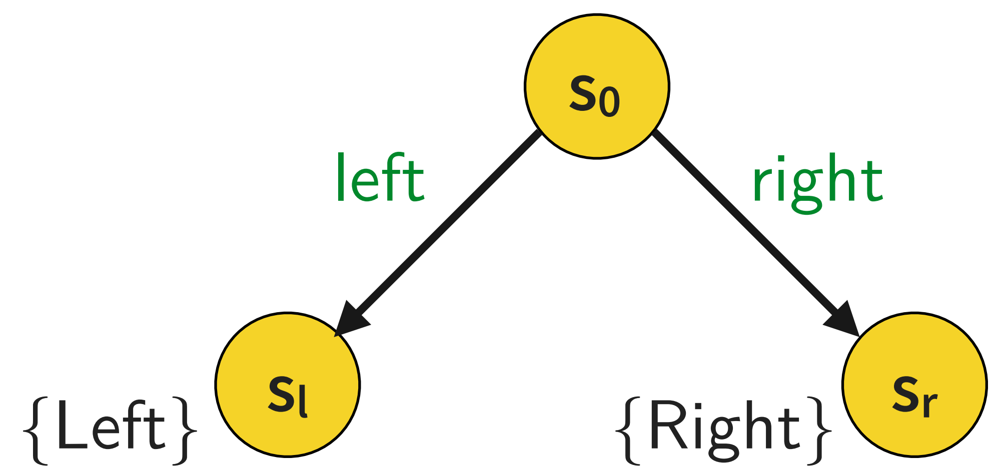
Target property: $\mathbf{P}_{>0}\ \mathbf{F}\ \text{Left} \wedge \mathbf{P}_{>0}\ \mathbf{F}\ \text{Right}$

Case D: Deterministic policy

Attempt 1

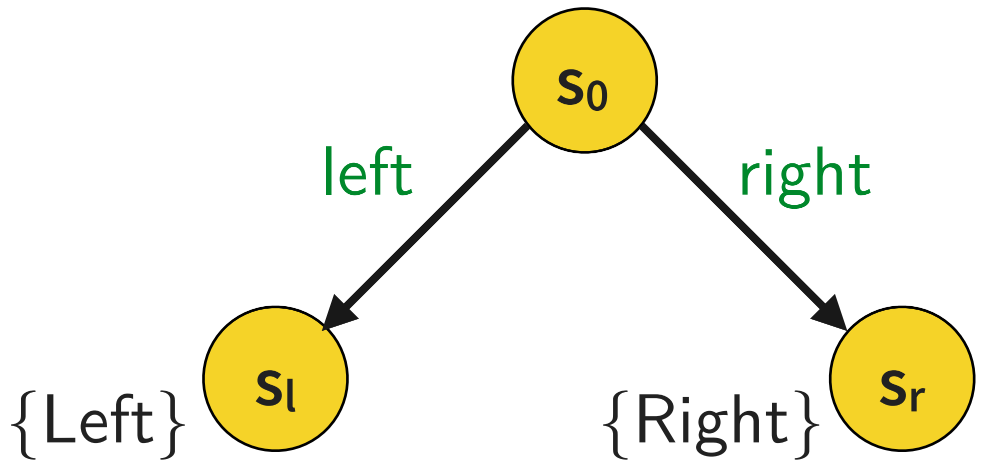
s_0: left ✓ $\mathbf{P}_{>0}\ \mathbf{F}\ \text{Left}$

✗ $\mathbf{P}_{>0}\ \mathbf{F}\ \text{Right}$



Policies - History Dependance and Randomization

Target property: $\mathbf{P}_{>0}\ \mathbf{F}\ \mathsf{Left} \wedge \mathbf{P}_{>0}\ \mathbf{F}\ \mathsf{Right}$



Case D: Deterministic policy

Attempt 1

s0: left ✓ $\mathbf{P}_{>0}\ \mathbf{F}\ \mathsf{Left}$

✗ $\mathbf{P}_{>0}\ \mathbf{F}\ \mathsf{Right}$

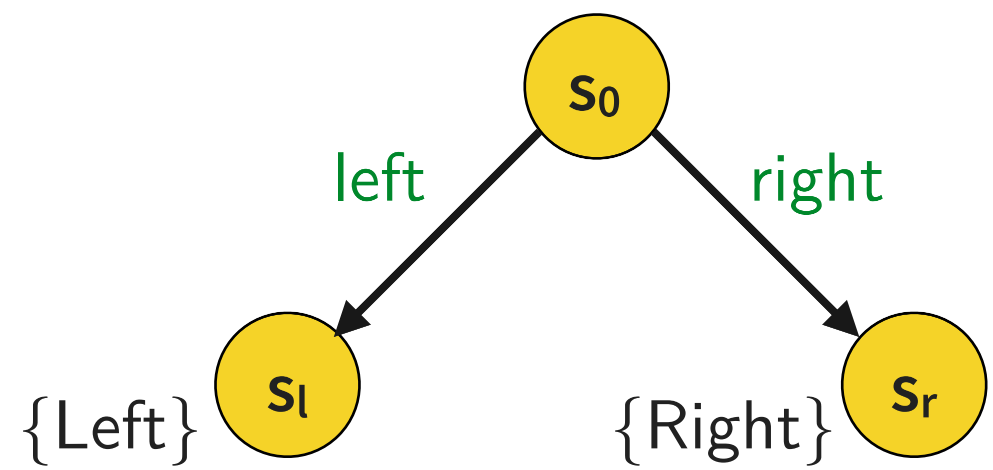
Attempt 2

s0: right ✗ $\mathbf{P}_{>0}\ \mathbf{F}\ \mathsf{Left}$

✓ $\mathbf{P}_{>0}\ \mathbf{F}\ \mathsf{Right}$

Policies - History Dependance and Randomization

Target property: $\mathbf{P}_{>0}$ **F** Left $\wedge$ $\mathbf{P}_{>0}$ **F** Right



Case D: Deterministic policy

Attempt 1

s_0: left   ✓ $\mathbf{P}_{>0}$ **F** Left
✗ $\mathbf{P}_{>0}$ **F** Right

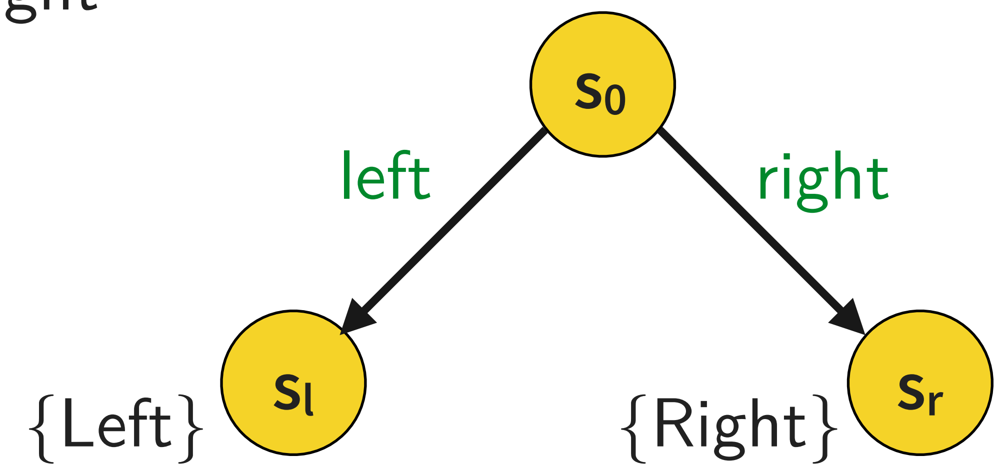
Attempt 2

s_0: right   ✗ $\mathbf{P}_{>0}$ **F** Left
✓ $\mathbf{P}_{>0}$ **F** Right

$\rightsquigarrow$ **Fix: randomized policies**

Policies - History Dependance and Randomization

Target property: $\mathbf{s_0} \models \mathbf{P}_{>0}\ \mathbf{F}\ \text{Left} \land \mathbf{P}_{>0}\ \mathbf{F}\ \text{Right}$



Case R: Randomized policy

σ is a **probability distribution** over actions for each state (history/state)

"In 6 out of 10 experiments chose left"

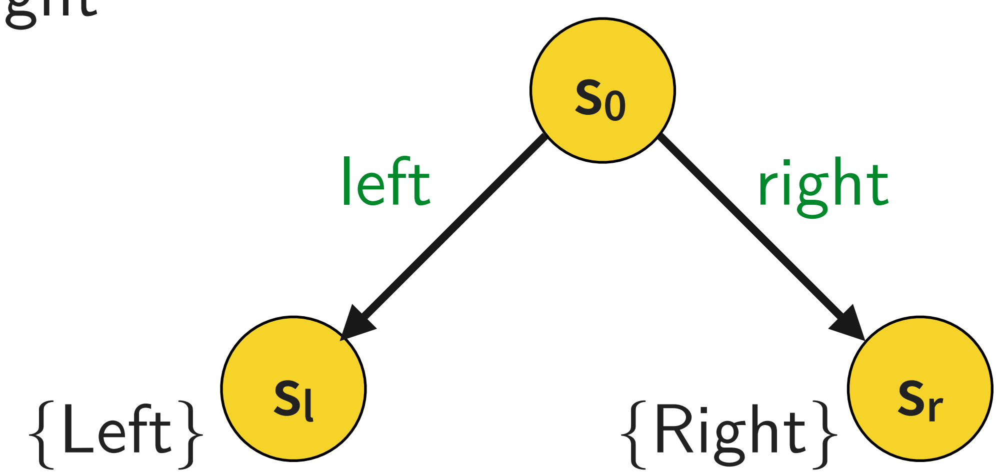
$\mathbf{s_0}$: [left $\to$ 0.6, right $\to$ 0.4]

✓ $\mathbf{P}_{>0}\ \mathbf{F}$ Left

✓ $\mathbf{P}_{>0}\ \mathbf{F}$ Right

Policies - History Dependance and Randomization

Target property: $s_0 \models \mathbf{P}_{>0}\ \mathbf{F}\ \text{Left} \wedge \mathbf{P}_{>0}\ \mathbf{F}\ \text{Right}$



Case R: Randomized policy

σ is a **probability distribution** over actions for each state (history/state)

"In 6 out of 10 experiments chose left"

s_0: [left $\rightarrow$ 0.6, right $\rightarrow$ 0.4]

✓ $\mathbf{P}_{>0}\ \mathbf{F}\ \text{Left}$

✓ $\mathbf{P}_{>0}\ \mathbf{F}\ \text{Right}$

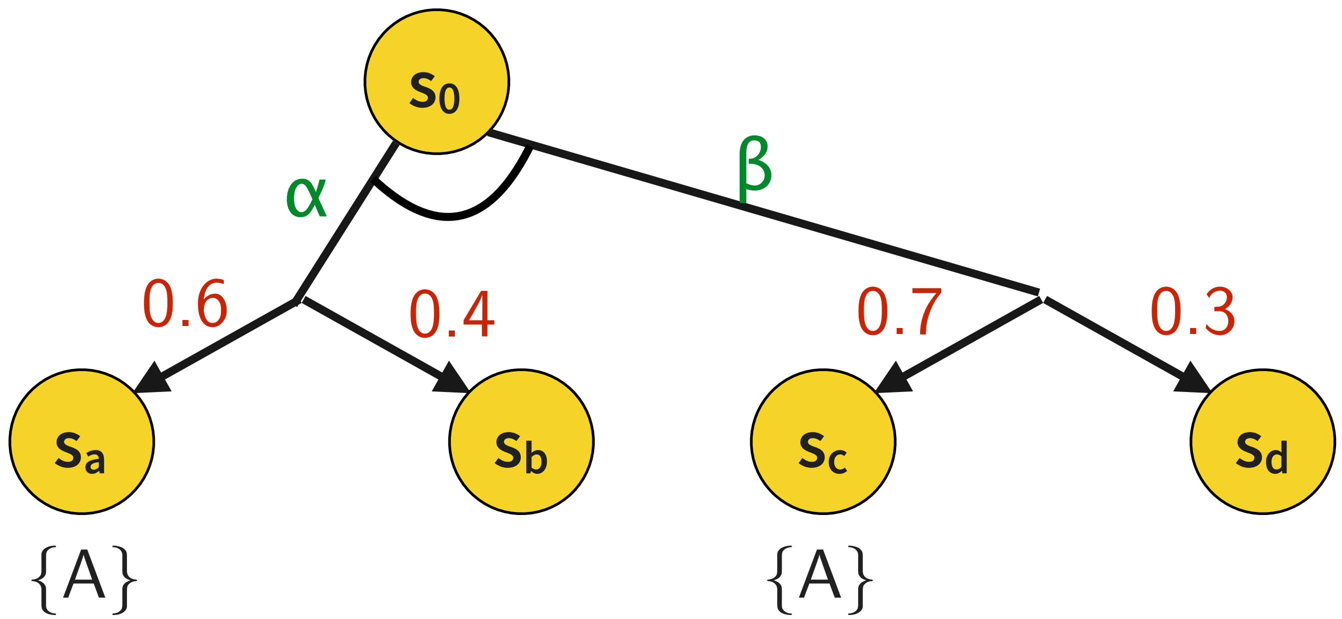
$\rightsquigarrow$ **Identified target policies: FR**

