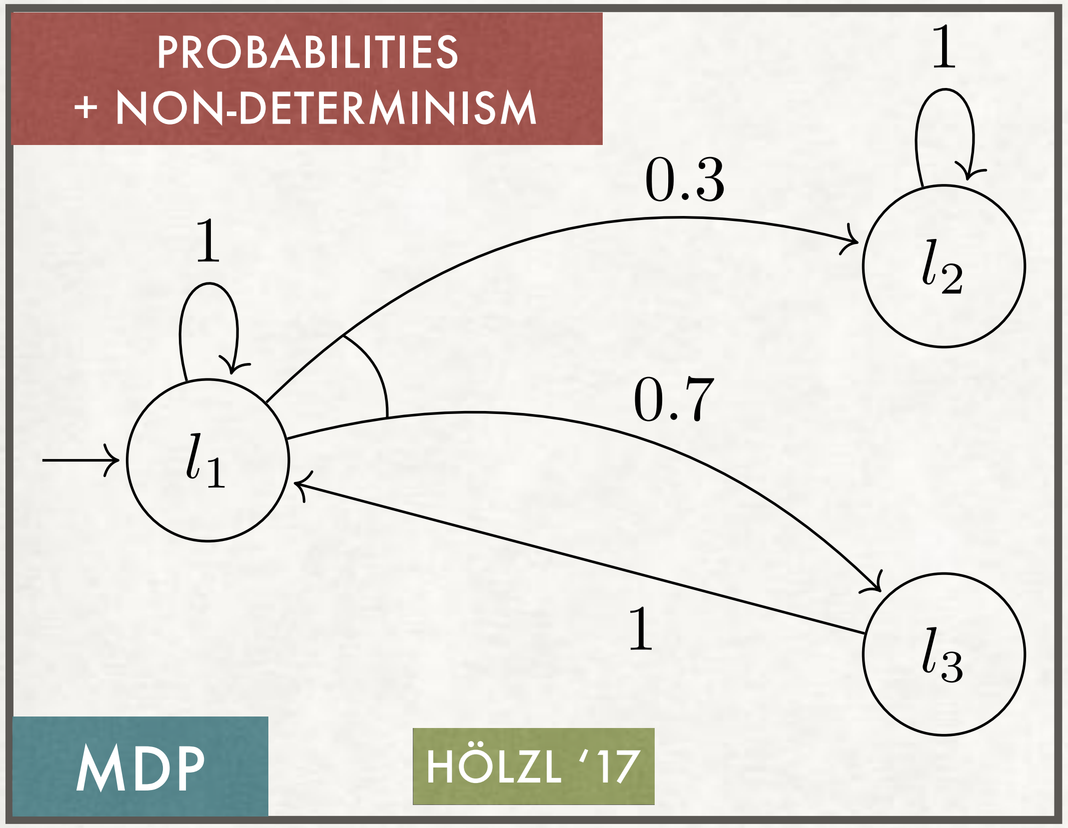
MDP + TA = PTA

PROBABILISTIC TIMED AUTOMATA, FORMALIZED

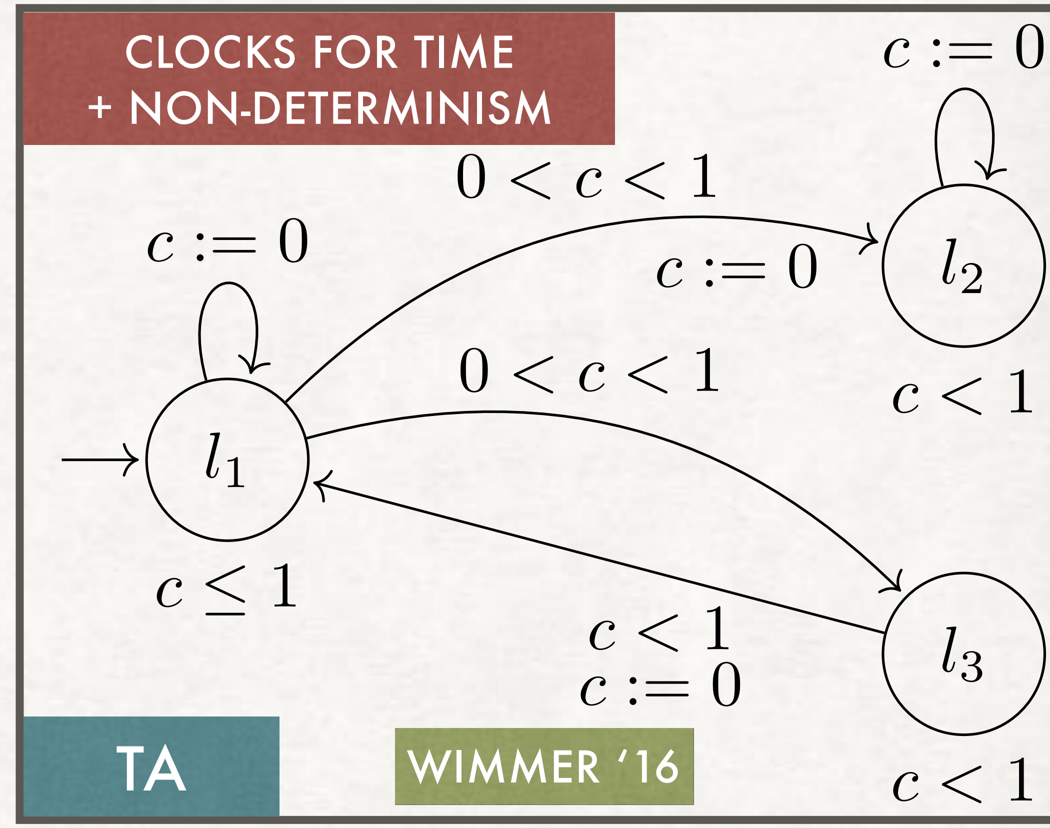
SIMON WIMMER & JOHANNES HÖLZL

TU MUNICH & VU AMSTERDAM

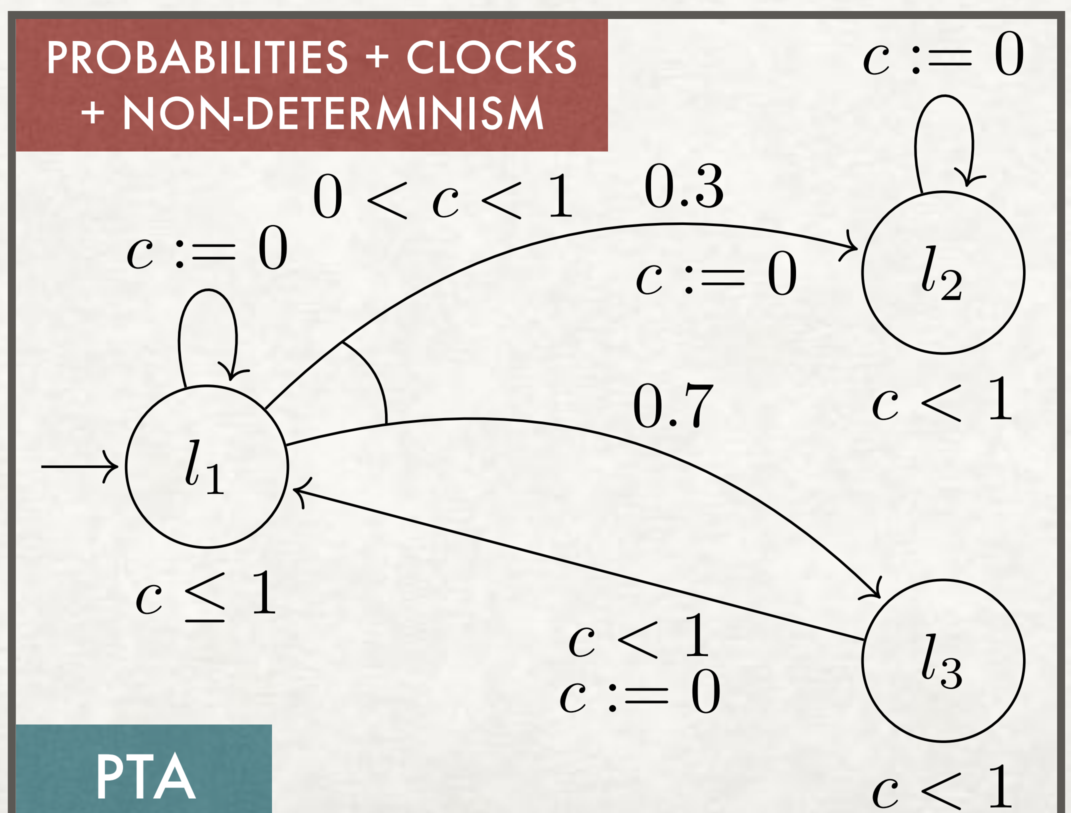
ON ONE SLIDE



+



=

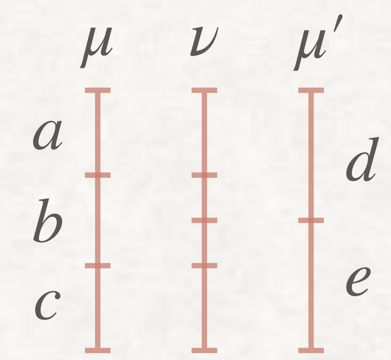


WHAT IS THE MAX./MIN. PROBABILITY TO REACH l_2 AMONG ALL ADVERSARIES?

PROBABILITY THEORY IN ISABELLE/HOL

QUICK TOUR

- Discrete distributions: probability mass function $\mu :: \sigma\,\mathsf{pmf}$
  - Constructed over type $\sigma \Rightarrow \mathbb{R}_{\geq 0}$
  - Countable support $\{x \mid \mu\, x \neq 0\}$ and $\sum_{x :: \sigma} \mu\, x = 1$
