PrIC3 : Property Directed Reachability for MDPs

Kevin Batz, Sebastian Junges, Benjamin Lucien Kaminski,
Joost-Pieter Katoen, Christoph Matheja, Philipp Schröer

Software Modeling and Verification Chair | RWTH AACHEN UNIVERSITY

Berkeley UNIVERSITY OF CALIFORNIA

ETH zürich

UCL Programming Principles, Logic and Verification Group

CAV 2020

Standard IC3 [Bradley 2011] [Eén *et al.* 2011]

- Verifies or refutes reachability properties of transition systems:

  “ Given a transition system, is some Bad state reachable? “

- Was a breakthrough for hardware verification
- Applications: Verification of hardware, software, hybrid systems, …

PrIC3

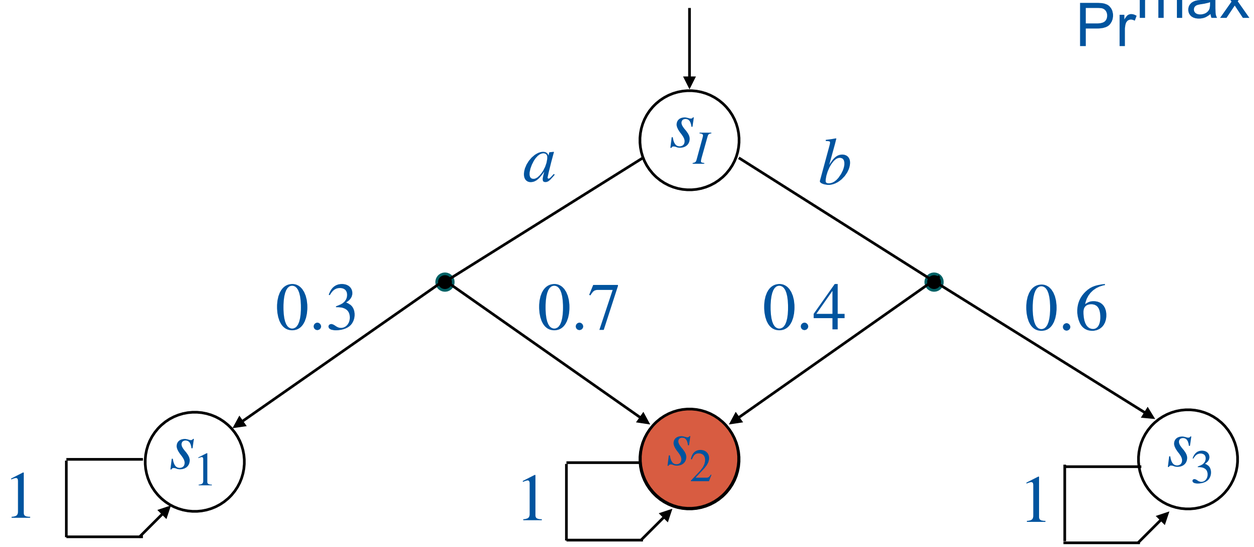
“ Given a Markov decision process, is the maximal probability
to reach some Bad state at most $\lambda \in [0,1]$? “

- Applications: Scalable verification of probabilistic systems, probabilistic programs, …

Markov Decision Processes

$\mathfrak{M} = (S, s_I, \text{Act}, P)$ $\quad$ $\text{Bad} \subseteq S$ $\quad$ $\lambda \in [0,1]$