Look at policy synthesis in more detail

Probabilities of Paths Again: Randomized case

Policy σ

$\mathbf{s_0}$: $[\alpha \to 0.6, \beta \to 0.4]$



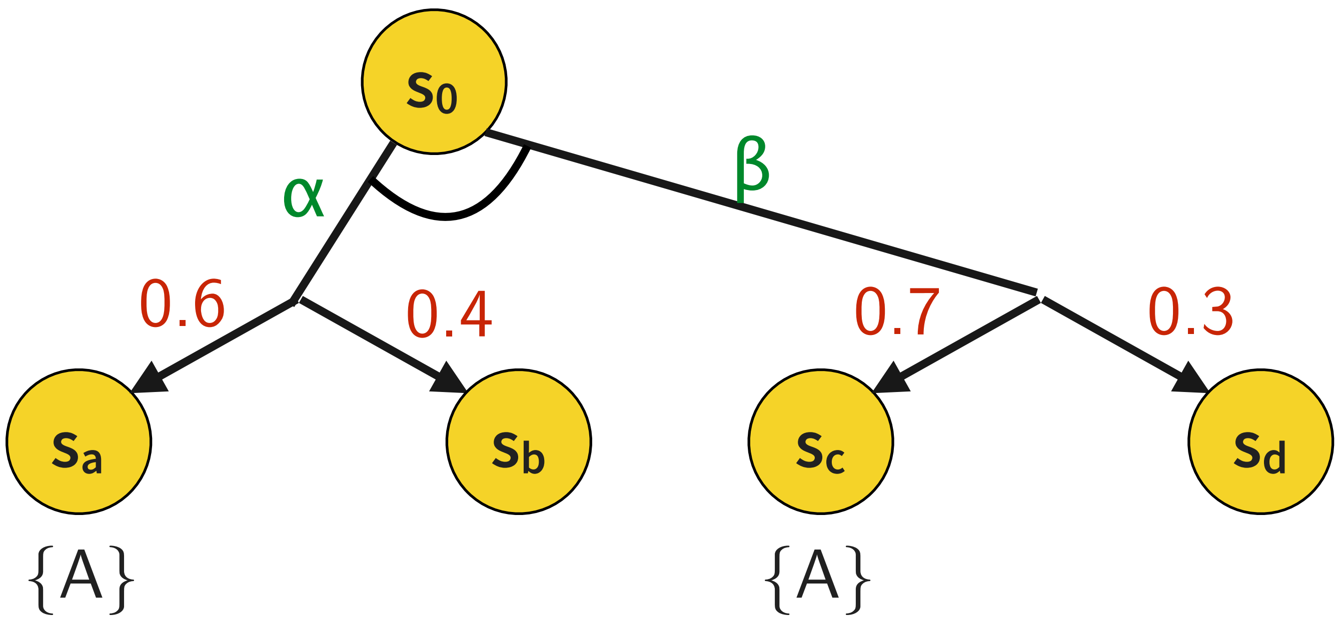
Evaluation

$\mathbf{s_0} \models \mathbf{P}_{>0.6}\ \mathbf{F}\ A$ *The probability of all paths from* $\mathbf{s_0}$ *satisfying* $\mathbf{F}$ A *is* > 0.6

Probabilities of Paths Again: Randomized case

Policy σ

$\mathbf{s_0}$: $[\alpha \rightarrow 0.6,\ \beta \rightarrow 0.4]$



Evaluation

$\mathbf{s_0} \models \mathbf{P}_{>0.6}\ \mathbf{F}\ A$ *The probability of all paths from* $\mathbf{s_0}$ *satisfying* $\mathbf{F}$ A *is* > 0.6

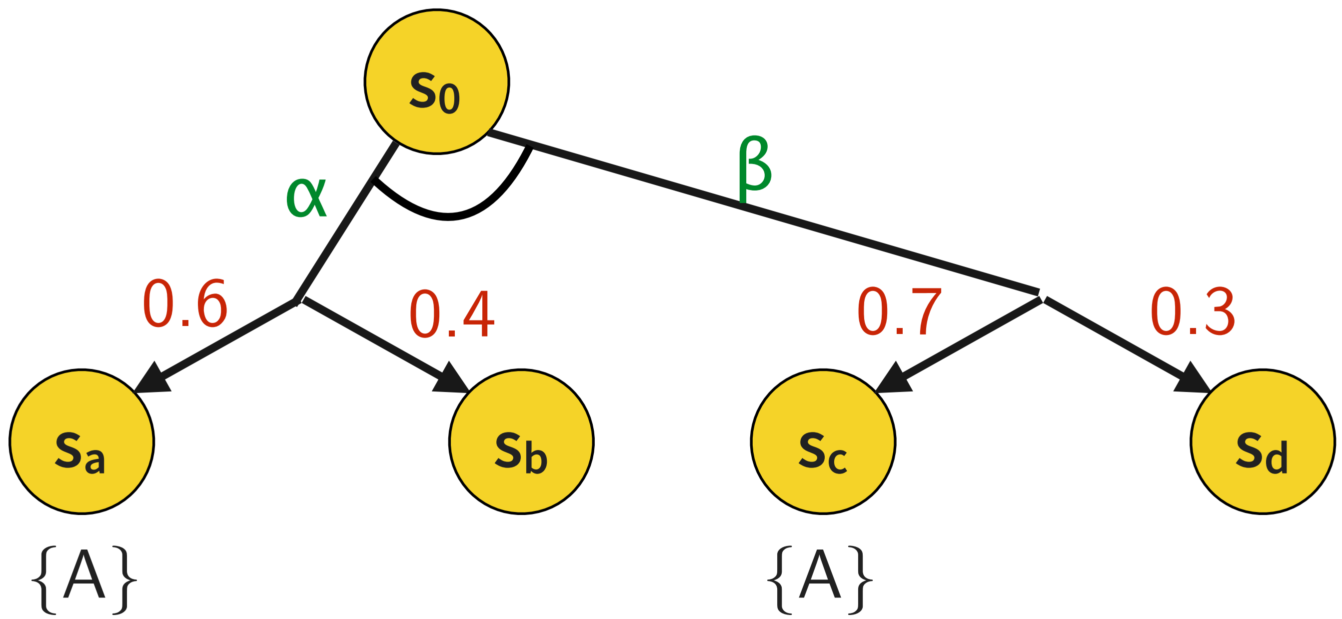
iff

$\Pr\{p \mid p \text{ is a } \sigma\text{-path from } \mathbf{s_0} \text{ and } p \models \mathbf{F}\ A\} > 0.6$

Probabilities of Paths Again: Randomized case

Policy σ

$\mathbf{s_0}$: $[\alpha \to 0.6, \beta \to 0.4]$



Evaluation

$\mathbf{s_0} \vDash \mathbf{P}_{>0.6}\ \mathbf{F}\ A$ *The probability of all paths from* $\mathbf{s_0}$ *satisfying* $\mathbf{F}$ A *is* > 0.6

iff

$\Pr\{p \mid p \text{ is a } \sigma\text{-path from } \mathbf{s_0} \text{ and } p \vDash \mathbf{F}\ A\} > 0.6$

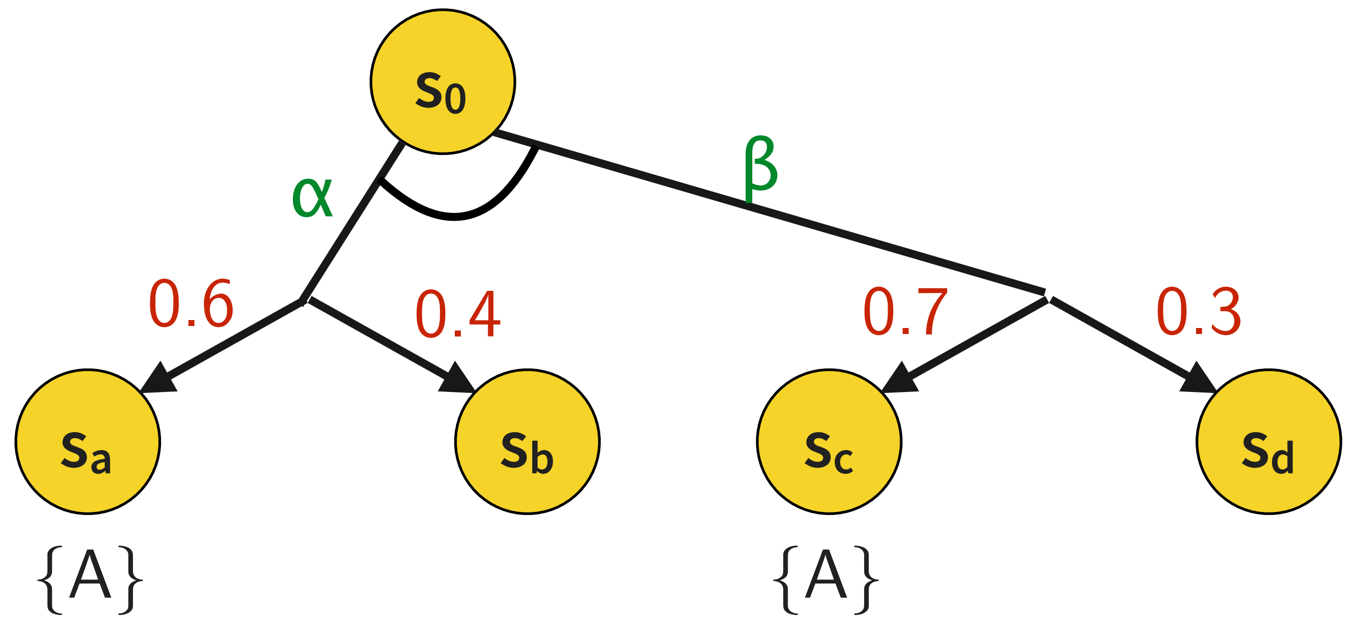
Non-probabilistic CTL/LTL/CTL*

σ-path: non-0 probability actions

Probabilities of Paths Again: Randomized case

Policy σ

$\mathbf{s_0}$: $[\alpha \to 0.6,\ \beta \to 0.4]$



Evaluation

$\mathbf{s_0} \models \mathbf{P}_{>0.6}\ \mathbf{F}\ A$ *The probability of all paths from* $\mathbf{s_0}$ *satisfying* $\mathbf{F}$ A *is* > 0.6

iff

$\Pr\{p \mid \underline{p \text{ is a } \sigma\text{-path from } \mathbf{s_0} \text{ and } p \models \mathbf{F}\ A}\} > 0.6$

iff

$\Pr\{\mathbf{s_0 s_a},\ \mathbf{s_0 s_c}\} > 0.6$

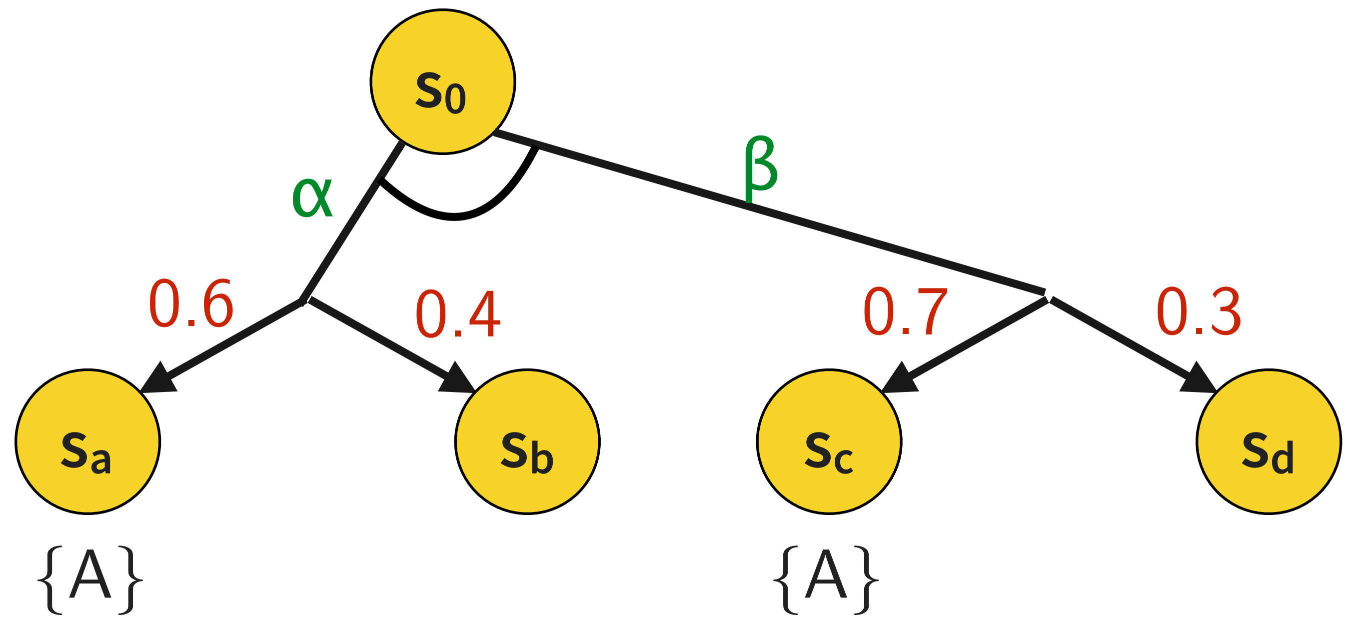
Non-probabilistic CTL/LTL/CTL*

σ-path: non-0 probability actions

Probabilities of Paths Again: Randomized case

Policy σ

$\mathbf{s_0}$: $[\alpha \to 0.6,\ \beta \to 0.4]$



Evaluation

$\mathbf{s_0} \models \mathbf{P}_{>0.6}\ \mathbf{F}\ A$ *The probability of all paths from* $\mathbf{s_0}$ *satisfying* $\mathbf{F}$ A *is* > 0.6

iff

$\Pr\{p \mid p \text{ is a } \sigma\text{-path from } \mathbf{s_0} \text{ and } p \models \mathbf{F}\ A\} > 0.6$

iff

$\Pr\{\mathbf{s_0 s_a},\ \mathbf{s_0 s_c}\} > 0.6$

iff

$0.6 \cdot 0.6 + 0.4 \cdot 0.7 = 0.64 > 0.6$

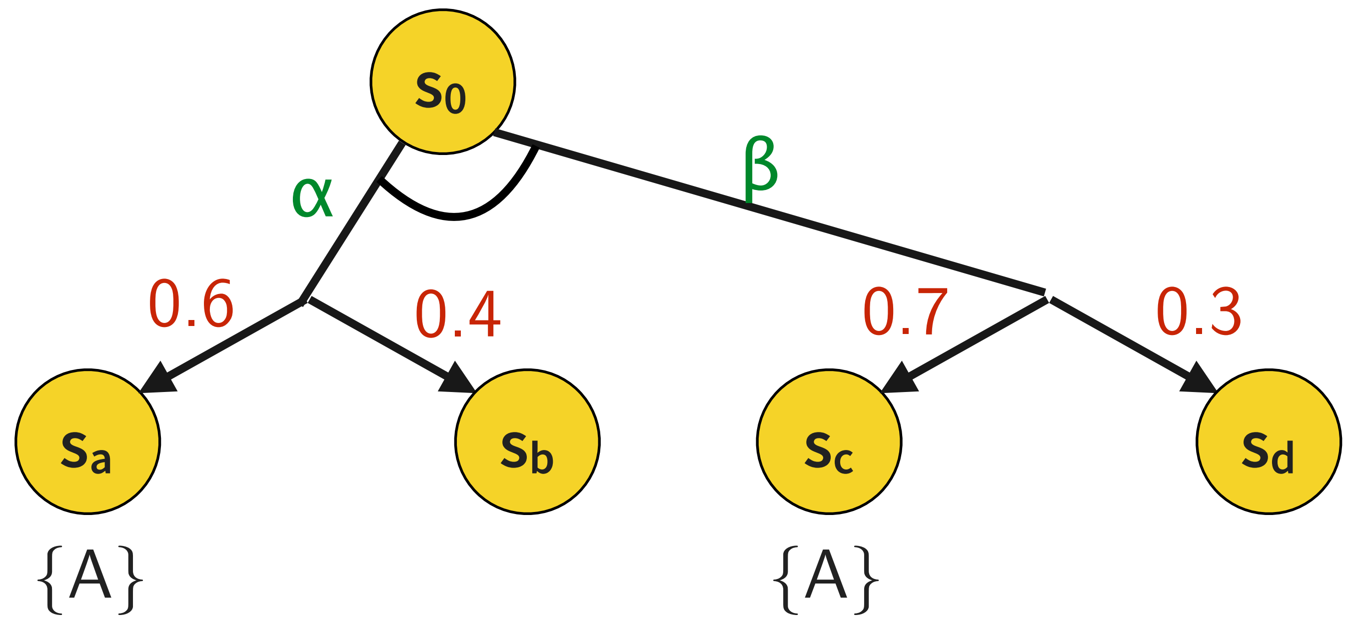
Non-probabilistic CTL/LTL/CTL*

σ-path: non-0 probability actions

Probabilities of Paths Again: Randomized case

Policy σ

$\mathbf{s_0}$: $[\alpha \to 0.6,\ \beta \to 0.4]$



Evaluation

$\mathbf{s_0} \vDash \mathbf{P}_{>0.6}\ \mathbf{F}\ \mathrm{A}$ *The probability of all paths from* $\mathbf{s_0}$ *satisfying* $\mathbf{F}$ A *is* > 0.6