  - Functorial structure: $(\mathsf{map}_{\mathsf{pmf}}\, f \mu)\, y = \mu\, \{x \mid f\, x = y\}$ and $(\mathsf{ret}_{\mathsf{pmf}}\, x)\, x = 1$
- Probabilistic coupling: $\mathsf{rel}_{\mathsf{pmf}}\, R\, \mu\, \mu'$ iff there exists ν s.t.
  - $\mu = \mathsf{map}_{\mathsf{pmf}}\, \pi_1\, \nu$ and $\mu' = \mathsf{map}_{\mathsf{pmf}}\, \pi_2\, \nu$
  - Support of ν is a subset of R



$$R = \{(a, d), (b, d), (b, e), (c, e)\}$$

MARKOV DECISION PROCESSES

QUICK TOUR

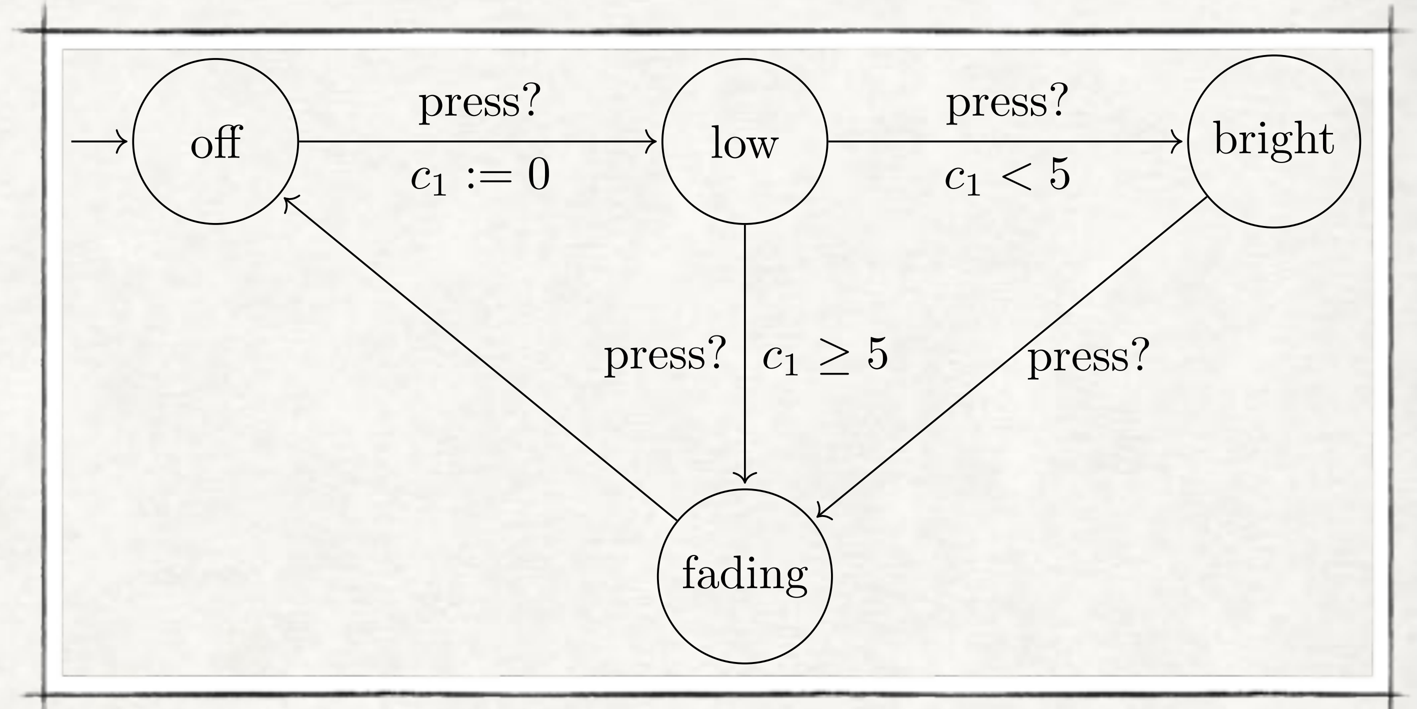
- Markov Chains
  - Transition System $K :: \sigma \Rightarrow \sigma\,\text{pmf}$ ("kernel")
  - Trace Space $T_K\, s\, (x_0 \cdots x_n) = K\, s\, x_0 * \cdots * K\, x_{n-1}\, x_n$