$\Pr^{\max}(s_I \models \Diamond \text{Bad}) = 0.7 \leq \lambda \ ?$

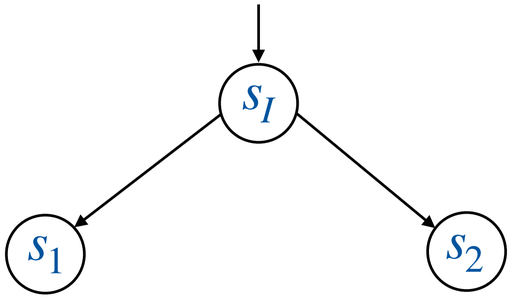


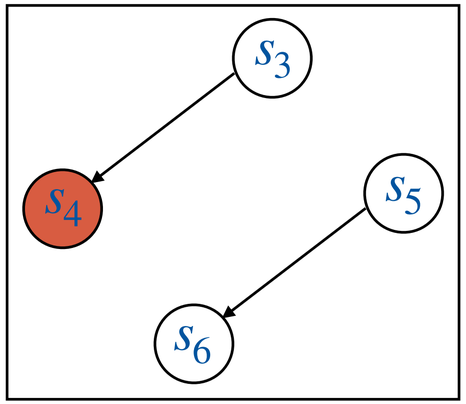
Contributions

- Understand IC3 on the level of sets/functions rather than formulae/SAT queries
- A PrIC3 framework conservatively extending (reverse) IC3
- Prototypical implementation and empirical evaluation
  - Operate on program level (PRISM) by means of an SMT encoding
  - Repushing obligations, propagation, (first ideas on) generalization

Proving Unreachability

TS $= (S, s_I, T)$ Bad $\subseteq S$

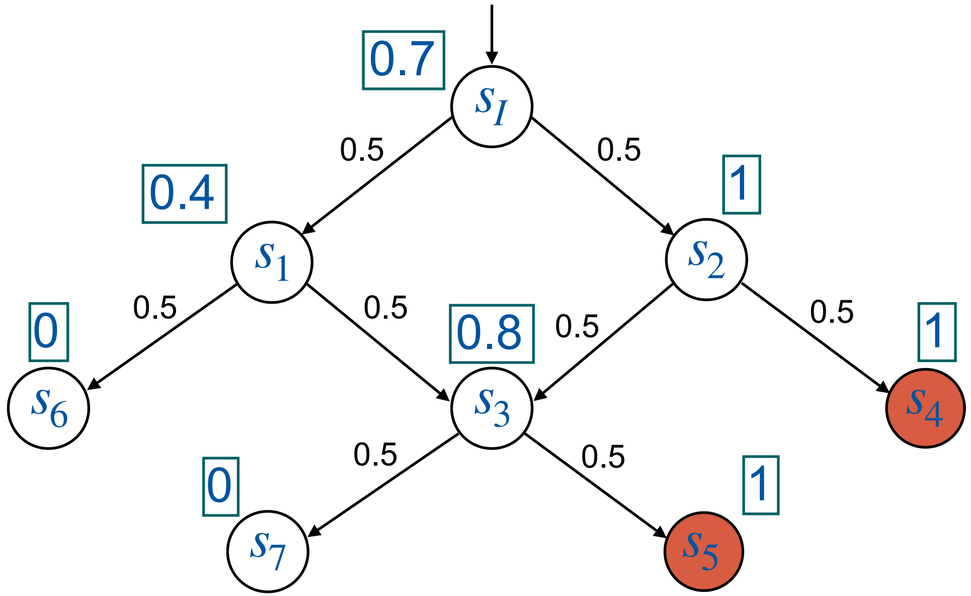




Inductive invariant
$F \subseteq S$ with $s_I \notin F$

or:
$F\colon S \to \{0,1\}$ with $F[s_I] = 0$

MC $= (S, s_I, P)$ Bad $\subseteq S$ $\lambda = 0.7$
Pr $(s_I \models \Diamond \text{Bad}) = 0.5$



$$\sum_{s' \in S} P(s, s') \cdot F[s'] \leq F[s]$$

Inductive invariant
$F\colon S \to [0,1]$ with $F[s_I] \leq \lambda$

The Theory underlying (Pr)IC3

TS $= (S, s_I, T)$ Bad $\subseteq S$

Call $F\colon S \to \{0,1\}$ a frame.

Frames are partially ordered by

$$F \leq F' \quad \text{iff} \quad \forall s\colon F[s] \leq F'[s] \ .$$

$$\Phi\colon 2^S \to 2^S,$$
$$\Phi(F) = \text{Bad} \cup \text{Pred}(F)$$

Then:

$s \vDash \Diamond \text{Bad}$ iff $s \in \Phi^\omega(\varnothing)$ iff $s \in \text{lfp}.\Phi$

If $\Phi(F) \leq F$, then F is an inductive invariant.