iff

$\Pr\{p \mid \underline{p \text{ is a } \sigma\text{-path from } \mathbf{s_0} \text{ and } p \vDash \mathbf{F}\ \mathrm{A}}\} > 0.6$

iff

Non-probabilistic CTL/LTL/CTL*

σ-path: non-0 probability actions

$\Pr\{\mathbf{s_0 s_a},\ \mathbf{s_0 s_c}\} > 0.6$

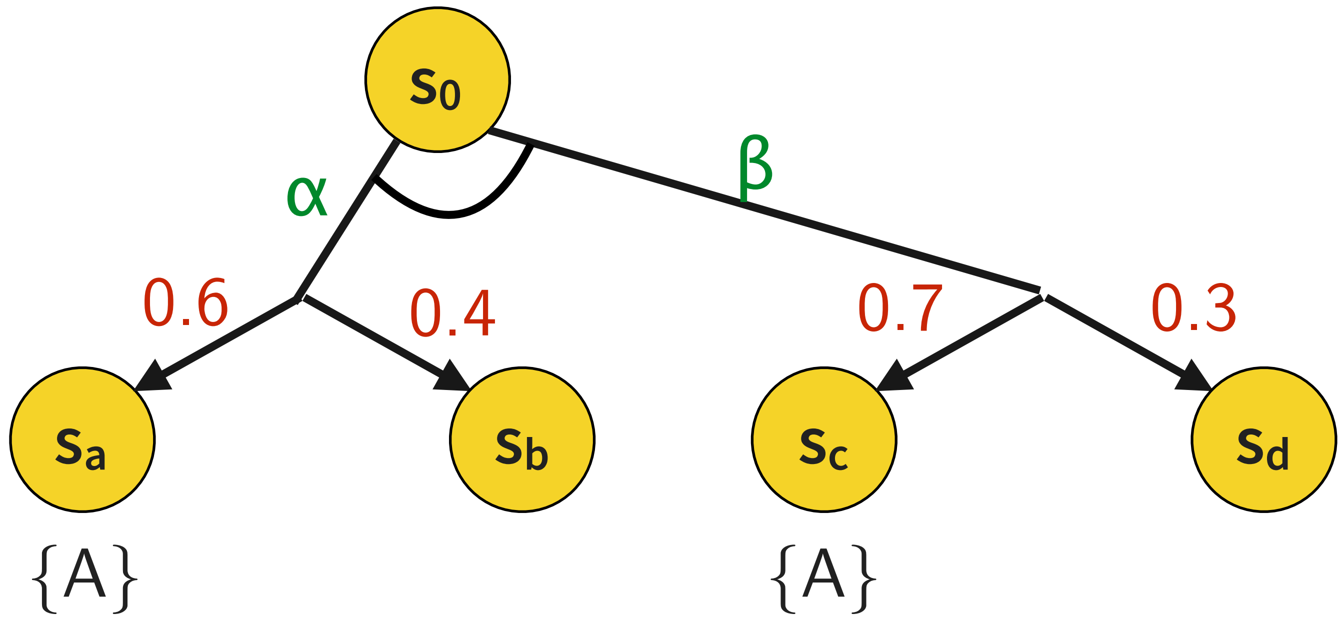
iff

$0.6 \cdot 0.6 + 0.4 \cdot 0.7 = 0.64 > 0.6$

$\leadsto$ **Synthesis: quantify over action probabilities**

Policy Synthesis

Policy σ ?

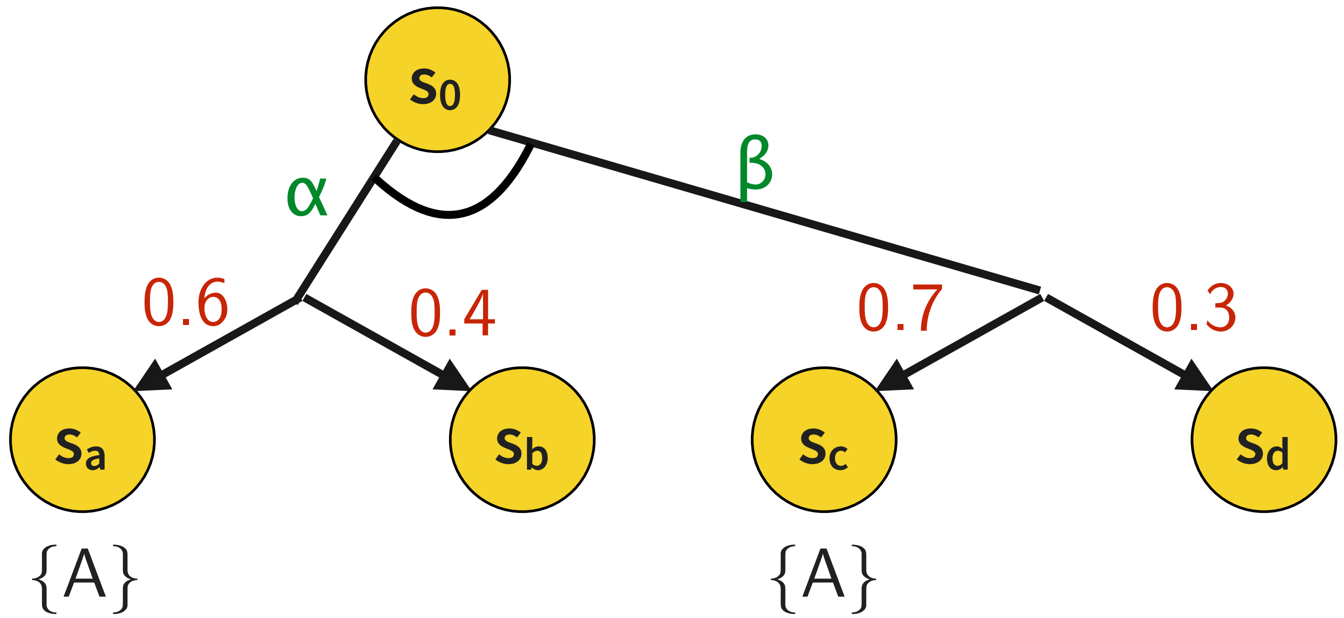


Synthesis

$\mathbf{s_0} \models \mathbf{P}_{>0.6}\ \mathbf{F}\ \mathrm{A}$ *The probability of all paths from* $\mathbf{s_0}$ *satisfying* $\mathbf{F}$ A *is* > 0.6

Policy Synthesis

Policy σ ?



Synthesis

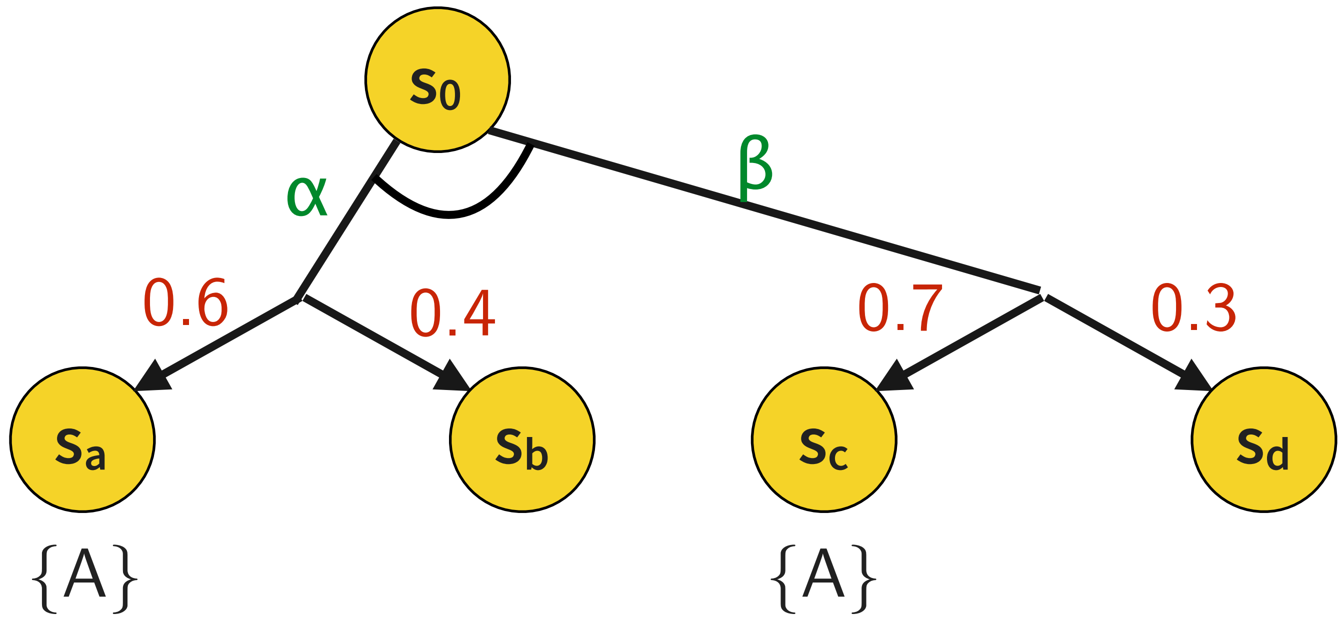
$\mathbf{s_0} \models \mathbf{P}_{>0.6}\ \mathbf{F}\ \mathrm{A}$ *The probability of all paths from* $\mathbf{s_0}$ *satisfying* $\mathbf{F}$ A *is* > 0.6

iff

$\Pr\{p \mid p \text{ is a } \sigma\text{-path from } \mathbf{s_0} \text{ and } p \models \mathbf{F}\ \mathrm{A}\} > 0.6$

Policy Synthesis

Policy σ ?



Synthesis

$\mathbf{s_0} \models \mathbf{P}_{>0.6}\ \mathbf{F}\ \mathrm{A}$ *The probability of all paths from* $\mathbf{s_0}$ *satisfying* $\mathbf{F}$ A *is* > 0.6

iff

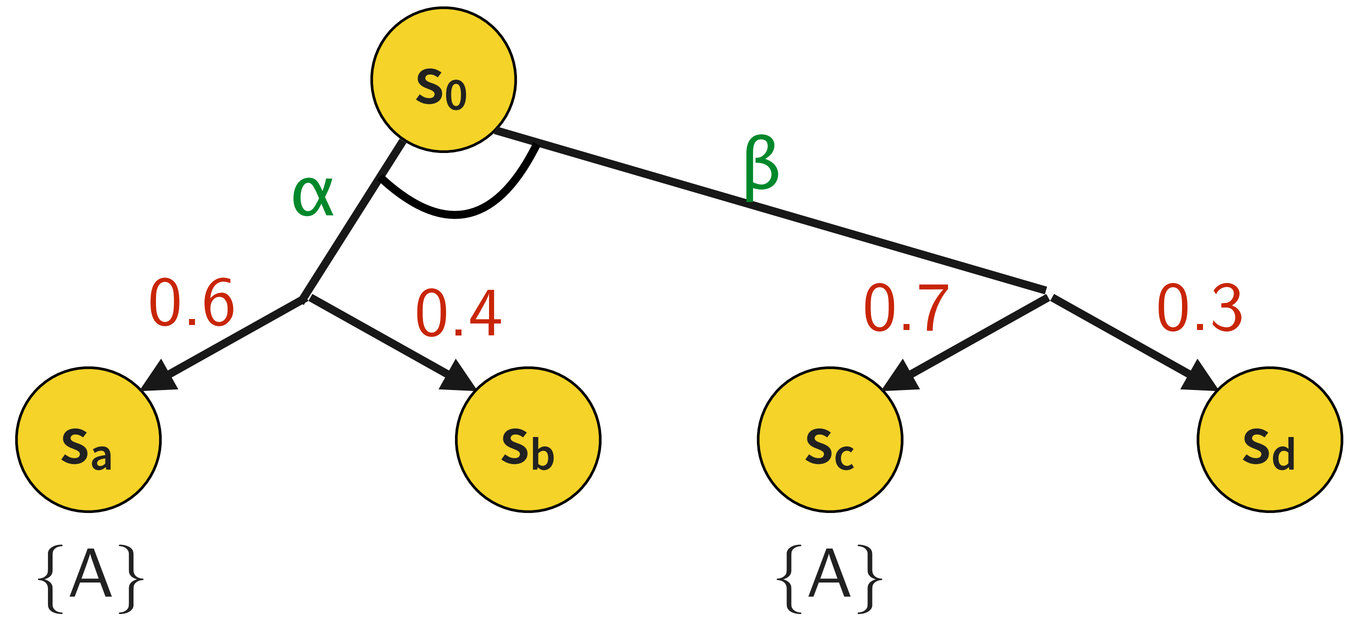
$\Pr\{p \mid p \text{ is a } \sigma\text{-path from } \mathbf{s_0} \text{ and } p \models \mathbf{F}\ \mathrm{A}\} > 0.6$

iff

$\Pr\{\mathbf{s_0 s_a},\ \mathbf{s_0 s_c}\} > 0.6$

Policy Synthesis

Policy σ ?