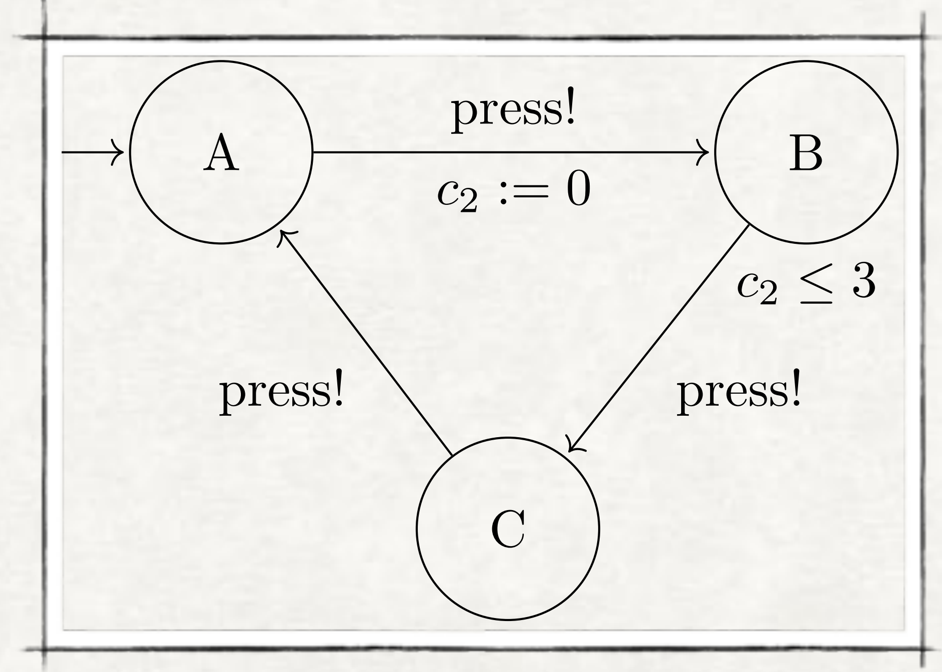
    SET OF STATE TRACES STARTING WITH $x_0 \cdots x_n$
- Markov Decision Processes
  - Add non-determinism $K :: \sigma \Rightarrow \sigma\,\text{pmf}\,\text{set}$
  - Coinductive configurations resolve non-determinism: state σ, action $\sigma\,\text{pmf}$, continuation $\sigma \Rightarrow \sigma\,\text{cfg}$
  - MC on configurations: $K_c :: \sigma\,\text{cfg} \Rightarrow \sigma\,\text{cfg}\,\text{pmf}$

TIMED AUTOMATA

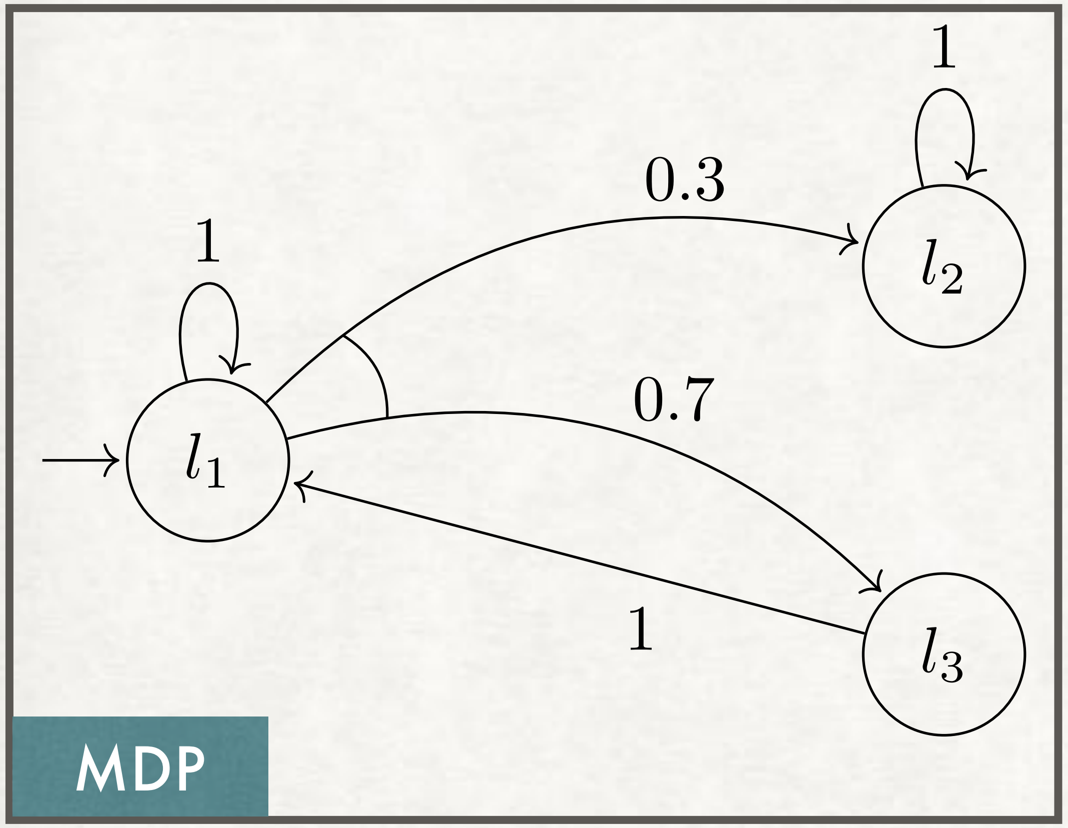
SEMANTICS

- Types of transitions: **delay** and **action**
- Clock valuations: $nat \Rightarrow real$
  → Infinite Semantics
- Clock constraints: $(\lambda c.\, 1) \vdash c_1 > 0 \land c_2 \leq 3$
  → Invariants on nodes and guards on edges