MC $= (S, s_I, P)$ Bad $\subseteq S$ $\lambda \in [0,1]$

Call $F\colon S \to [0,1]$ a frame.

Frames are partially ordered by

$$F \leq F' \quad \text{iff} \quad \forall s\colon F[s] \leq F'[s] \ .$$

$$\Phi\colon [0,1]^S \to [0,1]^S \ ,$$

$$\Phi(F)[s] = \begin{cases} 1, & \text{if } s \in \text{Bad} \\ \sum_{s' \in S} P(s,s') \cdot F[s'], & \text{else} \end{cases}$$

Then:

$\Pr\left(s \vDash \Diamond \text{Bad}\right) = (\Phi^\omega(\mathbf{0}))[s] = (\text{lfp}.\Phi)[s]$

If $\Phi(F) \leq F$, then F is an inductive invariant.

The Theory underlying (reverse) IC3: The IC3 Invariants

TS $= (S, s_I, T)$ Bad $\subseteq S$

Call $F\colon S \to \{0,1\}$ a frame.

For increasing $k = 0,1,\ldots$, compute sequence

$$F_0, \ldots, F_k$$

such that

1. Initiality: $F_0 = [\text{Bad}] = \Phi(\varnothing)$
2. Chain-Property: $\forall 0 \leq i < k\colon F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k\colon F_i[s_I] = 0$
4. Relative inductivity: $\forall 0 \leq i < k\colon \Phi(F_i) \leq F_{i+1}$

- $\Diamond^{\leq i}\text{Bad} \leq F_i$
- If $F_i = F_{i+1}$, then
  $\Phi(F_i) \leq F_i$ hence $s_I \not\models \Diamond\text{Bad}$

The Theory underlying PrIC3: The PrIC3 Invariants

MC $= (S, s_I, P)$ Bad $\subseteq S$ $\lambda \in [0,1]$

Call $F\colon S \to [0,1]$ a frame.

For increasing $k = 0,1,\ldots$, compute sequence

$$F_0, \ldots, F_k$$

such that

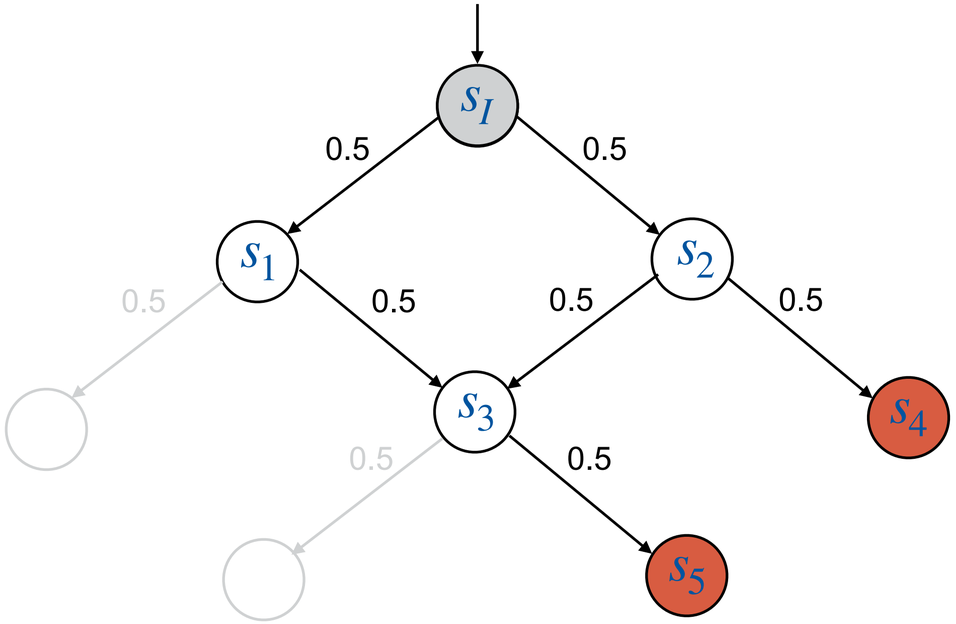
1. Initiality: $F_0 = [\text{Bad}] = \Phi(\mathbf{0})$
2. Chain-Property: $\forall 0 \leq i < k\colon F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k\colon F_i[s_I] \leq \lambda$
4. Relative inductivity: $\forall 0 \leq i < k\colon \Phi(F_i) \leq F_{i+1}$