Synthesis

$\mathbf{s_0} \models \mathbf{P}_{>0.6}\ \mathbf{F}\ A$ *The probability of all paths from* $\mathbf{s_0}$ *satisfying* $\mathbf{F}$ A *is* > 0.6

iff

$\Pr\{p \mid p \text{ is a } \sigma\text{-path from } \mathbf{s_0} \text{ and } p \models \mathbf{F}\ A\} > 0.6$

iff

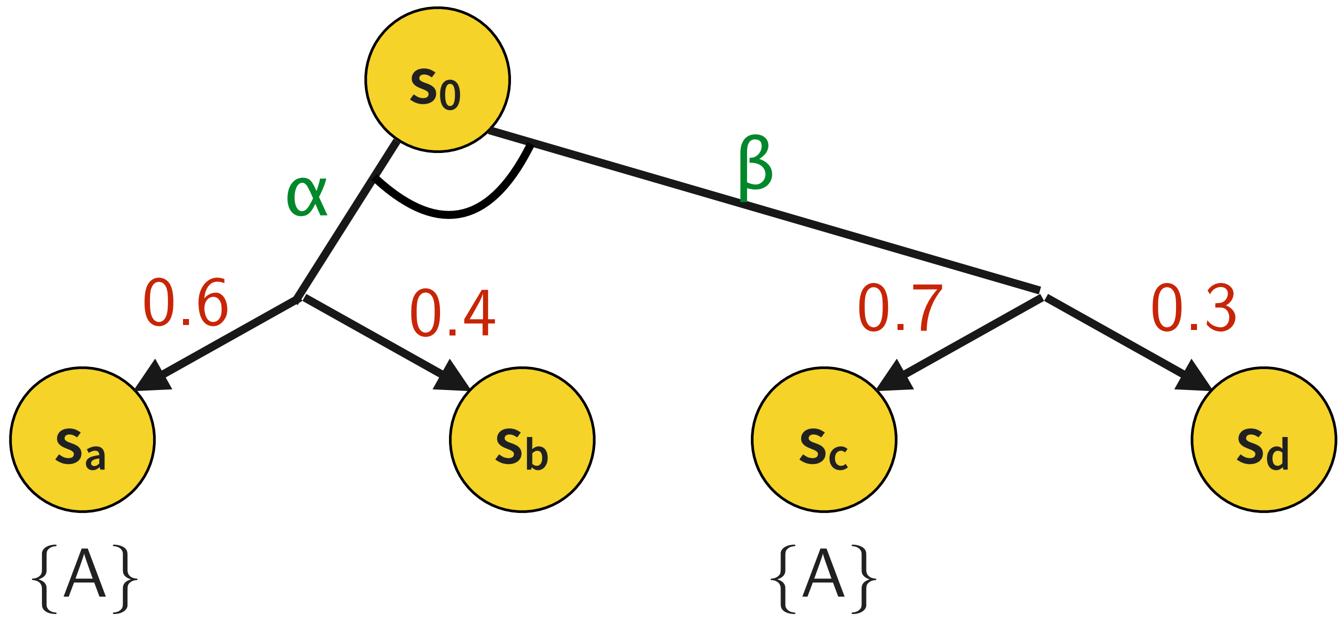
$\Pr\{\mathbf{s_0 s_a},\ \mathbf{s_0 s_c}\} > 0.6$

iff

$\mathbf{x}(\mathbf{s_0}, \alpha) \cdot 0.6 + \mathbf{x}(\mathbf{s_0}, \beta) \cdot 0.7 > 0.6$ and

Policy Synthesis

Policy σ ?



Synthesis

$s_0 \models \mathbf{P}_{>0.6}\ \mathbf{F}\ A$ *The probability of all paths from* s_0 *satisfying* $\mathbf{F}\ A$ *is* > 0.6

iff

$Pr\{p \mid p \text{ is a } \sigma\text{-path from } s_0 \text{ and } p \models \mathbf{F}\ A\} > 0.6$

iff

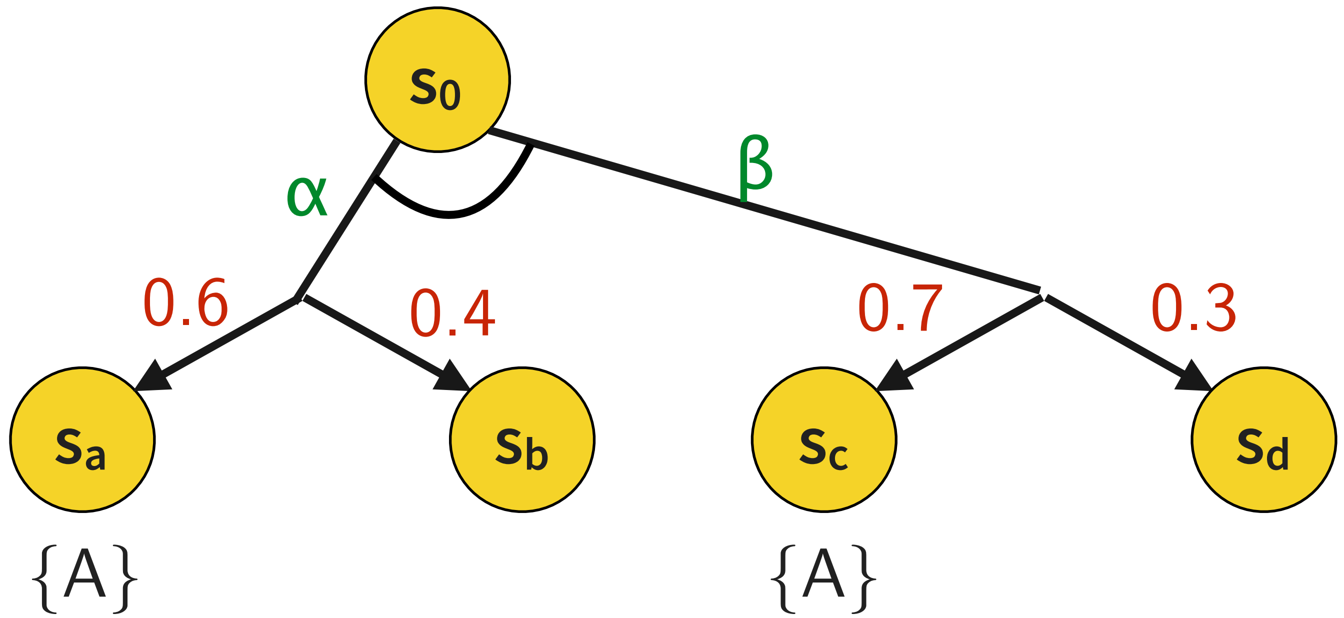
$Pr\{s_0 s_a,\ s_0 s_c\} > 0.6$

iff

$x(s_0, \alpha) \cdot 0.6 + x(s_0, \beta) \cdot 0.7 > 0.6$ and

$x(s_0, \alpha) + x(s_0, \beta) = 1$ and $x(s_0, \alpha) > 0$ and $x(s_0, \beta) > 0$

Policy Synthesis



Policy σ ?

Synthesis

$\mathbf{s_0} \models \mathbf{P}_{>0.6}\ \mathbf{F}\ A$ *The probability of all paths from* $\mathbf{s_0}$ *satisfying* $\mathbf{F}$ A *is* > 0.6

iff

$\Pr\{p \mid p \text{ is a } \sigma\text{-path from } \mathbf{s_0} \text{ and } p \models \mathbf{F}\ A\} > 0.6$

iff

$\Pr\{\mathbf{s_0 s_a},\ \mathbf{s_0 s_c}\} > 0.6$

iff

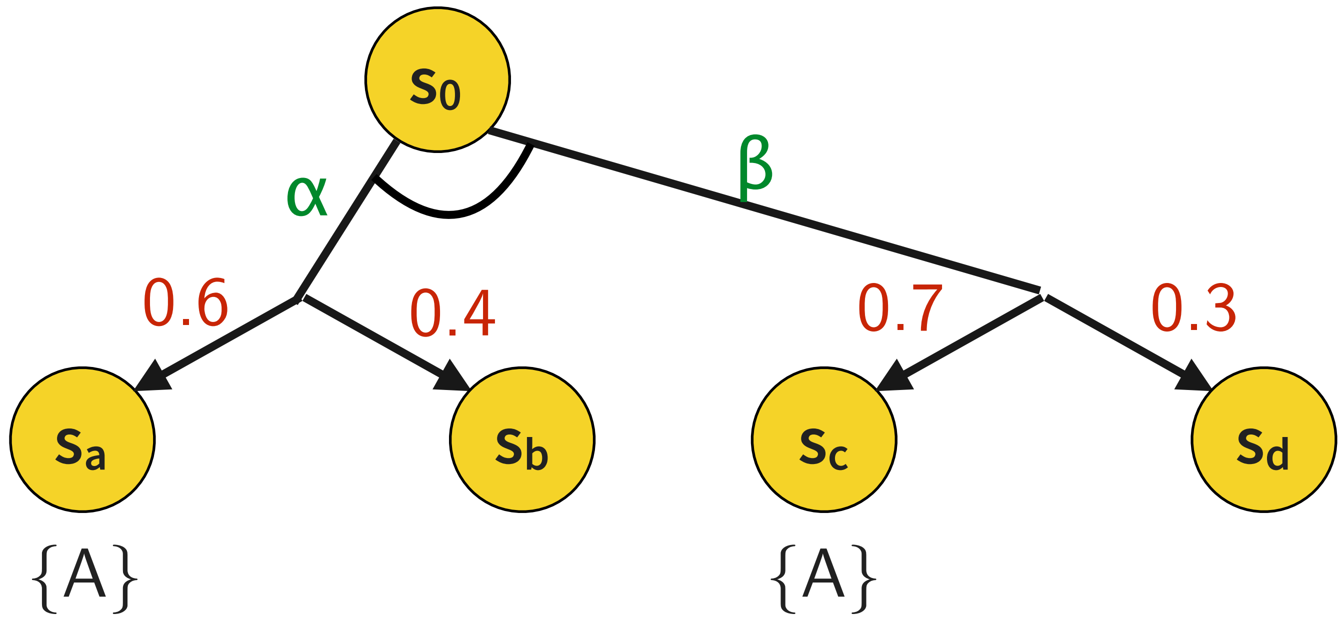
Prescribed actions, define σ-paths

$\mathbf{x}(s_0,\ \alpha) \cdot 0.6 + \mathbf{x}(s_0,\ \beta) \cdot 0.7 > 0.6$ and

$\mathbf{x}(s_0,\ \alpha) + \mathbf{x}(s_0,\ \beta) = 1$ and $\mathbf{x}(s_0,\ \alpha) > 0$ and $\mathbf{x}(s_0,\ \beta) > 0$

Policy Synthesis

Policy σ ?



Synthesis

$\mathbf{s_0} \models \mathbf{P}_{>0.6}\ \mathbf{F}\ \mathrm{A}$ *The probability of all paths from* $\mathbf{s_0}$ *satisfying* $\mathbf{F}$ A *is* > 0.6

iff

$\Pr\{p \mid p \text{ is a } \sigma\text{-path from } \mathbf{s_0} \text{ and } p \models \mathbf{F}\ \mathrm{A}\} > 0.6$

iff

$\Pr\{\mathbf{s_0 s_a},\ \mathbf{s_0 s_c}\} > 0.6$

⇝ **Tableau calculus deriving a set of (in)equations whose solutions, if any, provide a policy**

iff

Prescribed actions, define σ-paths

$\mathbf{x}(\mathbf{s_0}, \alpha) \cdot 0.6 + \mathbf{x}(\mathbf{s_0}, \beta) \cdot 0.7 > 0.6$ and

$\mathbf{x}(\mathbf{s_0}, \alpha) + \mathbf{x}(\mathbf{s_0}, \beta) = 1$ and $\mathbf{x}(\mathbf{s_0}, \alpha) > 0$ and $\mathbf{x}(\mathbf{s_0}, \beta) > 0$

Tableau Calculus

Previous slides: basic notions, intuition, trivial examples

Now: the general case, tableau calculus

Issues

- Fix a class of **target policies**: FR-policies (done)
- Fix a **logic** for target specifications: PCTL*
- **Tableau** calculus: complications
  - "Loop check" to prune infinite paths (aka "runs")
  - Special treatment of bottom strongly connected component (BSCCs)
- **Soundness and completeness proof** (see paper)

Tableau Calculus

Previous slides: basic notions, intuition, trivial examples

Now: the general case, tableau calculus

Issues

- Fix a class of **target policies**: FR-policies (done)
- Fix a **logic** for target specifications: PCTL*
- **Tableau** calculus: complications
  - "Loop check" to prune infinite paths (aka "runs")
  - Special treatment of bottom strongly connected component (BSCCs)
- **Soundness and completeness proof** (see paper)

$\leadsto$ **PCTL*, Tableau calculus**

PCTL*

PCTL* is like CTL*, but E path quantifier replaced by P

$\phi := A \mid \phi \wedge \phi \mid \neg\phi \mid \mathbf{P}_{\sim z}\,\psi$ State formula

$\psi := \phi \mid \psi \wedge \psi \mid \neg\psi \mid \mathbf{X}\,\psi \mid \psi\,\mathbf{U}\,\psi$ Path formula

where $\sim \in \{ <, \leq, >, \geq \}$ and $z \in [0..1]$

Sub-languages "probabilistic LTL" and "PCTL" obtained analogously

$\mathbf{P}_{\geq 0.8}\,\mathbf{G}\,((T > 30°) \rightarrow \mathbf{P}_{\geq 0.5}\,\mathbf{F}\,\mathbf{G}\,(T < 24°))$

With probability at least 0.8, whenever the temperature exceeds 30°
it will eventually stay below 24° with probability at least 0.5

Semantics

Parametric in policy σ

Like CTL* but patched for **P** path quantifier

$$\mathbf{s} \vDash \mathbf{P}_{\sim z}\,\psi \text{ iff } \Pr\{r \mid r \text{ is a } \sigma\text{-run from } \mathbf{s} \text{ and } r \vDash \psi\} \sim z$$

Sequent Data Structure

The tableau inference rules manipulate sequents of the following form

$$\Gamma \vdash \langle \mathbf{m}, \mathbf{s} \rangle : \Psi$$

Sequent Data Structure

The tableau inference rules manipulate sequents of the following form

$$\Gamma \vdash \langle \mathbf{m}, \mathbf{s} \rangle : \Psi$$

$\langle \mathbf{m}, \mathbf{s} \rangle$

Current policy state $\langle$*history*, *current state*$\rangle$, e.g. $\langle \boldsymbol{\epsilon}, \mathbf{s_0} \rangle$

Sequent Data Structure

The tableau inference rules manipulate sequents of the following form

$$\Gamma \vdash \langle \mathbf{m}, \mathbf{s} \rangle : \Psi$$

$\langle \mathbf{m}, \mathbf{s} \rangle$

Current policy state $\langle$*history*, *current state*$\rangle$, e.g. $\langle \boldsymbol{\epsilon}, \mathbf{s_0} \rangle$

$\Psi = \{ \psi_1, \ldots, \psi_n \}$

A set of formulas, e.g. $\{ \mathbf{P}_{>0.9}\, \mathbf{F}\, (\mathrm{Eve} \wedge \mathbf{X}\, \mathbf{P}_{>0.8}\, \mathbf{F}\, \mathrm{Done}) \}$

Sequent Data Structure

The tableau inference rules manipulate sequents of the following form

$$\Gamma \vdash \langle \mathbf{m}, \mathbf{s} \rangle : \Psi$$

$\langle \mathbf{m}, \mathbf{s} \rangle$

Current policy state $\langle$*history*, *current state*$\rangle$, e.g. $\langle \boldsymbol{\epsilon}, \mathbf{s_0} \rangle$

$\Psi = \{ \psi_1, \ldots, \psi_n \}$

A set of formulas, e.g. $\{ \mathbf{P}_{>0.9}\, \mathbf{F}\, (\text{Eve} \wedge \mathbf{X}\, \mathbf{P}_{>0.8}\, \mathbf{F}\, \text{Done}) \}$

$\langle \mathbf{m}, \mathbf{s} \rangle : \Psi$

Stands for $\{ r \mid r$ is a run from $\langle \mathbf{m}, \mathbf{s} \rangle$ and $r \vDash \bigwedge \Psi$

Sequent Data Structure

The tableau inference rules manipulate sequents of the following form

$$\Gamma \vdash \langle \mathbf{m}, \mathbf{s} \rangle : \Psi$$

$\langle \mathbf{m}, \mathbf{s} \rangle$

Current policy state $\langle$*history*, *current state*$\rangle$, e.g. $\langle \boldsymbol{\epsilon}, \mathbf{s_0} \rangle$

$\Psi = \{ \psi_1, \ldots, \psi_n \}$

A set of formulas, e.g. $\{ \mathbf{P}_{>0.9}\, \mathbf{F}\, (\text{Eve} \wedge \mathbf{X}\, \mathbf{P}_{>0.8}\, \mathbf{F}\, \text{Done}) \}$

$\langle \mathbf{m}, \mathbf{s} \rangle : \Psi$

Stands for $\{ r \mid r \text{ is a run from } \langle \mathbf{m}, \mathbf{s} \rangle \text{ and } r \models \bigwedge \Psi$

Γ

"Program": set of (non-linear) constraints on $\langle \mathbf{m}, \mathbf{s} \rangle : \Psi$, e.g.