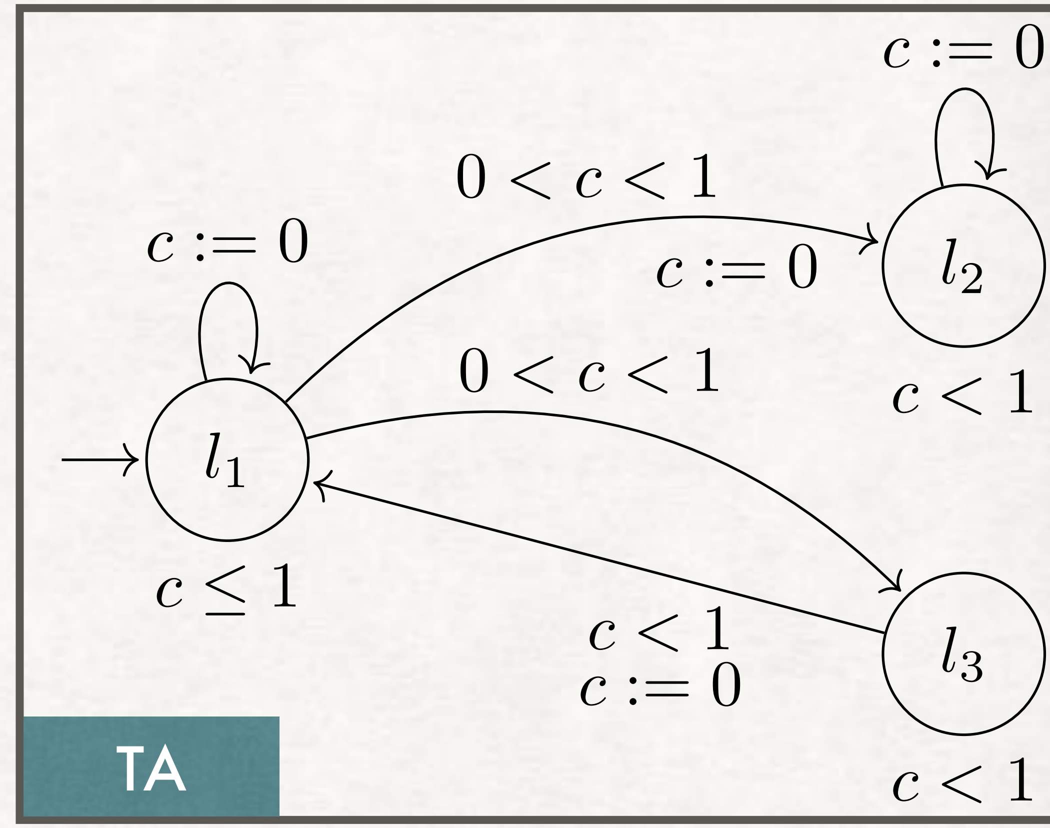




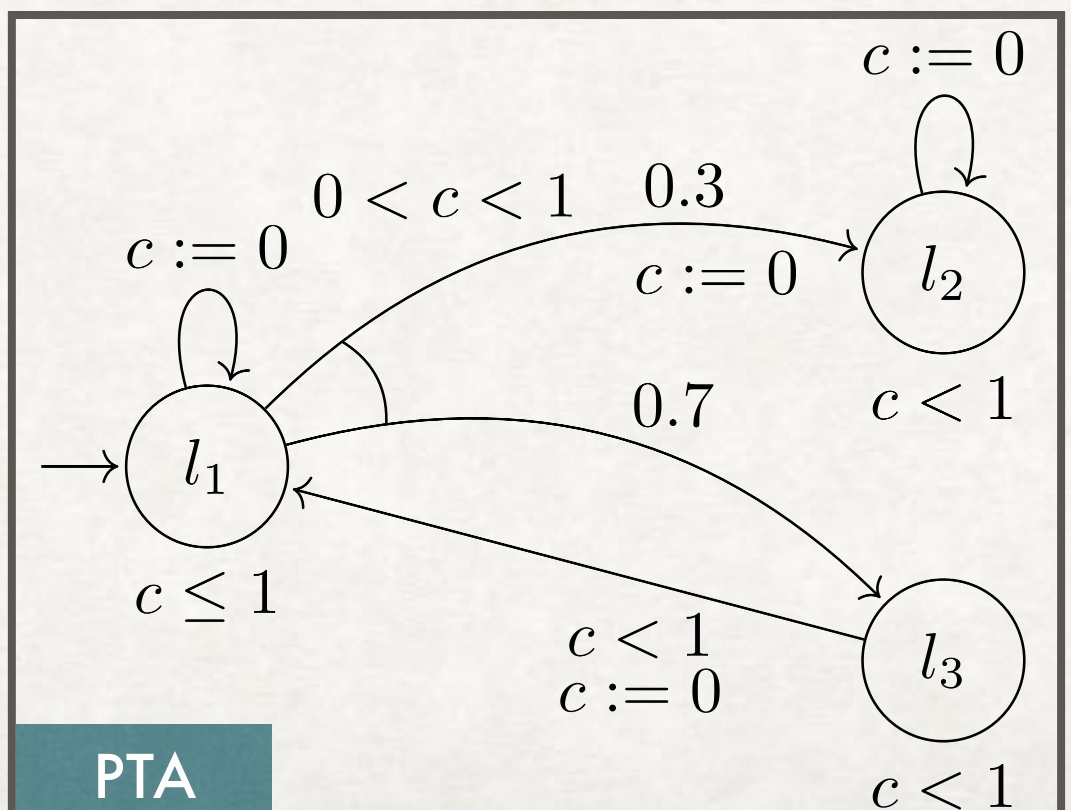
PROBABILISTIC TIMED AUTOMATA



+



=

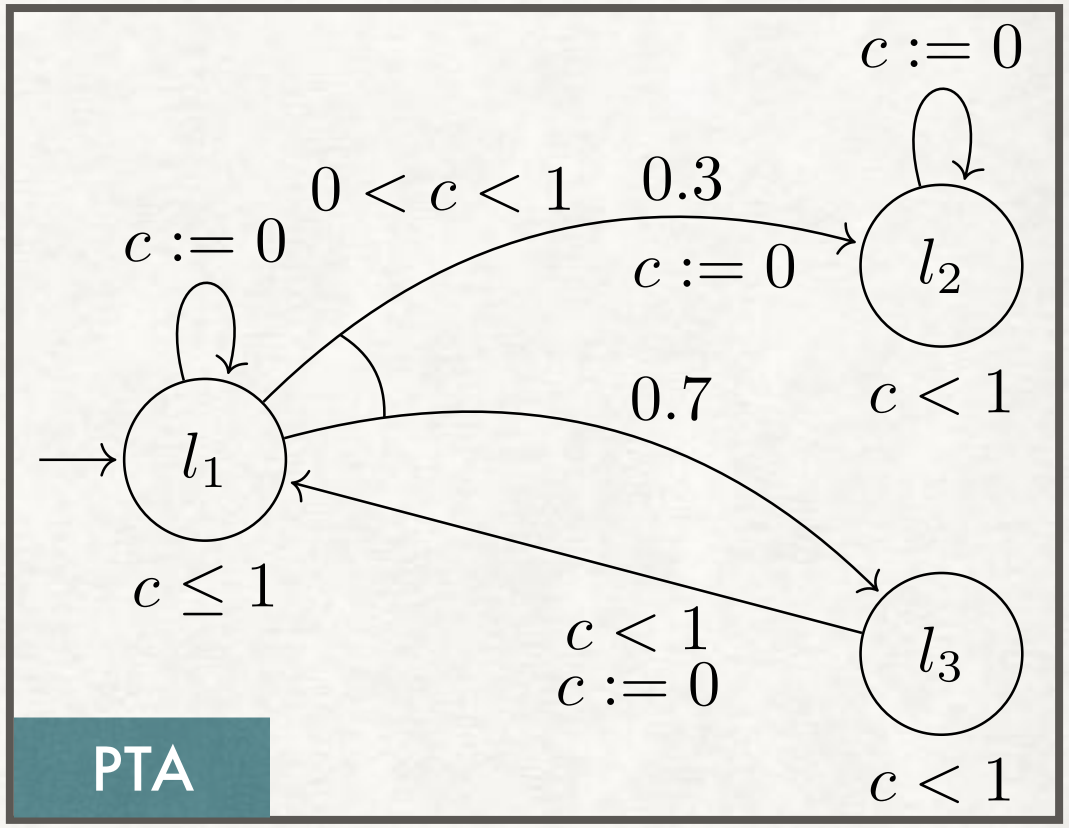


WHAT IS THE MAX./MIN. PROBABILITY TO REACH l_2 AMONG ALL ADVERSARIES?

PROBABILISTIC TIMED AUTOMATA

SEMANTICS

- Formalize PTA as MDPs instead of probabilistic timed structures
- Defined through its kernel



DELAY

TA

$$\frac{(l, u) \in S \qquad t \geq 0 \qquad u \oplus t \vdash \mathcal{I}\, l}{(l, u) \rightarrow^{d} (l, u \oplus d)}$$