- $\Pr\left(s \models \Diamond^{\leq i} \text{Bad}\right) \leq F_i[s]$
- If $F_i = F_{i+1}$, then
  $\Phi(F_i) \leq F_i$ hence $\Pr\left(s_I \models \Diamond \text{Bad}\right) \leq \lambda$

PrIC3

$\text{MC} = (S, s_I, P)$ $\quad \text{Bad} \subseteq S \quad$ $\lambda = 0.7$

1. Initiality: $F_0 = [\text{Bad}] = \Phi(\mathbf{0})$
2. Chain-Property: $\forall 0 \leq i < k : F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k : F_i[s_I] \leq 0.7$
4. Relative inductivity: $\forall 0 \leq i < k : \Phi(F_i) \leq F_{i+1}$



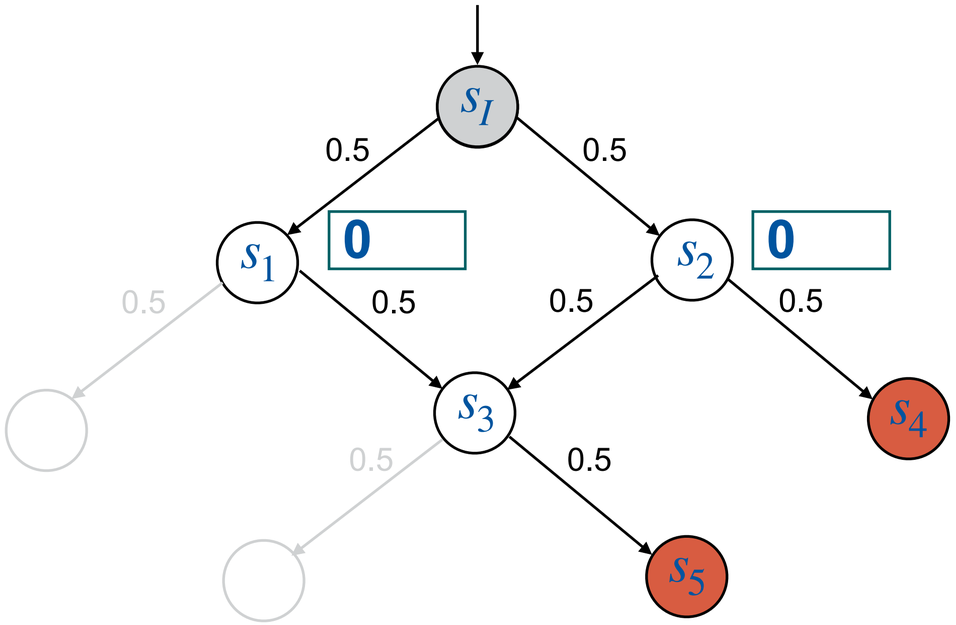
$$F_1 = (\ \underset{s_I}{1}\ ,\ \underset{s_1}{1}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

$$F_0[s] = \begin{cases} 0, & \text{if } s \notin \text{Bad} \\ 1, & \text{if } s \in \text{Bad} \end{cases}$$

PrIC3

$\text{MC} = (S, s_I, P)$ $\quad \text{Bad} \subseteq S \quad$ $\lambda = 0.7$

1. Initiality: $F_0 = [\text{Bad}] = \Phi(\mathbf{0})$
2. Chain-Property: $\forall 0 \leq i < k\colon F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k\colon F_i[s_I] \leq 0.7$
4. Relative inductivity: $\forall 0 \leq i < k\colon \Phi(F_i) \leq F_{i+1}$



Check: $0.5 \cdot F_0[s_1] + 0.5 \cdot F_0[s_2] > 0.7$?