$\mathbf{x}_{\langle \mathbf{m}, \mathbf{s} \rangle}{}^{\Psi} > 0.5$ *The probability of* $\langle \mathbf{m}, \mathbf{s} \rangle : \Psi$ *is* > 0.5

Sequent Data Structure

The tableau inference rules manipulate sequents of the following form

$$\Gamma \vdash \langle \mathbf{m}, \mathbf{s} \rangle : \Psi$$

$\langle \mathbf{m}, \mathbf{s} \rangle$

Current policy state $\langle$*history*, *current state*$\rangle$, e.g. $\langle \boldsymbol{\epsilon}, \mathbf{s_0} \rangle$

$\Psi = \{ \psi_1, \ldots, \psi_n \}$

A set of formulas, e.g. $\{ \mathbf{P}_{>0.9}\, \mathbf{F}\, (\text{Eve} \land \mathbf{X}\, \mathbf{P}_{>0.8}\, \mathbf{F}\, \text{Done}) \}$

$\langle \mathbf{m}, \mathbf{s} \rangle : \Psi$

Stands for $\{ r \mid r$ is a run from $\langle \mathbf{m}, \mathbf{s} \rangle$ and $r \models \bigwedge\Psi$

Γ

$\leadsto$ **Tableau: derive definitions $\mathbf{x}_{\langle \mathbf{m}, \mathbf{s} \rangle}^{\Psi} \doteq \ldots$?**

"Program": set of (non-linear) constraints on $\langle \mathbf{m}, \mathbf{s} \rangle : \Psi$, e.g.

$\mathbf{x}_{\langle \mathbf{m}, \mathbf{s} \rangle}^{\Psi} > 0.5$ *The probability of* $\langle \mathbf{m}, \mathbf{s} \rangle : \Psi$ *is* > 0.5

Tableau Derivations

Initialization

Given state formula ϕ, e.g. $\mathbf{P}_{>0.9}\ \mathbf{F}\ (\mathrm{Eve} \wedge \mathbf{X}\ \mathbf{P}_{>0.8}\ \mathbf{F}\ \mathrm{Done})$

Initial tableau with root node $\mathbf{x}_{\langle \epsilon,\ \mathbf{s0}\rangle}{}^{\{\phi\}} \doteq 1 \quad \vdash \langle \boldsymbol{\epsilon},\ \mathbf{s_0}\rangle : \{\phi\}$

Obligation to derive a satisfiable Γ that specifies σ and value for $\mathbf{x}_{\langle \epsilon,\ \mathbf{s0}\rangle}{}^{\{\phi\}}$

Inference rules invariant

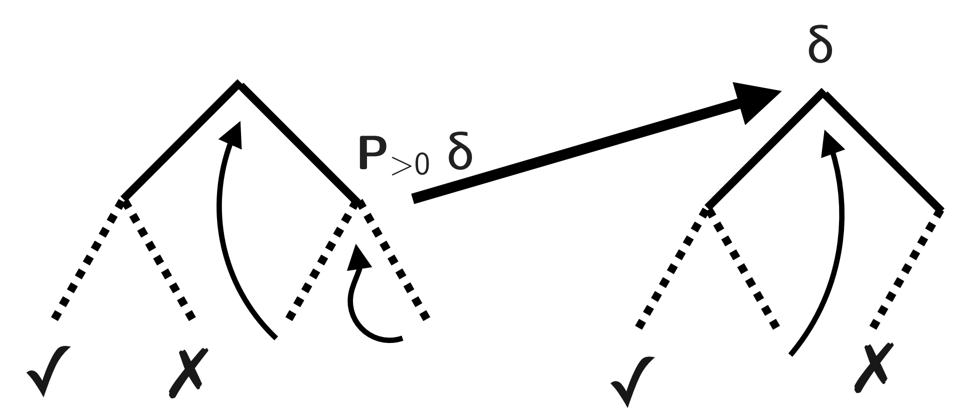
$$\frac{\Gamma \vdash \langle \mathbf{m},\ \mathbf{s}\rangle : \Psi}{\Gamma,\ \mathbf{x}_{\langle \mathbf{m},\ \mathbf{s}\rangle}{}^{\Psi} \doteq \ldots \vdash \Psi'}$$

$\langle \mathbf{m},\ \mathbf{s}\rangle : \Psi$ is eliminated by

adding to Γ an equation $\mathbf{x}_{\langle \mathbf{m},\ \mathbf{s}\rangle}{}^{\Psi} \doteq \ldots$

for the probability of $\langle \mathbf{m},\ \mathbf{s}\rangle : \Psi$

Derivation structure



Sub-derivations by nested **P**-formulas

Final Γ accumulated from sub-derivations

Solution of final Γ provides policy σ

Some Inference Rules

Rules for classical formulas

$$\checkmark \quad \frac{\Gamma \vdash \langle m, s \rangle : \emptyset}{\Gamma, x^{\emptyset}_{\langle m,s \rangle} \doteq 1 \vdash \checkmark}$$

$$\text{✗} \quad \frac{\Gamma \vdash \langle m, s \rangle : \{\psi\} \uplus \Psi}{\Gamma, x^{\{\psi\} \uplus \Psi}_{\langle m,s \rangle} \doteq 0 \vdash \text{✗}} \begin{cases} \text{if } \psi \text{ is clas-} \\ \text{sical and} \\ L(s) \not\models \psi \end{cases}$$

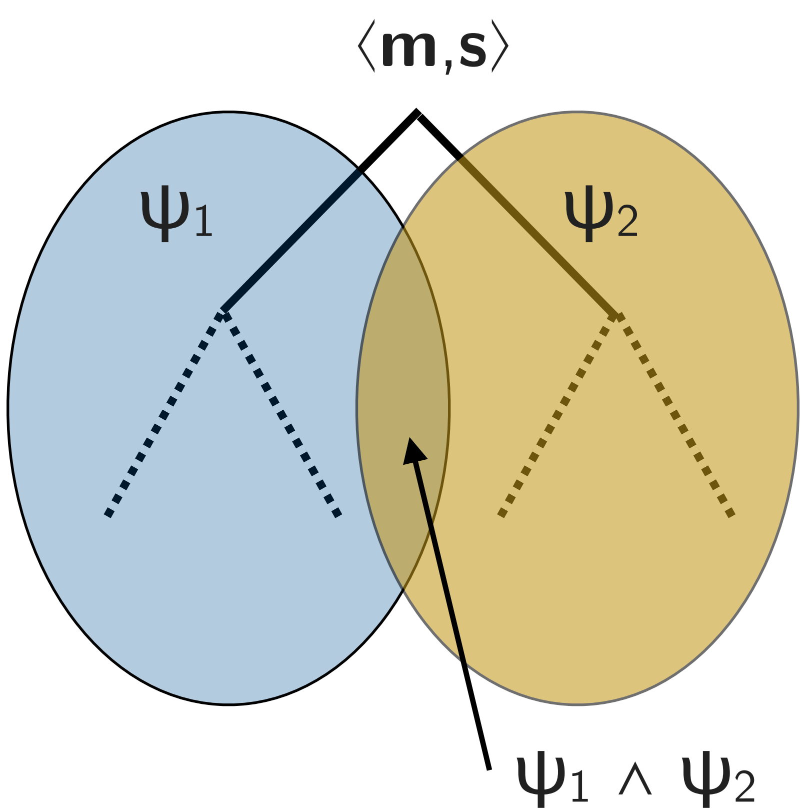
$$\top \quad \frac{\Gamma \vdash \langle m, s \rangle : \{\psi\} \uplus \Psi}{\Gamma, \gamma_{\text{one}} \vdash \langle m, s \rangle : \Psi} \begin{cases} \text{if } \psi \text{ is clas-} \\ \text{sical and} \\ L(s) \models \psi \end{cases}$$

Some Inference Rules

Rules for conjunctions (1)

$$\wedge \quad \frac{\Gamma \vdash \langle m, s\rangle : \{\psi_1 \wedge \psi_2\} \uplus \Psi}{\Gamma, \gamma_{\text{one}} \vdash \langle m, s\rangle : \{\psi_1, \psi_2\} \cup \Psi}$$

$\langle \mathbf{m},\mathbf{s}\rangle$: $\psi_1 \wedge \psi_2$ is intersection of $\langle \mathbf{m},\mathbf{s}\rangle$: ψ_1 and $\langle \mathbf{m},\mathbf{s}\rangle$: ψ_1



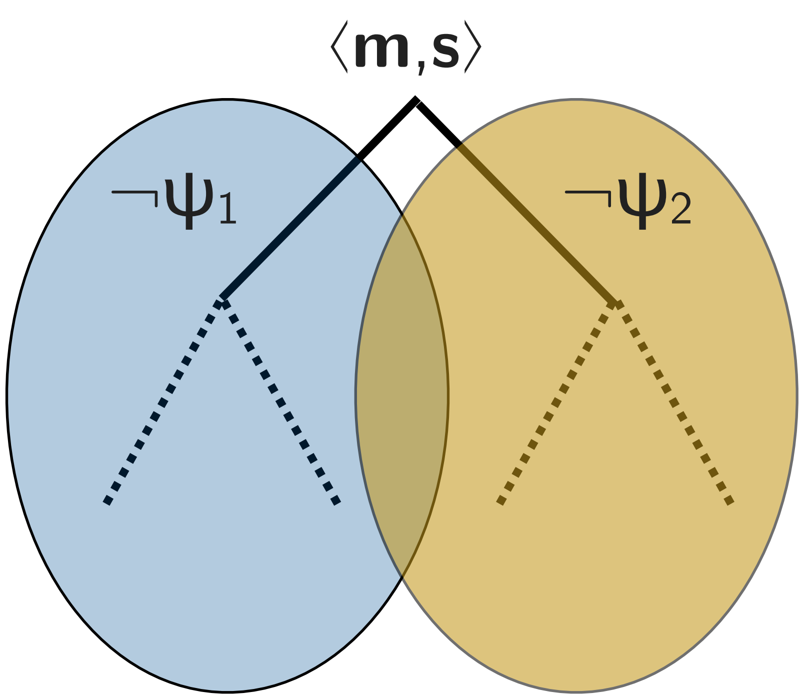
Some Inference Rules

Rules for conjunctions (2) (disjunctions, really)

$$\neg\wedge \quad \frac{\Gamma \vdash \langle m, s\rangle : \{\neg(\psi_1 \wedge \psi_2)\} \uplus \Psi}{\Gamma \vdash \langle m, s\rangle : \{\neg\psi_1\} \cup \Psi \quad \cup \quad \Gamma, \gamma \vdash \langle m, s\rangle : \{\psi_1, \neg\psi_2\} \cup \Psi}$$

$$\text{where } \gamma \;=\; x_{\langle m,s\rangle}^{\{\neg(\psi_1\wedge\psi_2)\}\uplus\Psi} \doteq x_{\langle m,s\rangle}^{\{\neg\psi_1\}\cup\Psi} + x_{\langle m,s\rangle}^{\{\psi_1,\neg\psi_2\}\cup\Psi}$$

Branching on disjoint union $\neg(\psi_1 \wedge \psi_2) \equiv \neg\psi_1 \vee \neg\psi_2 \equiv \neg\psi_1 \vee (\psi_1 \wedge \neg\psi_2)$