PTA

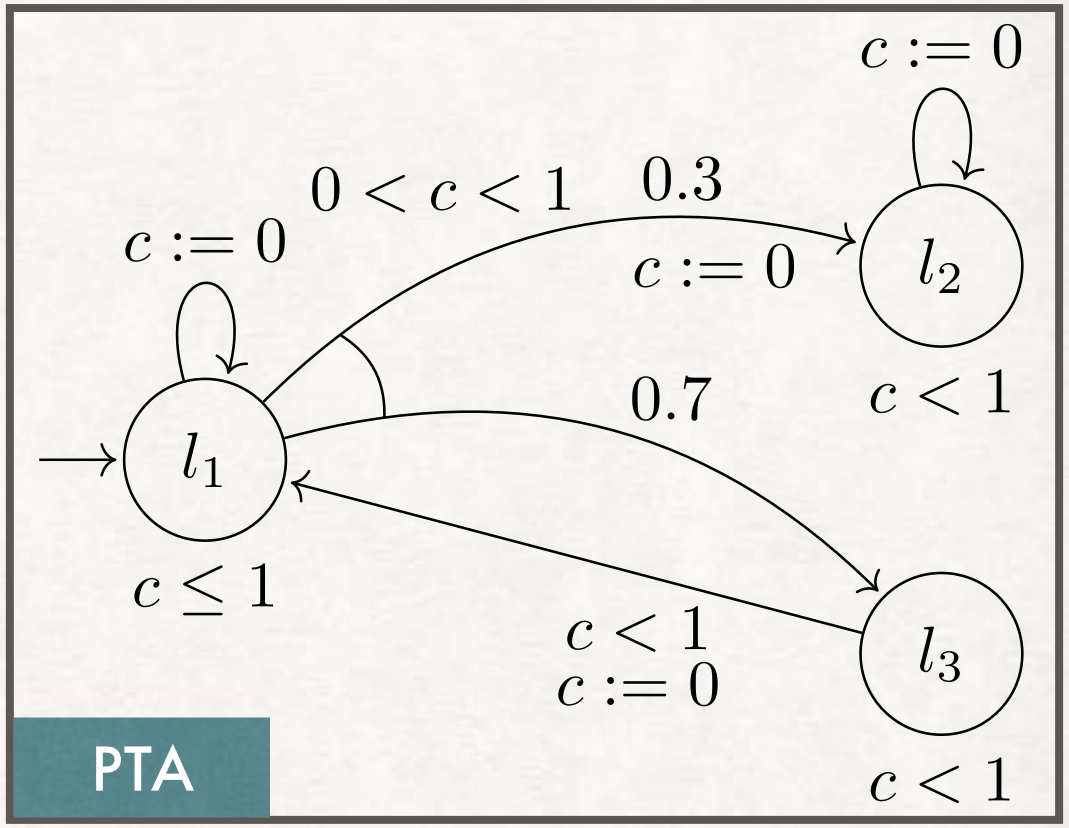
$$\frac{(l, u) \in S \qquad t \geq 0 \qquad u \oplus t \vdash \mathcal{I}\, l}{\mathsf{ret}_{\mathsf{pmf}}\, (l, u \oplus t) \in K\ (l, u)}$$

PROBABILISTIC TIMED AUTOMATA

SEMANTICS

- Formalize PTA as MDPs instead of probabilistic timed structures

- Defined through its kernel



ACTION

TA

$$\frac{(l,u) \in S \qquad A \vdash l \longrightarrow^{g,r} l' \qquad u \vdash g}{(l,u) \rightarrow_a (l', [r \rightarrow 0]u)}$$