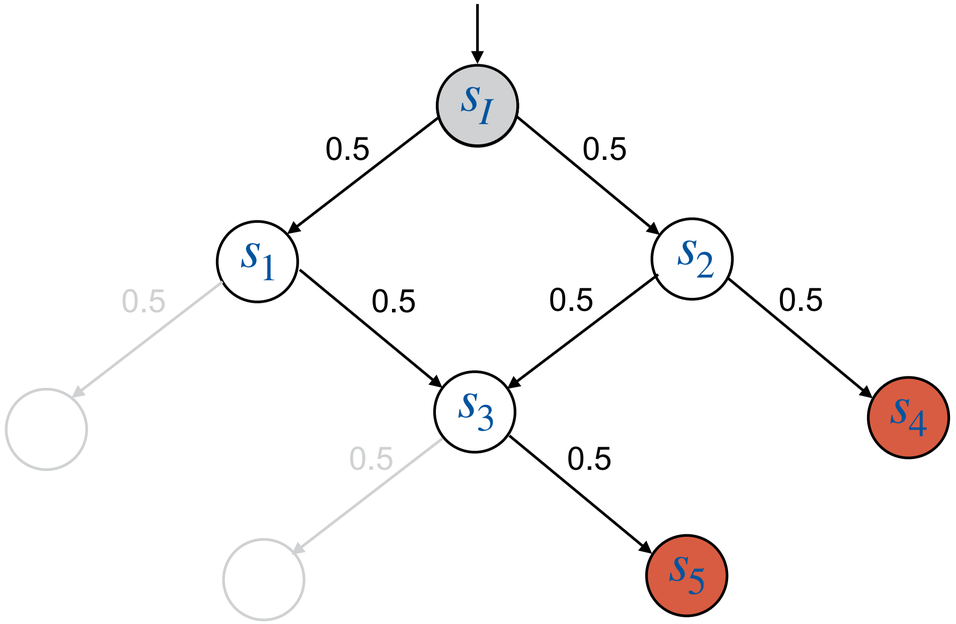
	s_I	s_1	s_2	s_3	s_4	s_5
$F_1 =$	1	1	1	1	1	1

$$\mathbf{F_0(s)} = \begin{cases} \mathbf{0}, & \text{if } s \notin \text{Bad} \\ 1, & \text{if } s \in \text{Bad} \end{cases}$$

PrIC3

$\text{MC} = (S, s_I, P)$ $\quad \text{Bad} \subseteq S \quad$ $\lambda = 0.7$

1. Initiality: $F_0 = [\text{Bad}] = \Phi(\mathbf{0})$
2. Chain-Property: $\forall 0 \leq i < k : F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k : F_i[s_I] \leq 0.7$
4. Relative inductivity: $\forall 0 \leq i < k : \Phi(F_i) \leq F_{i+1}$



$$F_2 = (\ \underset{s_I}{1}\ ,\ \underset{s_1}{1}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

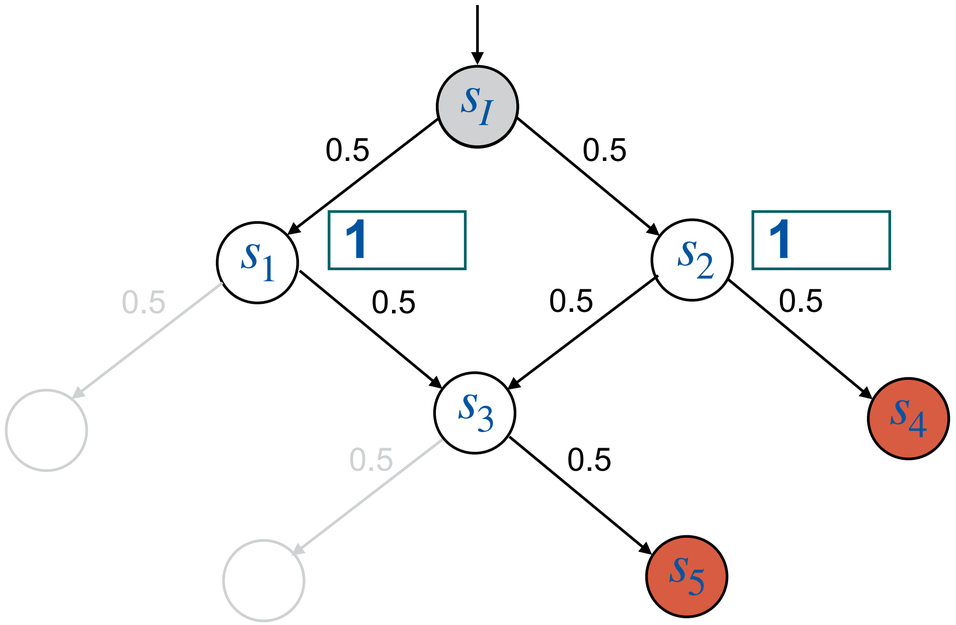
$$F_1 = (\ \underset{s_I}{0.7}\ ,\ \underset{s_1}{1}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