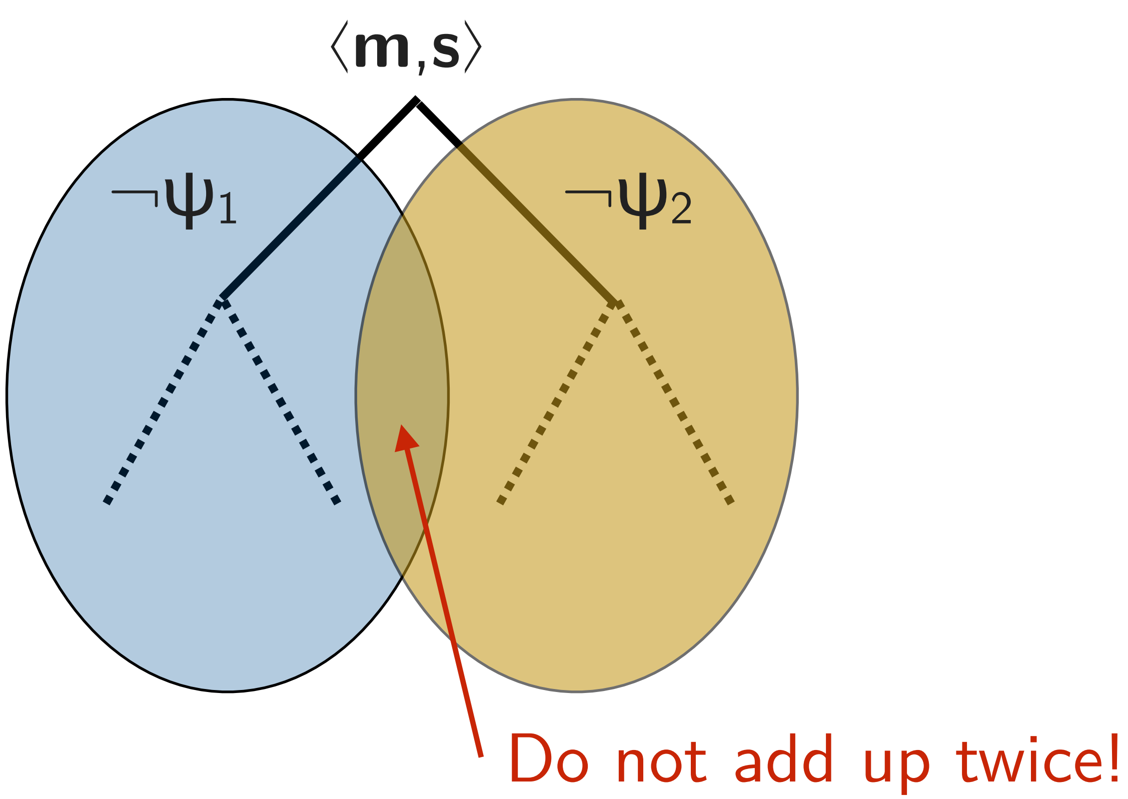
Some Inference Rules

Rules for conjunctions (2) (disjunctions, really)

$$\neg\wedge \quad \frac{\Gamma \vdash \langle m, s\rangle : \{\neg(\psi_1 \wedge \psi_2)\} \uplus \Psi}{\Gamma \vdash \langle m, s\rangle : \{\neg\psi_1\} \cup \Psi \quad \cup \quad \Gamma, \gamma \vdash \langle m, s\rangle : \{\psi_1, \neg\psi_2\} \cup \Psi}$$

$$\text{where } \gamma \; = \; x_{\langle m,s\rangle}^{\{\neg(\psi_1 \wedge \psi_2)\} \uplus \Psi} \doteq x_{\langle m,s\rangle}^{\{\neg\psi_1\} \cup \Psi} + x_{\langle m,s\rangle}^{\{\psi_1, \neg\psi_2\} \cup \Psi}$$

Branching on disjoint union $\neg(\psi_1 \wedge \psi_2) \equiv \neg\psi_1 \vee \neg\psi_2 \equiv \neg\psi_1 \vee (\psi_1 \wedge \neg\psi_2)$



Some Inference Rules

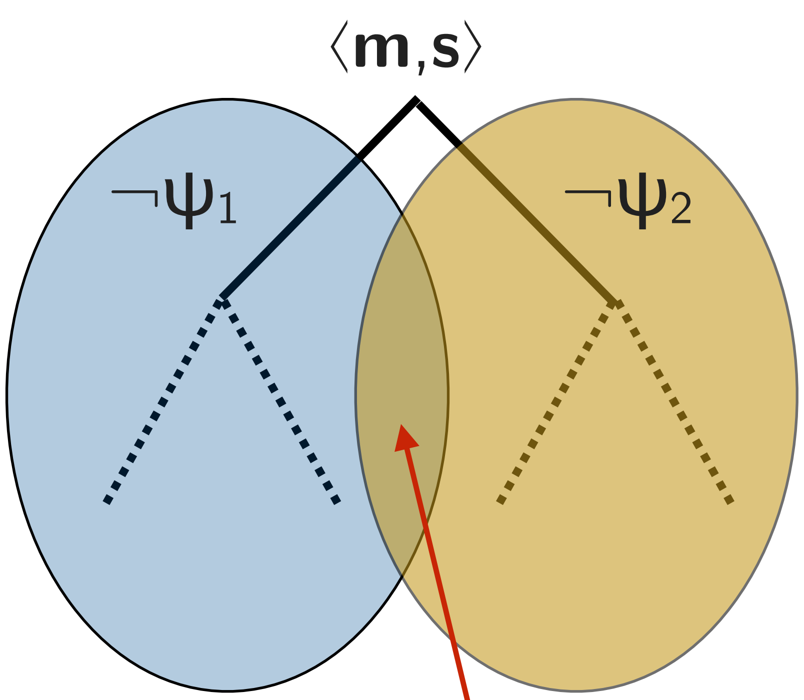
Rules for conjunctions (2) (disjunctions, really)

$$\neg\wedge \quad \frac{\Gamma \vdash \langle m, s\rangle : \{\neg(\psi_1 \wedge \psi_2)\} \uplus \Psi}{\Gamma \vdash \langle m, s\rangle : \{\neg\psi_1\} \cup \Psi \quad \cup \quad \Gamma, \gamma \vdash \langle m, s\rangle : \{\psi_1, \neg\psi_2\} \cup \Psi}$$

$$\text{where } \gamma \;=\; x^{\{\neg(\psi_1\wedge\psi_2)\}\uplus\Psi}_{\langle m,s\rangle} \doteq x^{\{\neg\psi_1\}\cup\Psi}_{\langle m,s\rangle} + x^{\{\psi_1,\neg\psi_2\}\cup\Psi}_{\langle m,s\rangle}$$

Need **both** branches

Branching on disjoint union $\neg(\psi_1 \wedge \psi_2) \equiv \neg\psi_1 \vee \neg\psi_2 \equiv \neg\psi_1 \vee (\psi_1 \wedge \neg\psi_2)$



Do not add up twice!

Some Inference Rules

Rules for P-formulas

Similar to classical state formula, but ...

$$\mathbf{P}\ \frac{\Gamma \vdash \langle \mathbf{m},\ \mathbf{s} \rangle : \{\ \mathbf{P}_{\sim z}\ \psi\ \} \uplus \Psi}{\text{“}\langle \mathbf{m},\ \mathbf{s} \rangle \models \mathbf{P}_{\sim z}\ \psi\text{”} \qquad \text{OR} \qquad \text{“}\langle \mathbf{m},\ \mathbf{s} \rangle \not\models \mathbf{P}_{\sim z}\ \psi\text{”}}$$

Cannot know at this stage if $\langle \mathbf{m},\ \mathbf{s} \rangle \models \mathbf{P}_{\sim z}\ \psi$ holds or not - may depend on final Γ

Hence guess by branching out and invoke tableau with respective constraint

$\mathbf{x}_{\langle \mathbf{m},\ \mathbf{s} \rangle} \sim z$ or $\mathbf{x}_{\langle \mathbf{m},\ \mathbf{s} \rangle} \not\sim z$

In any case simplify premise with decision made to make progress

Some Inference Rules

Rules for U-formulas

Basically: unfold using equivalences

$$\psi_1 \,\mathbf{U}\, \psi_2 \equiv \psi_2 \vee (\psi_1 \wedge \mathbf{X}\,(\psi_1 \,\mathbf{U}\, \psi_2))$$

$$\neg(\psi_1 \,\mathbf{U}\, \psi_2) \equiv \neg\psi_2 \wedge (\neg\psi_1 \vee \mathbf{X}\,\neg(\psi_1 \,\mathbf{U}\, \psi_2))$$

Disjoint union again

$$\mathbf{U}\ \frac{\Gamma \vdash \langle m, s\rangle : \{\psi_1 \,\mathbf{U}\, \psi_2\} \uplus \Psi}{\Gamma \vdash \langle m, s\rangle : \{\psi_2\} \cup \Psi \qquad \cup \qquad \Gamma, \gamma \vdash \langle m, s\rangle : \{\psi_1, \neg\psi_2, \mathbf{X}\,(\psi_1 \,\mathbf{U}\, \psi_2)\} \cup \Psi}$$

$$\text{where } \gamma \;=\; x_{\langle m,s\rangle}^{\{\psi_1 \,\mathbf{U}\, \psi_2\} \uplus \Psi} \doteq x_{\langle m,s\rangle}^{\{\psi_2\} \cup \Psi} + x_{\langle m,s\rangle}^{\{\psi_1, \neg\psi_2, \mathbf{X}\,(\psi_1 \,\mathbf{U}\, \psi_2)\} \cup \Psi}$$

$$\neg\mathbf{U}\ \frac{\Gamma \vdash \langle m, s\rangle : \{\neg(\psi_1 \,\mathbf{U}\, \psi_2)\} \uplus \Psi}{\Gamma \vdash \langle m, s\rangle : \{\neg\psi_1, \neg\psi_2\} \cup \Psi \quad \cup \quad \Gamma, \gamma \vdash \langle m, s\rangle : \{\psi_1, \neg\psi_2, \mathbf{X}\,\neg(\psi_1 \,\mathbf{U}\, \psi_2)\} \cup \Psi}$$

$$\text{where } \gamma \;=\; x_{\langle m,s\rangle}^{\{\neg(\psi_1 \,\mathbf{U}\, \psi_2)\} \uplus \Psi} \doteq x_{\langle m,s\rangle}^{\{\neg\psi_1, \neg\psi_2\} \cup \Psi} + x_{\langle m,s\rangle}^{\{\psi_1, \neg\psi_2, \mathbf{X}\,\neg(\psi_1 \,\mathbf{U}\, \psi_2)\} \cup \Psi}$$

Some Inference Rules

Rules for U-formulas

Basically: unfold using equivalences

$$\psi_1 \,\mathbf{U}\, \psi_2 \equiv \psi_2 \lor (\psi_1 \land \mathbf{X}\,(\psi_1 \,\mathbf{U}\, \psi_2))$$

$$\neg(\psi_1 \,\mathbf{U}\, \psi_2) \equiv \neg\psi_2 \land (\neg\psi_1 \lor \mathbf{X}\,\neg(\psi_1 \,\mathbf{U}\, \psi_2))$$

Disjoint union again

$$\mathbf{U}\;\frac{\Gamma \vdash \langle m, s\rangle : \{\psi_1 \,\mathbf{U}\, \psi_2\} \uplus \Psi}{\Gamma \vdash \langle m, s\rangle : \{\psi_2\} \cup \Psi \qquad \cup \qquad \Gamma, \gamma \vdash \langle m, s\rangle : \{\psi_1, \neg\psi_2, \mathbf{X}\,(\psi_1 \,\mathbf{U}\, \psi_2)\} \cup \Psi}$$

$$\text{where } \gamma \;=\; x_{\langle m,s\rangle}^{\{\psi_1 \,\mathbf{U}\, \psi_2\}\uplus\Psi} \doteq x_{\langle m,s\rangle}^{\{\psi_2\}\cup\Psi} + x_{\langle m,s\rangle}^{\{\psi_1,\neg\psi_2,\mathbf{X}\,(\psi_1 \,\mathbf{U}\, \psi_2)\}\cup\Psi}$$

$$\neg\mathbf{U}\;\frac{\Gamma \vdash \langle m, s\rangle : \{\neg(\psi_1 \,\mathbf{U}\, \psi_2)\} \uplus \Psi}{\Gamma \vdash \langle m, s\rangle : \{\neg\psi_1, \neg\psi_2\} \cup \Psi \quad \cup \quad \Gamma, \gamma \vdash \langle m, s\rangle : \{\psi_1, \neg\psi_2, \mathbf{X}\,\neg(\psi_1 \,\mathbf{U}\, \psi_2)\} \cup \Psi}$$

$$\text{where } \gamma \;=\; x_{\langle m,s\rangle}^{\{\neg(\psi_1 \,\mathbf{U}\, \psi_2)\}\uplus\Psi} \doteq x_{\langle m,s\rangle}^{\{\neg\psi_1,\neg\psi_2\}\cup\Psi} + x_{\langle m,s\rangle}^{\{\psi_1,\neg\psi_2,\mathbf{X}\,\neg(\psi_1 \,\mathbf{U}\, \psi_2)\}\cup\Psi}$$

→ At this stage premise Ψ is $\{\ \mathbf{X}\ \psi_1, \ldots, \mathbf{X}\ \psi_n\ \}$

Some Inference Rules

$\mathbf{X}$ { $\psi_1,\ldots,\psi_n$ } shorthand for poised { $\mathbf{X}\ \psi_1,\ldots,\mathbf{X}\ \psi_n$ }

Rules for X-formulas

Advance to the next state by expansion

$$\mathbf{X}\quad \frac{\Gamma \vdash \langle \mathbf{m}, \mathbf{s} \rangle : \mathbf{X}\ \psi}{\text{“}\langle \Delta(\mathbf{m}, \mathbf{s}), \mathbf{s_1} \rangle \models \psi\text{”} \quad \cup \quad \text{“}\langle \Delta(\mathbf{m}, \mathbf{s}), \mathbf{s_n} \rangle \models \psi\text{”}}$$

where

$\mathbf{s}_1$ … $\mathbf{s}_n$ are all “prescribed” successor states of $\mathbf{s}$, i.e,
successor states reachable with non-0 probability

Some Inference Rules

$\mathbf{X}\ \{\ \psi_1,\ldots,\psi_n\ \}$ shorthand for poised $\{\ \mathbf{X}\ \psi_1,\ldots,\mathbf{X}\ \psi_n\ \}$

Rules for X-formulas

Advance to the next state by expansion

$$\mathbf{X}\quad \frac{\Gamma \vdash \langle \mathbf{m},\ \mathbf{s}\rangle : \mathbf{X}\ \psi}{\text{“}\langle \Delta(\mathbf{m},\ \mathbf{s}),\ \mathbf{s_1}\rangle \models \psi\text{”} \quad \cup \quad \text{“}\langle \Delta(\mathbf{m},\ \mathbf{s}),\ \mathbf{s_n}\rangle \models \psi\text{”}}$$

where

$\mathbf{s}_1$ … $\mathbf{s}_n$ are all "prescribed" successor states of $\mathbf{s}$, i.e,
successor states reachable with non-0 probability

Requires guessing rule for action probabilities
"$\mathbf{x}_{\langle \mathbf{m},\ \mathbf{s}\rangle}{}^{\boldsymbol{\alpha}} > 0$" OR "$\mathbf{x}_{\langle \mathbf{m},\ \mathbf{s}\rangle}{}^{\boldsymbol{\alpha}} \doteq 0$"

Some Inference Rules

$\mathbf{X}$ { $\psi_1,\dots,\psi_n$ } shorthand for poised { $\mathbf{X}\ \psi_1,\dots,\mathbf{X}\ \psi_n$ }

Rules for X-formulas

Advance to the next state by expansion

$$\mathbf{X}\quad \frac{\Gamma \vdash \langle \mathbf{m},\ \mathbf{s}\rangle : \mathbf{X}\ \psi}{\text{“}\langle \Delta(\mathbf{m},\ \mathbf{s}),\ \mathbf{s_1}\rangle \models \psi\text{”} \quad \cup \quad \text{“}\langle \Delta(\mathbf{m},\ \mathbf{s}),\ \mathbf{s_n}\rangle \models \psi\text{”}}$$

where

$\mathbf{s}_1$ … $\mathbf{s}_n$ are all “prescribed” successor states of $\mathbf{s}$, i.e,
successor states reachable with non-0 probability