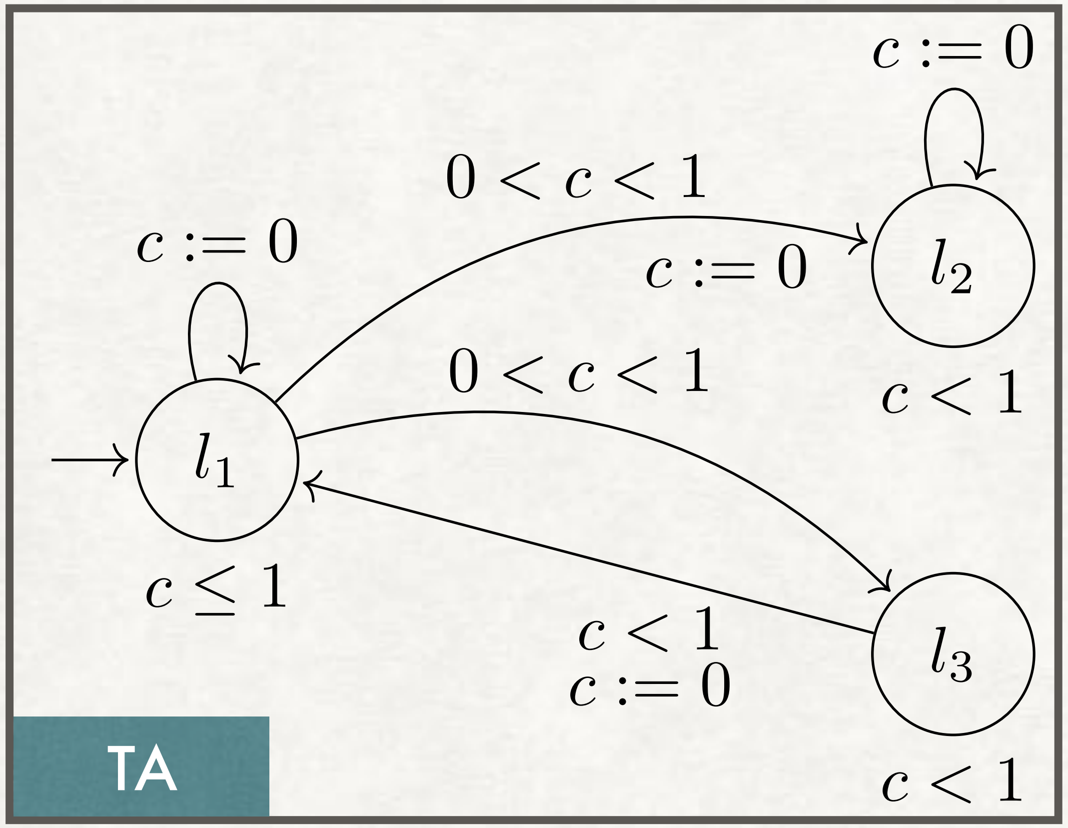
PTA

$$\frac{(l,u) \in S \qquad A \vdash l \longrightarrow^{g} \mu \qquad u \vdash g}{\text{map}_{\text{pmf}}\, (\lambda(r,l).\, (l, [r \rightarrow 0]u))\, \mu \in K\ (l,u)}$$

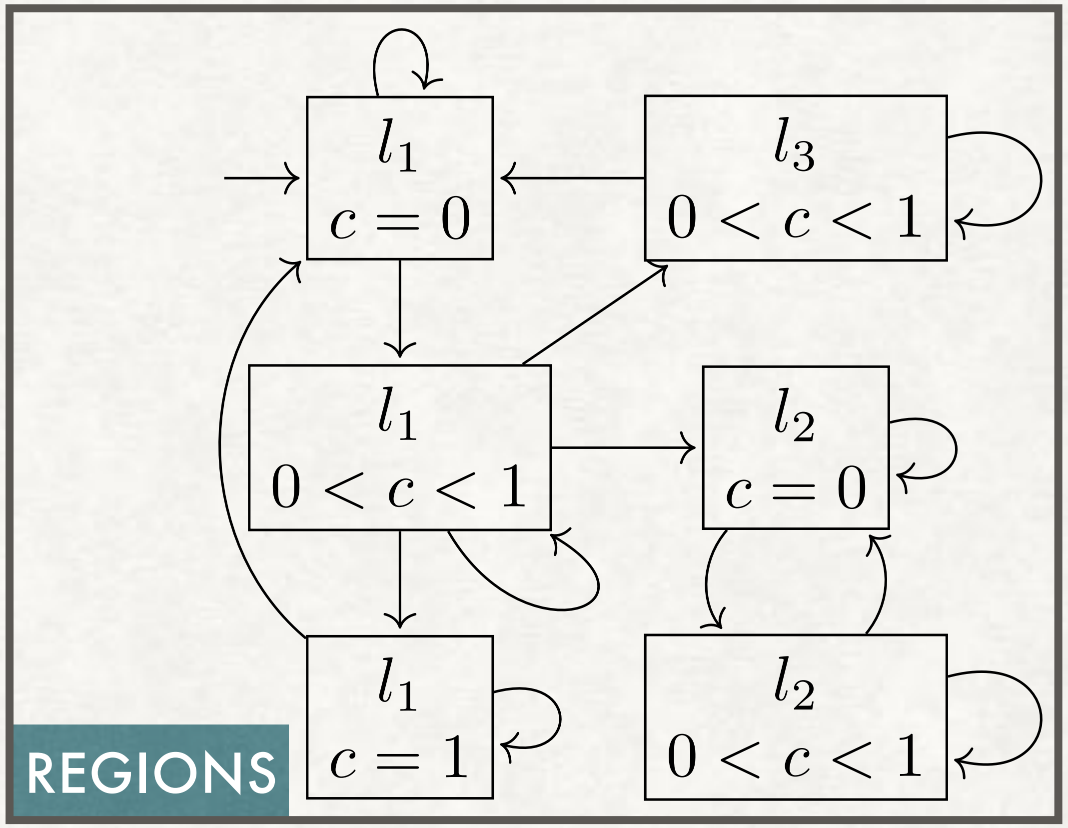
REACHABILITY IN TIMED AUTOMATA

THE REGION CONSTRUCTION

- Reachability for TA shown decidable by Alur & Dill
via the **region construction** to reduce TA to a finite automaton



IS l_2 REACHABLE?