$$F_0(s) = \begin{cases} 0, & \text{if } s \notin \text{Bad} \\ 1, & \text{if } s \in \text{Bad} \end{cases}$$

PrIC3

$\text{MC} = (S, s_I, P)$ Bad $\subseteq S$ $\lambda = 0.7$

1. Initiality: $F_0 = [\text{Bad}] = \Phi(\mathbf{0})$
2. Chain-Property: $\forall 0 \leq i < k\colon F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k\colon F_i[s_I] \leq 0.7$
4. Relative inductivity: $\forall 0 \leq i < k\colon \Phi(F_i) \leq F_{i+1}$



Check: $0.5 \cdot F_1[s_1] + 0.5 \cdot F_1[s_2] > 0.7$?

$$F_2 = \begin{matrix} s_I & s_1 & s_2 & s_3 & s_4 & s_5 \\ (1 , & 1 , & 1 , & 1 , & 1 , & 1) \end{matrix}$$

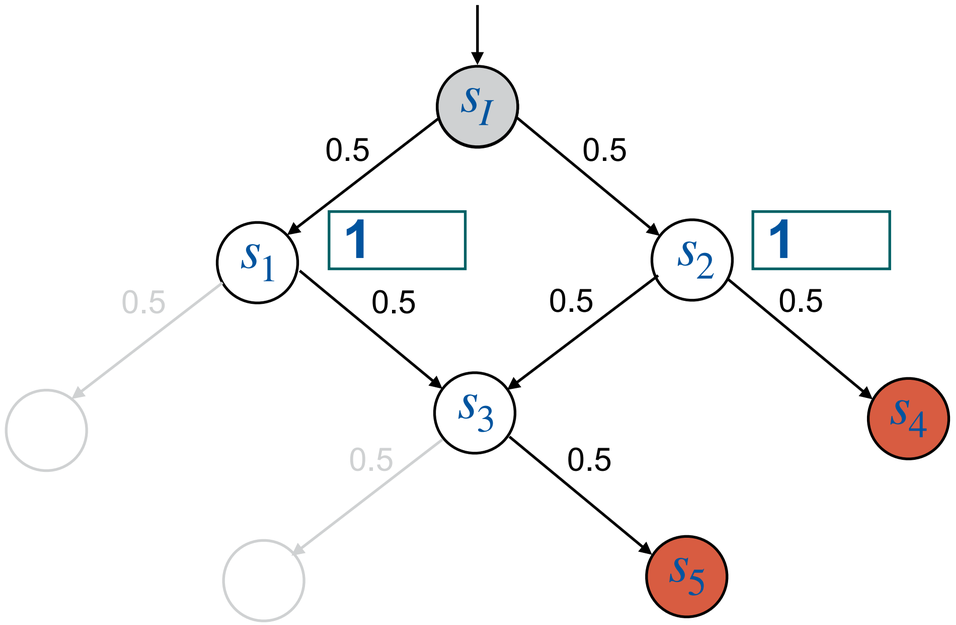
$$F_1 = \begin{matrix} s_I & s_1 & s_2 & s_3 & s_4 & s_5 \\ (0.7 , & \mathbf{1} , & \mathbf{1} , & 1 , & 1 , & 1) \end{matrix}$$

$$F_0(s) = \begin{cases} 0, & \text{if } s \notin \text{Bad} \\ 1, & \text{if } s \in \text{Bad} \end{cases}$$