Requires guessing rule for action probabilities
“$\mathbf{x}_{\langle \mathbf{m},\ \mathbf{s}\rangle}{}^{\boldsymbol{\alpha}} > 0$” OR “$\mathbf{x}_{\langle \mathbf{m},\ \mathbf{s}\rangle}{}^{\boldsymbol{\alpha}} \doteq 0$”

→ **The X-rule is not applied in case of a “loop”**

Loop Check

Adapted from LTL satisfiability tableau by Mark Reynolds

Recurring eventualities **G** (**F A** $\wedge$ **F B** $\wedge$ **F C**)

Loop Check

Adapted from LTL satisfiability tableau by Mark Reynolds

Recurring eventualities $\mathbf{G}\ (\mathbf{F\ A} \wedge \mathbf{F\ B} \wedge \mathbf{F\ C})$

$$\langle \mathbf{m}, \mathbf{s} \rangle : \mathbf{X\ F\ A}, \mathbf{X\ F\ B}, \mathbf{X\ F\ C}, \ldots$$

Loop Check

Adapted from LTL satisfiability tableau by Mark Reynolds

Recurring eventualities $\mathbf{G}\ (\mathbf{F\ A} \wedge \mathbf{F\ B} \wedge \mathbf{F\ C})$

$=: \mathbf{X}\ \Psi$

$\langle \mathbf{m}, \mathbf{s} \rangle : \mathbf{X\ F\ A}, \mathbf{X\ F\ B}, \mathbf{X\ F\ C}, \ldots$

Loop Check

Adapted from LTL satisfiability tableau by Mark Reynolds

Recurring eventualities $\mathbf{G}\ (\mathbf{F}\ \mathbf{A} \wedge \mathbf{F}\ \mathbf{B} \wedge \mathbf{F}\ \mathbf{C})$

$=: \mathbf{X}\ \Psi$

$$\langle \mathbf{m}, \mathbf{s} \rangle : \mathbf{X}\ \mathbf{F}\ \mathbf{A},\ \mathbf{X}\ \mathbf{F}\ \mathbf{B},\ \mathbf{X}\ \mathbf{F}\ \mathbf{C},\ \ldots$$

Loop Check

Adapted from LTL satisfiability tableau by Mark Reynolds

Recurring eventualities **G** (**F A** $\wedge$ **F B** $\wedge$ **F C**)

$=:$ **X** Ψ

$\langle$**m**, **s**$\rangle$: **X F A**, **X F B**, **X F C**, ...

"**A**"

Loop Check

Adapted from LTL satisfiability tableau by Mark Reynolds

Recurring eventualities $\mathbf{G}\ (\mathbf{F}\ \mathbf{A} \wedge \mathbf{F}\ \mathbf{B} \wedge \mathbf{F}\ \mathbf{C})$

$=: \mathbf{X}\ \Psi$

$\langle \mathbf{m}, \mathbf{s} \rangle : \mathbf{X}\ \mathbf{F}\ \mathbf{A}, \mathbf{X}\ \mathbf{F}\ \mathbf{B}, \mathbf{X}\ \mathbf{F}\ \mathbf{C}, \ldots$

“**A**”

$\langle \mathbf{m}, \mathbf{s} \rangle : \mathbf{X}\ \Psi$

Loop Check

Adapted from LTL satisfiability tableau by Mark Reynolds

Recurring eventualities **G** (**F A** $\wedge$ **F B** $\wedge$ **F C**)

=: **X** Ψ

$\langle$**m**, **s**$\rangle$: **X F A**, **X F B**, **X F C**, ...

“**A**”

$\langle$**m**, **s**$\rangle$: **X** Ψ

“**A**”

$\langle$**m**, **s**$\rangle$: **X** Ψ

Loop Check

Adapted from LTL satisfiability tableau by Mark Reynolds

Recurring eventualities $\mathbf{G}\ (\mathbf{F}\ \mathbf{A} \wedge \mathbf{F}\ \mathbf{B} \wedge \mathbf{F}\ \mathbf{C})$

$=: \mathbf{X}\ \psi$

$\langle \mathbf{m}, \mathbf{s} \rangle : \mathbf{X}\ \mathbf{F}\ \mathbf{A}, \mathbf{X}\ \mathbf{F}\ \mathbf{B}, \mathbf{X}\ \mathbf{F}\ \mathbf{C}, \ldots$

"**A**"

$\langle \mathbf{m}, \mathbf{s} \rangle : \mathbf{X}\ \psi$

No progress made

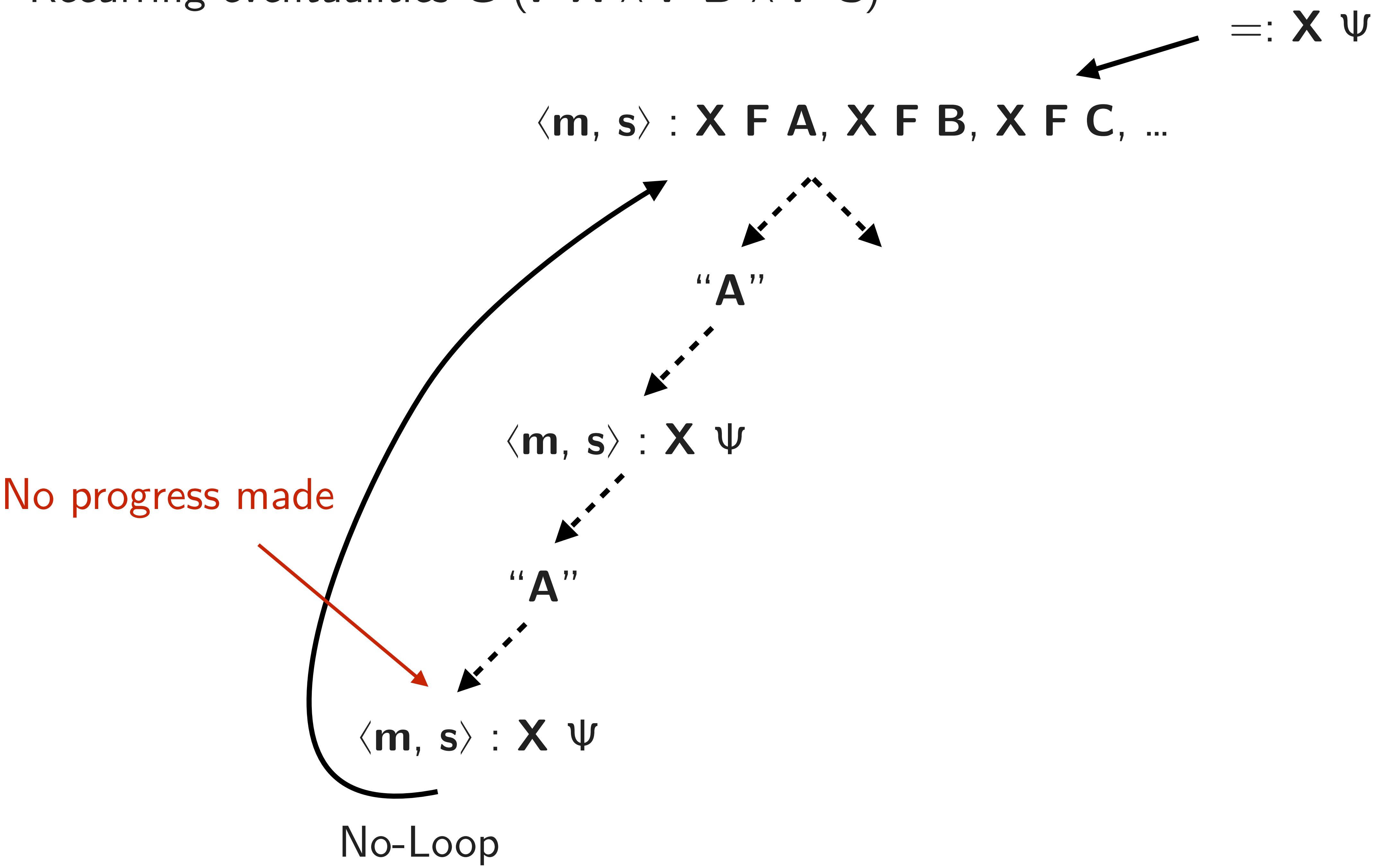
"**A**"

$\langle \mathbf{m}, \mathbf{s} \rangle : \mathbf{X}\ \psi$

Loop Check

Adapted from LTL satisfiability tableau by Mark Reynolds

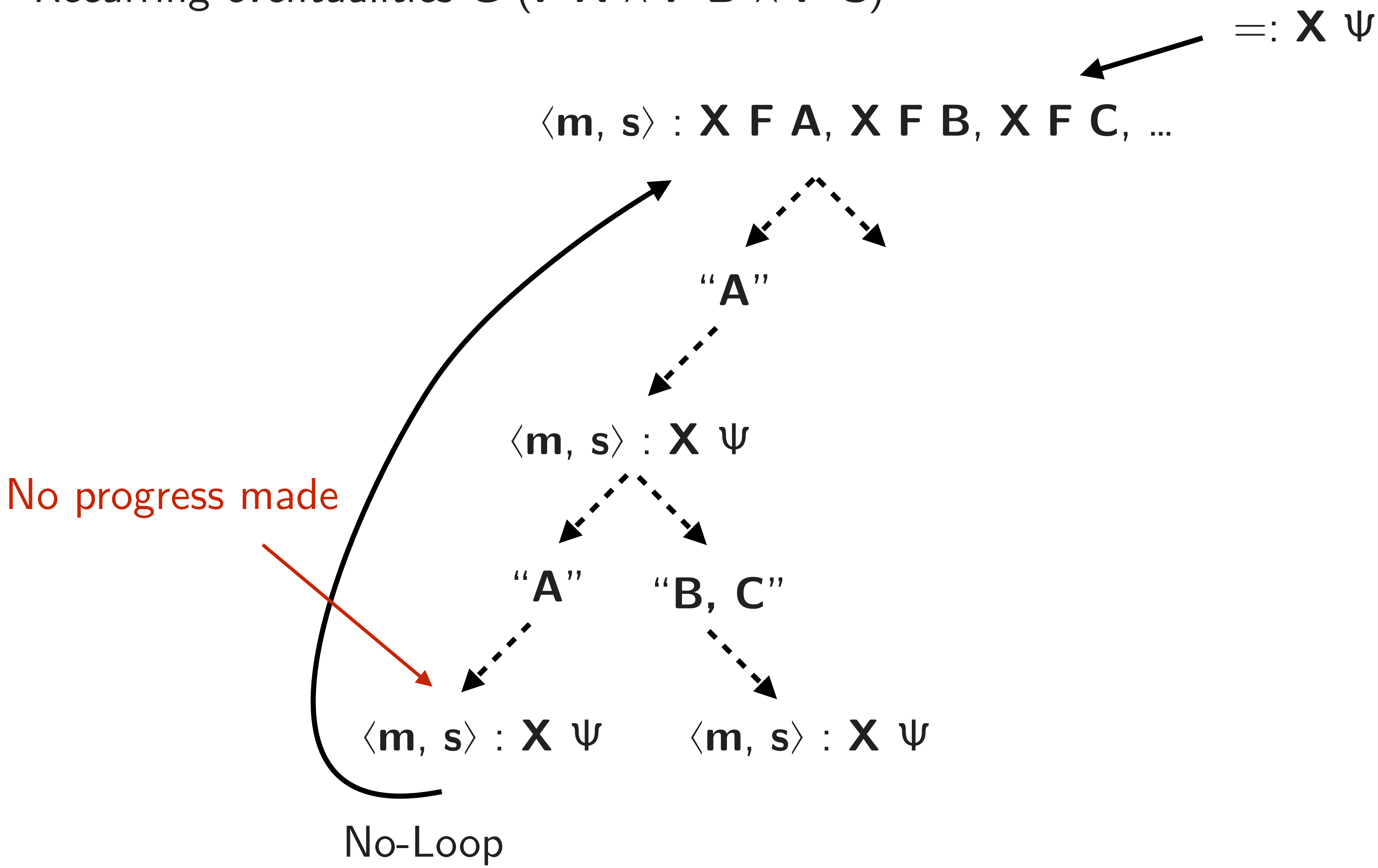
Recurring eventualities **G** (**F A** $\wedge$ **F B** $\wedge$ **F C**)



Loop Check

Adapted from LTL satisfiability tableau by Mark Reynolds

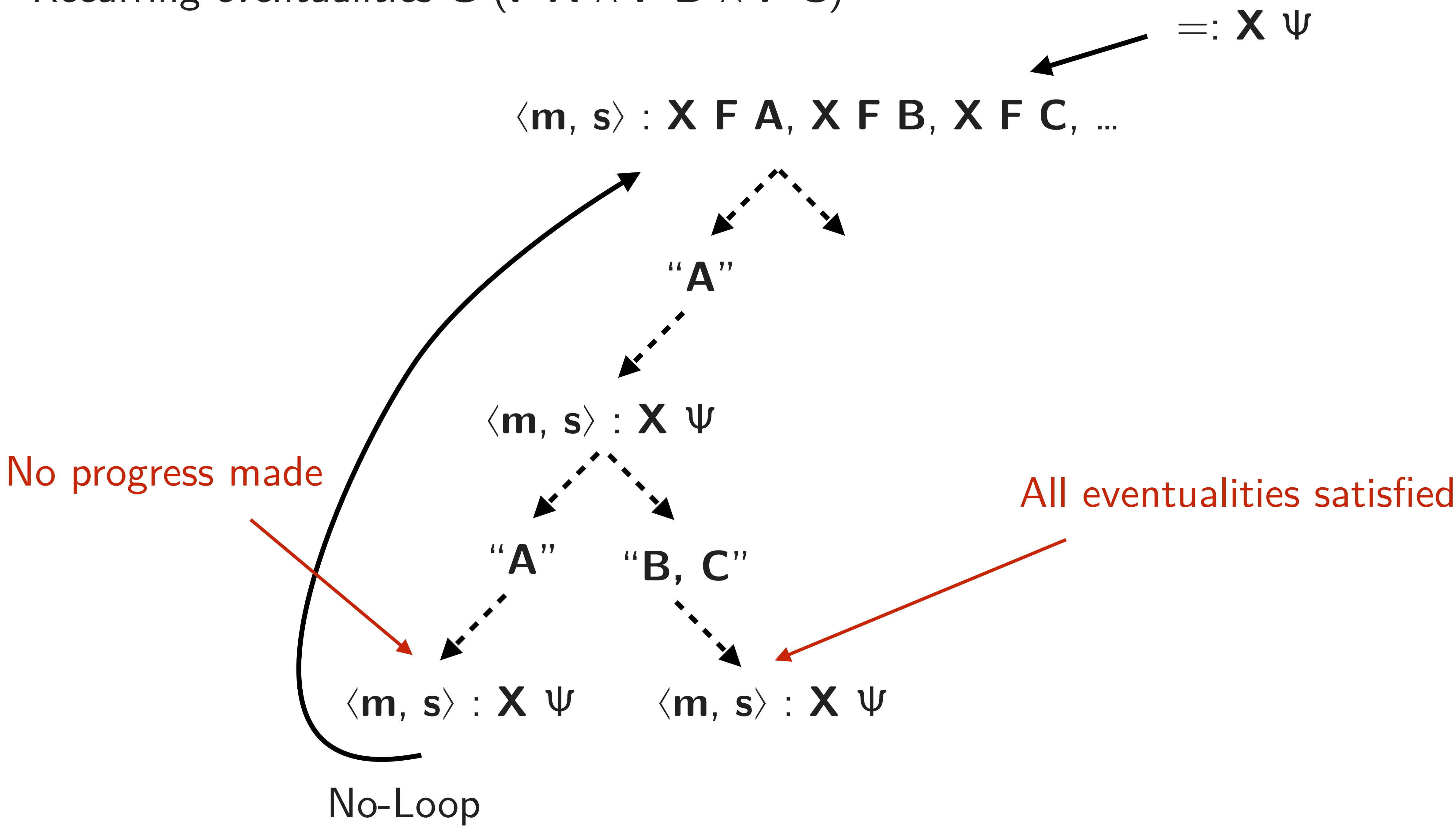
Recurring eventualities $\mathbf{G}\ (\mathbf{F\ A} \wedge \mathbf{F\ B} \wedge \mathbf{F\ C})$