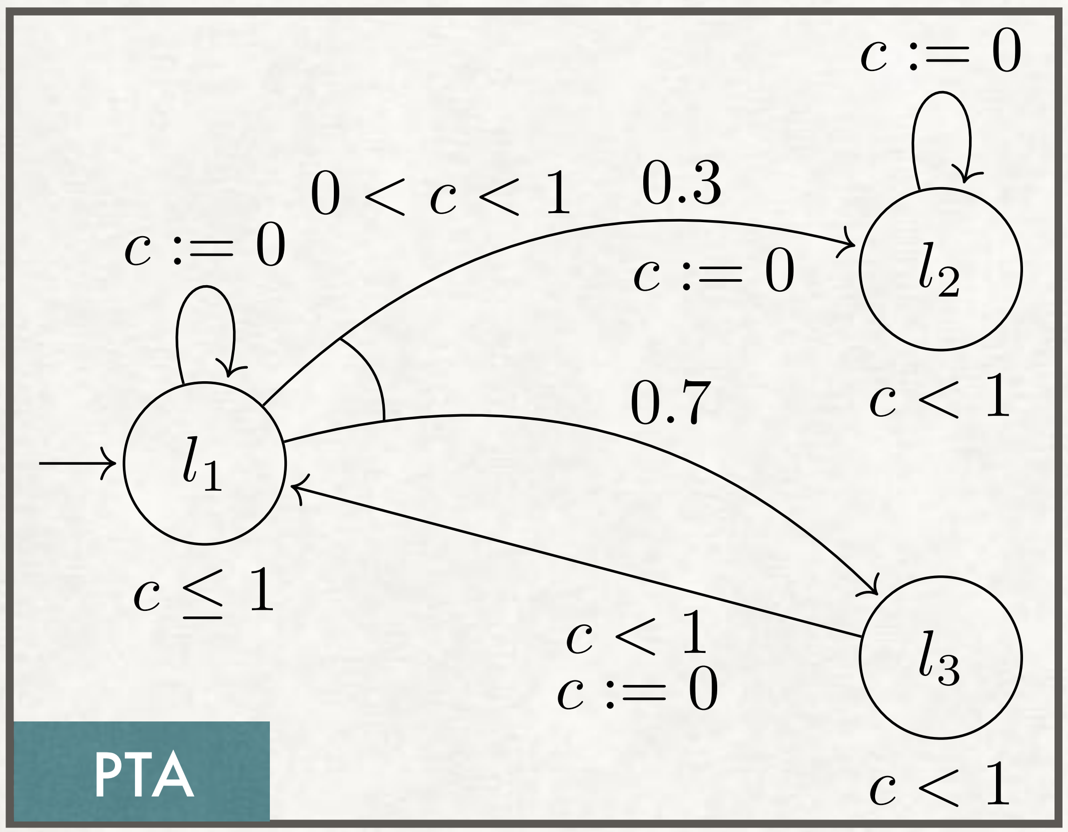


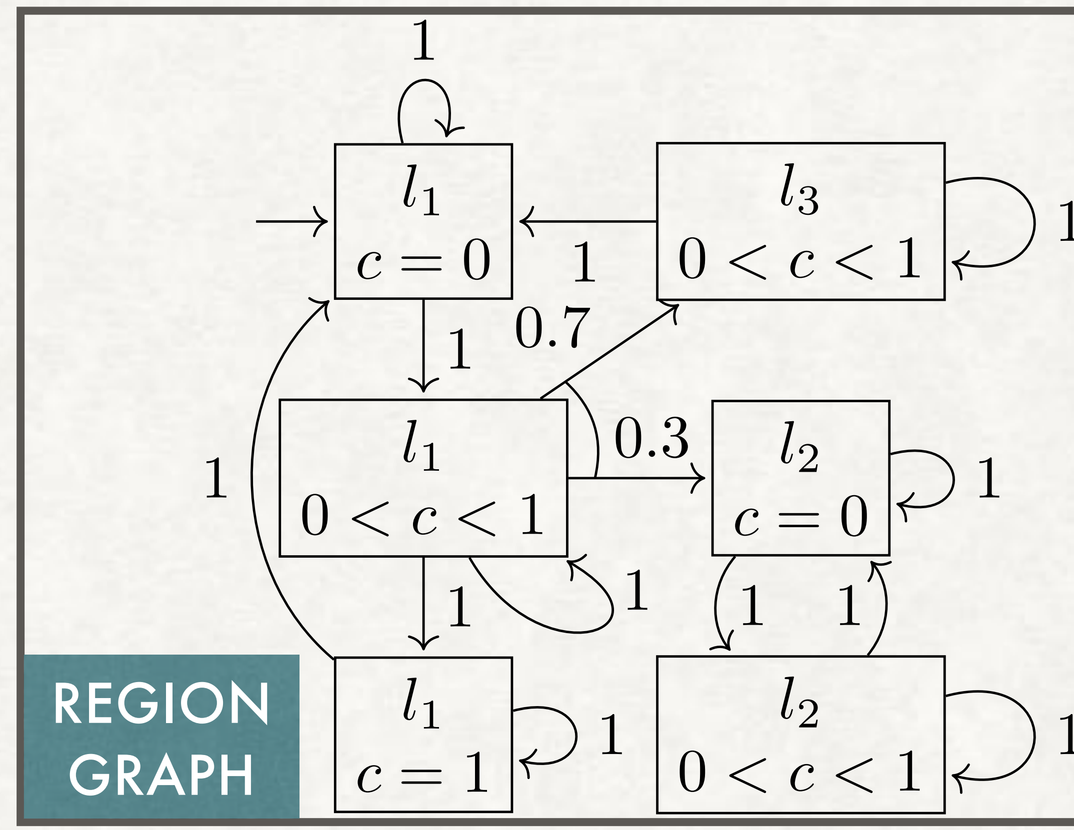
l_2 IS REACHABLE!

REACHABILITY IN PTA

THE REGION CONSTRUCTION

- Reachability for PTA shown decidable by Kwiatkowska et al. via the **region construction** to reduce PTA to a finite MDP