Loop Check

Adapted from LTL satisfiability tableau by Mark Reynolds

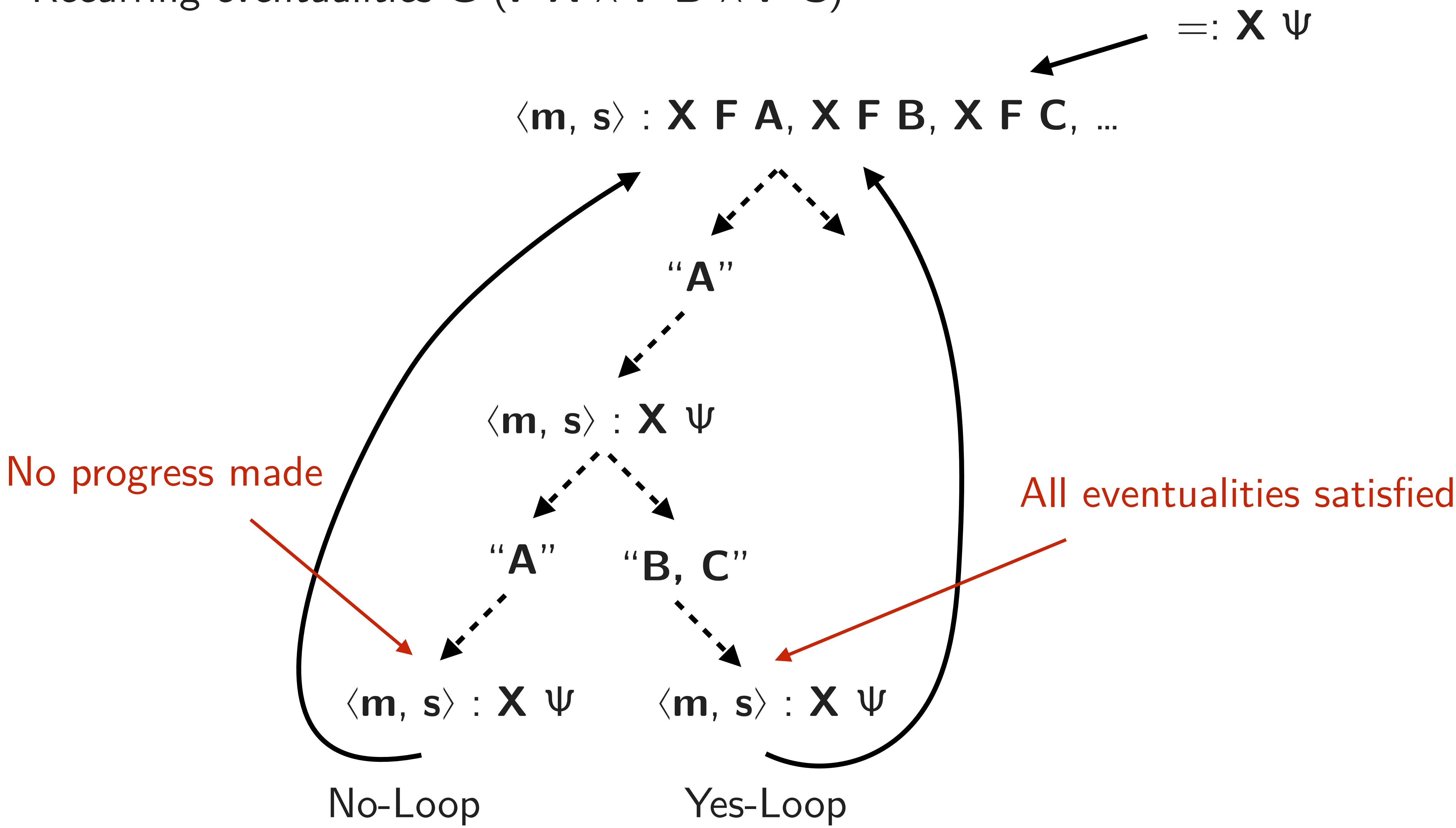
Recurring eventualities **G** (**F A** ∧ **F B** ∧ **F C**)



Loop Check

Adapted from LTL satisfiability tableau by Mark Reynolds

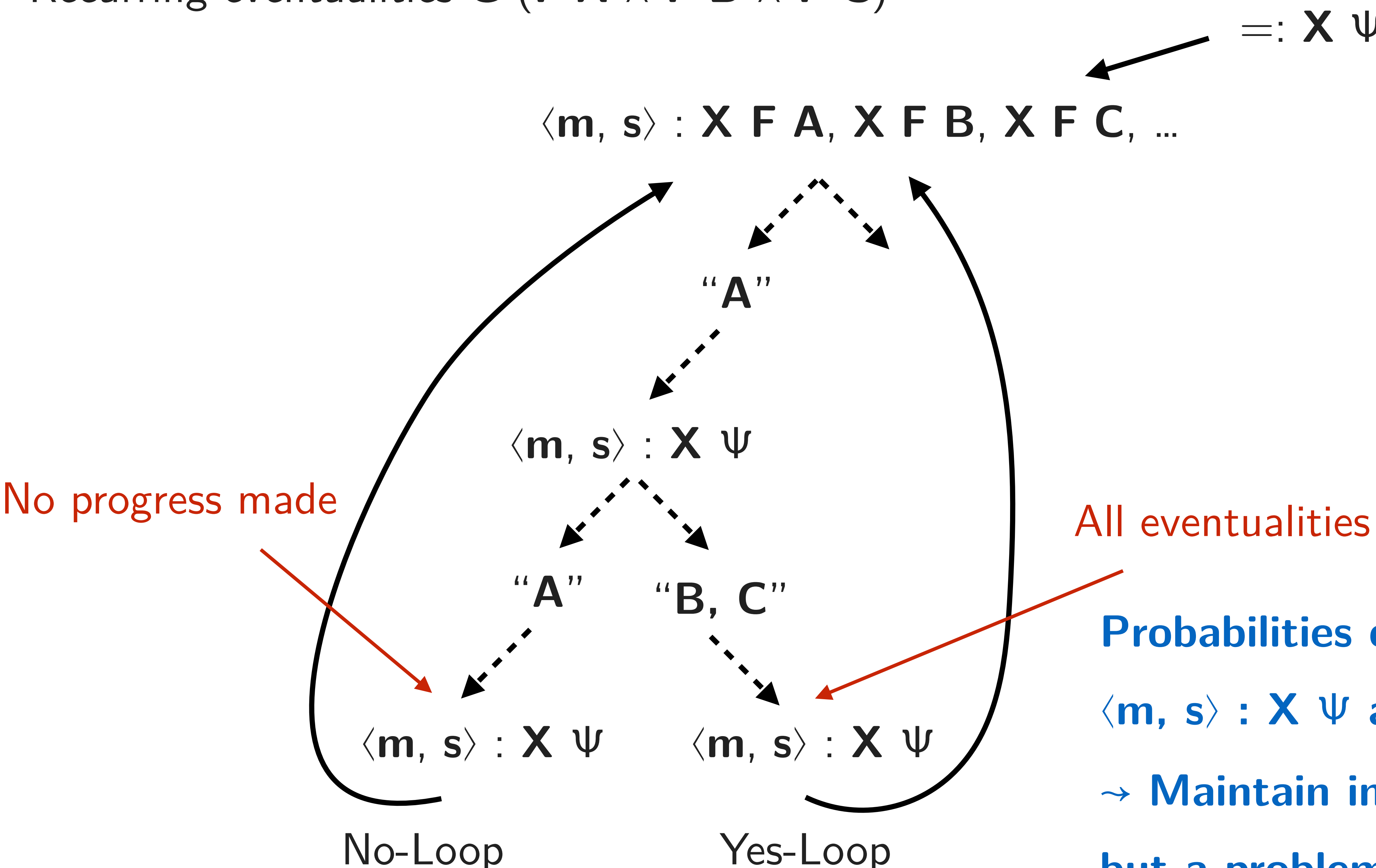
Recurring eventualities **G** (**F A** ∧ **F B** ∧ **F C**)



Loop Check

Adapted from LTL satisfiability tableau by Mark Reynolds

Recurring eventualities **G** (**F A** $\wedge$ **F B** $\wedge$ **F C**)



Probabilities of all

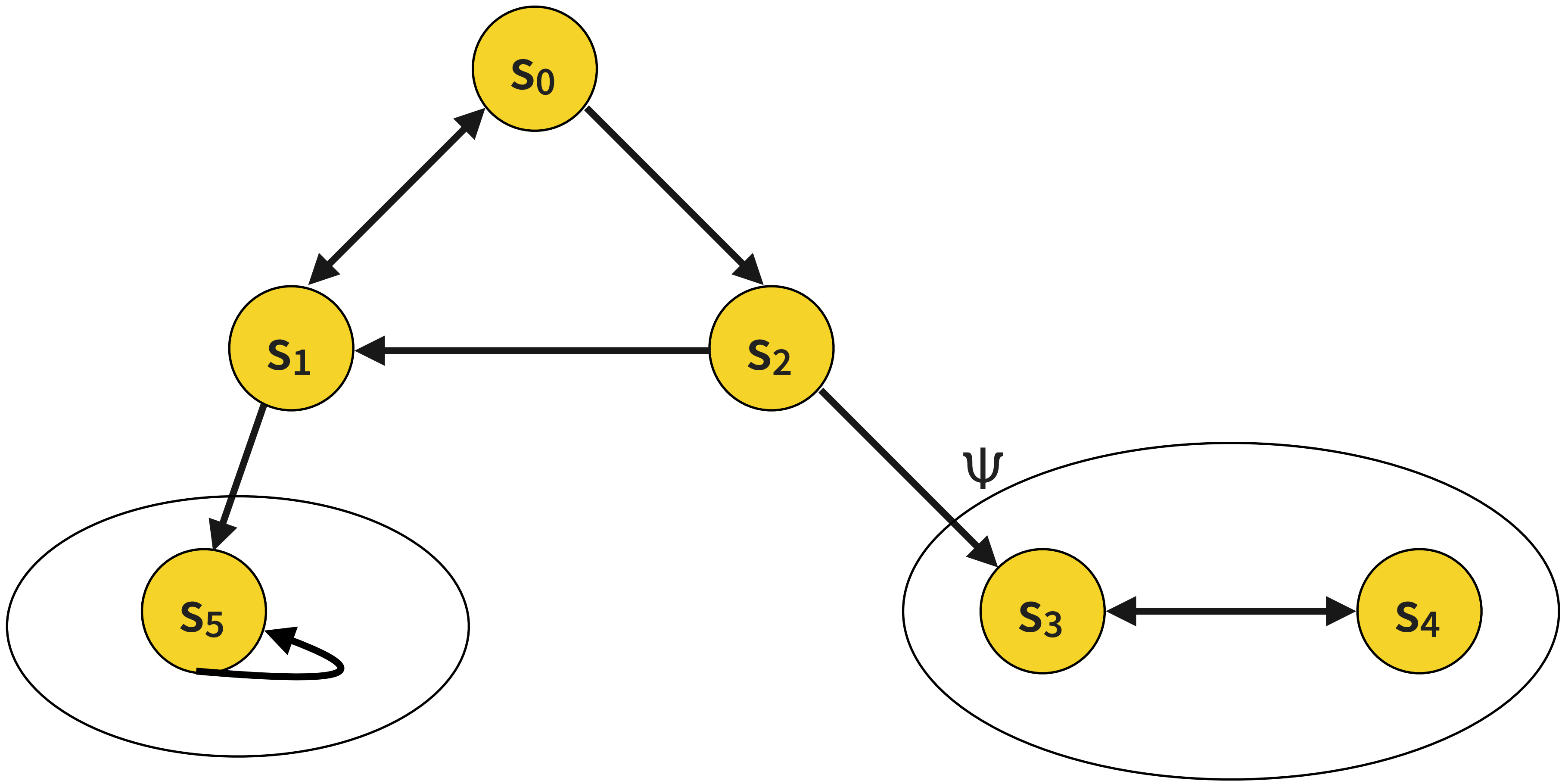
⟨m, s⟩ : X ψ are the same

→ Maintain invariant,

but a problem remains

Bottom Strongly Connected Components (BSCCs)

BSCC a reachable sub-graph that is impossible to leave



Problem: if tableau contains BSCC for problematic Ψ

then Γ underspecifies probability: "$\mathbf{x}_{\mathbf{s3}}{}^{\Psi} \doteq \mathbf{x}_{\mathbf{s3}}{}^{\Psi}$"

Solution: if have Yes-Loop then add $\mathbf{x}_{\mathbf{s3}}{}^{\Psi} \doteq 1$ to Γ else add $\mathbf{x}_{\mathbf{s3}}{}^{\Psi} \doteq 0$ to Γ

Conclusion

- Presented a tableau calculus for policy synthesis

  Many details left out
- Very expressive target specification language: PCTL*
- Had to restrict to policies with finite-memory fixed a priori to get decidability
- Novelty: no other algorithm for policy synthesis under stated conditions
- Novelty: explores **reachable** states “only”

  Traditional synthesis algorithms are based on automata