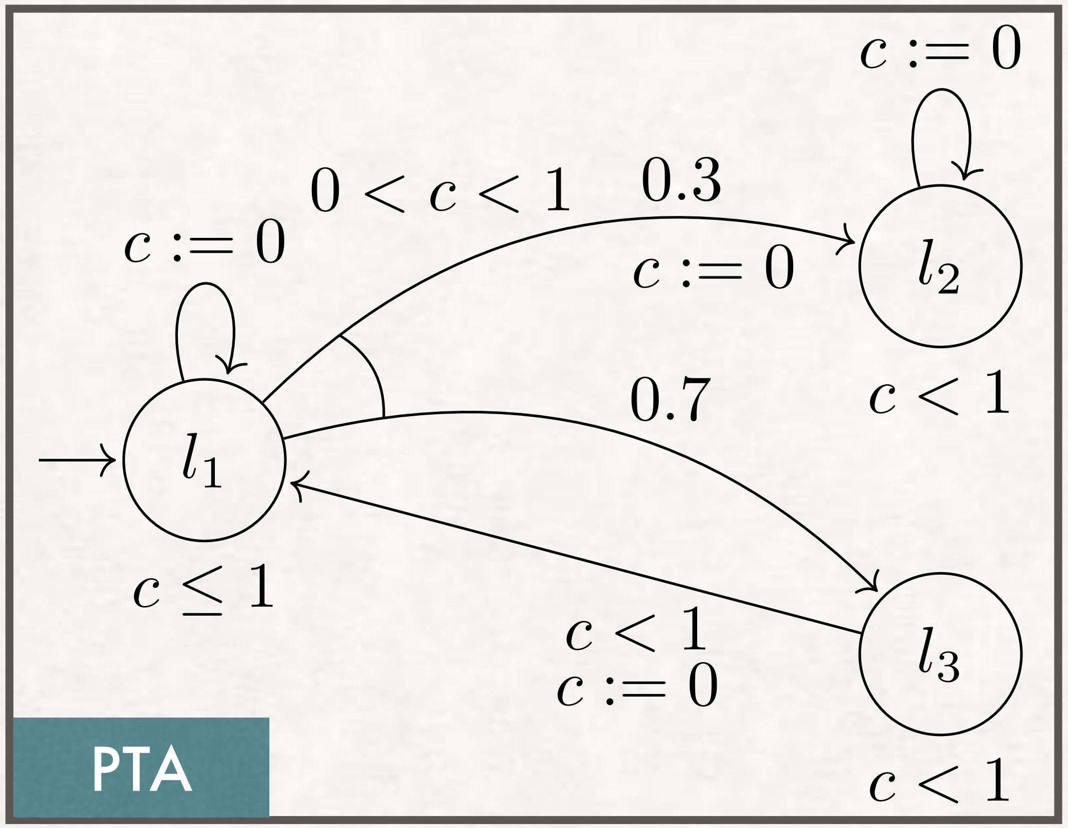


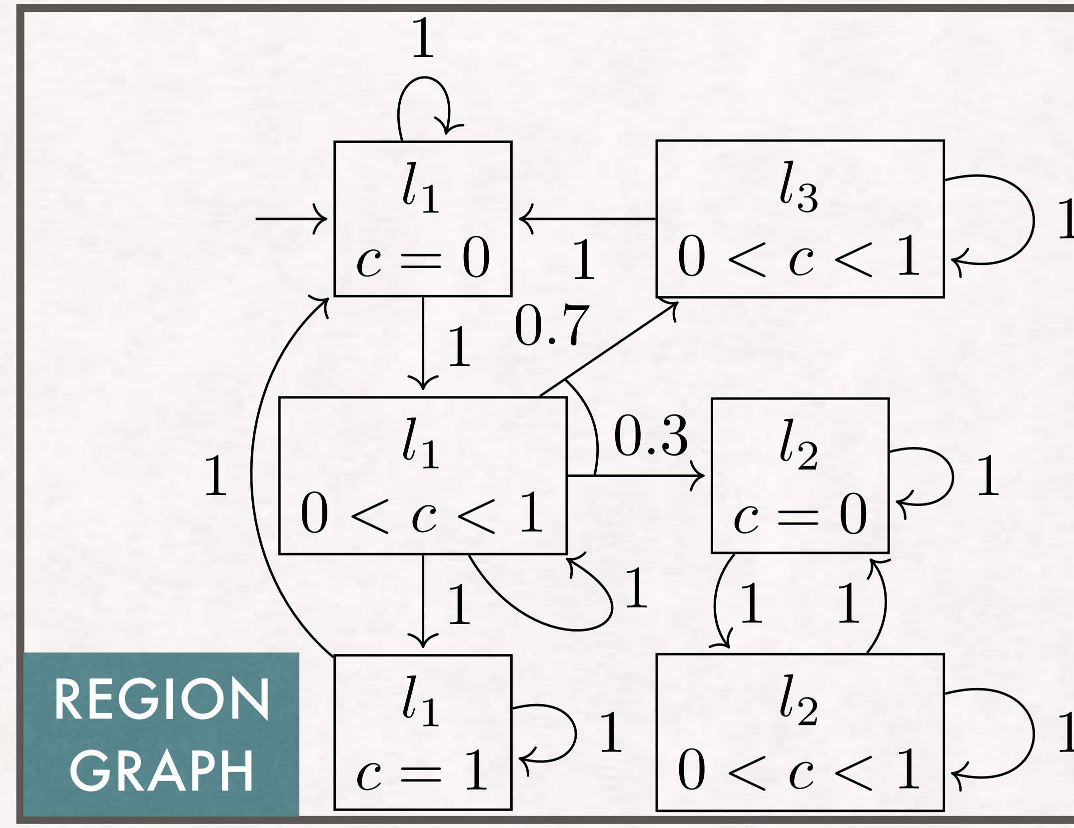
WHAT IS THE MAX./MIN. PROBABILITY TO REACH l_2 AMONG ALL ADVERSARIES?

THE MAX./MIN. PROBABILITY TO REACH l_2 IS 0.3/0!

REGION GRAPH

KERNEL





$$\frac{(l, R) \in \mathcal{S} \qquad R' \in \mathit{Succ}\ R \qquad \forall u \in R'.\, u \vdash \mathcal{I}\ l}{\mathsf{ret}_{\mathsf{pmf}}\ (l, R') \in \mathcal{K}\ (l, R)}\ \textsc{Delay}_{\textsc{R}}$$

$$\frac{(l, R) \in \mathcal{S} \qquad A \vdash l \longrightarrow^{g} \mu \qquad \forall u \in R.\, u \vdash g}{\mathsf{map}_{\mathsf{pmf}}\ (\lambda(r, l).\, (l, \{[r \to 0]u \mid u \in R\})\ \mu \in \mathcal{K}\ (l, R)}\ \textsc{Action}_{\textsc{R}}$$

REGION GRAPH

BISIMULATION

- Prove bisimulation between PTA and region graph

- Our bisimulation theorem on Markov chains:

  $T_K\ x\ A = T_L\ y\ B$ if $R\ x\ y$ and $\forall \omega\ \omega'.\ rel_{stream}\ R\ \omega\ \omega' \longrightarrow (\omega \in A \leftrightarrow \omega' \in B)$
  and $\forall x\ y.\ R\ x\ y \longrightarrow rel_{pmf}\ R\ (K\ x)\ (L\ y)$

TRACE SPACES OF MC KERNELS K, L

MC STATES

SETS OF STREAMS

- Can be instantiated for PTA and region graph

- Corollary: min./max. reachability probabilities are equal for PTA and region graph

REGION GRAPH

BISIMULATION

- Bisimulation on Markov chains

  $T_K\, x\, A = T_L\, y\, B$ if $R\, x\, y$ and $\forall \omega\, \omega' .\ rel_{stream}\, R\, \omega\, \omega' \longrightarrow (\omega \in A \leftrightarrow \omega' \in B)$
  and $\forall x\, y .\ R\, x\, y \longrightarrow rel_{pmf}\, R\, (K\, x)\, (L\, y)$

  TRACE SPACES OF MC KERNELS K, L | MC STATES | SETS OF STREAMS

- Instantiation for PTA and region graph

  - $K = K_c \quad L = \mathcal{K}_c \quad x = c \quad y = \alpha\, c$

  - $R\, c\, c' = (\alpha\, c = c')$

  - Defining α and establishing the probabilistic coupling property is a central part of the formalization

FINALLY

DISCUSSION & FUTURE WORK

- Separate discrete TA-related reasoning from probabilistic, MDP-related reasoning
- Levels of abstraction: MCs and trace spaces, MDPs and configuration traces, PTA and state traces
- In the paper: how to deal with **zenoness**?
- Future Work: Backward reachability of PRISM → requires us to pull a different probabilistic argument out of our hat
- Formalization in the Archive of Formal Proofs (isa-afp.org)