PrIC3

$\text{MC} = (S, s_I, P)$ Bad $\subseteq S$ $\lambda = 0.7$

1. Initiality: $F_0 = [\text{Bad}] = \Phi(\mathbf{0})$
2. Chain-Property: $\forall 0 \leq i < k : F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k : F_i[s_I] \leq 0.7$
4. Relative inductivity: $\forall 0 \leq i < k : \Phi(F_i) \leq F_{i+1}$



Find $x_1, x_2 \in [0,1]$ such that

$$0.5 \cdot x_1 + 0.5 \cdot x_2 \leq 0.7$$

Problem: Infinitely many choices.
There are “bad” choices.
Requires heuristic/oracle.

$$F_2 = \begin{pmatrix} s_I & s_1 & s_2 & s_3 & s_4 & s_5 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

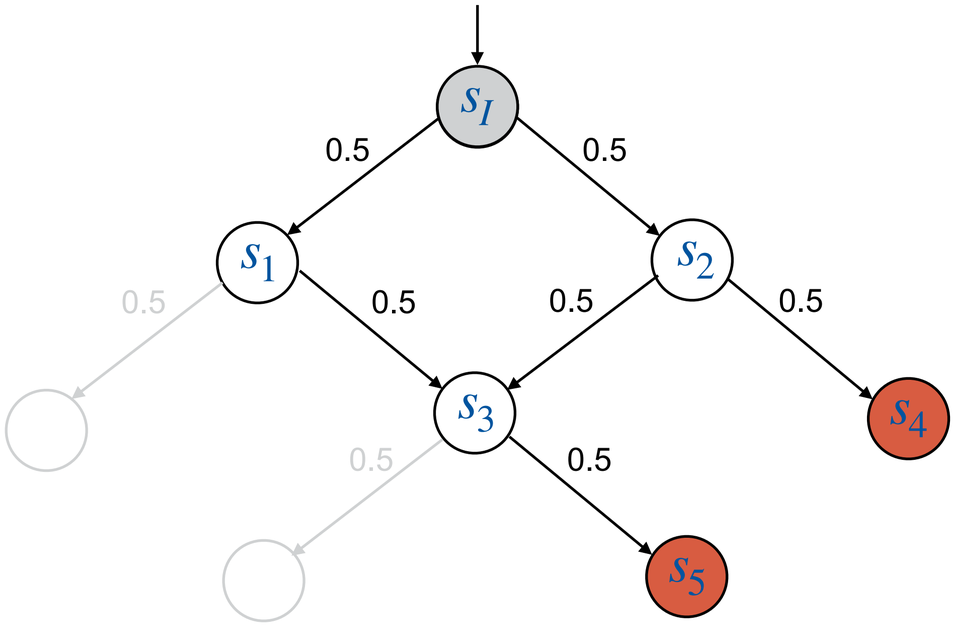
$$F_1 = \begin{pmatrix} s_I & s_1 & s_2 & s_3 & s_4 & s_5 \\ 0.7 & \mathbf{1} & \mathbf{1} & 1 & 1 & 1 \end{pmatrix}$$

$$F_0(s) = \begin{cases} 0, & \text{if } s \notin \text{Bad} \\ 1, & \text{if } s \in \text{Bad} \end{cases}$$

PrIC3

$\text{MC} = (S, s_I, P)$ $\quad \text{Bad} \subseteq S \quad$ $\lambda = 0.7$

1. Initiality: $F_0 = [\text{Bad}] = \Phi(\mathbf{0})$
2. Chain-Property: $\forall 0 \leq i < k : F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k : F_i[s_I] \leq 0.7$
4. Relative inductivity: $\forall 0 \leq i < k : \Phi(F_i) \leq F_{i+1}$



$$F_2 = (\ \underset{s_I}{1}\ ,\ \underset{s_1}{1}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

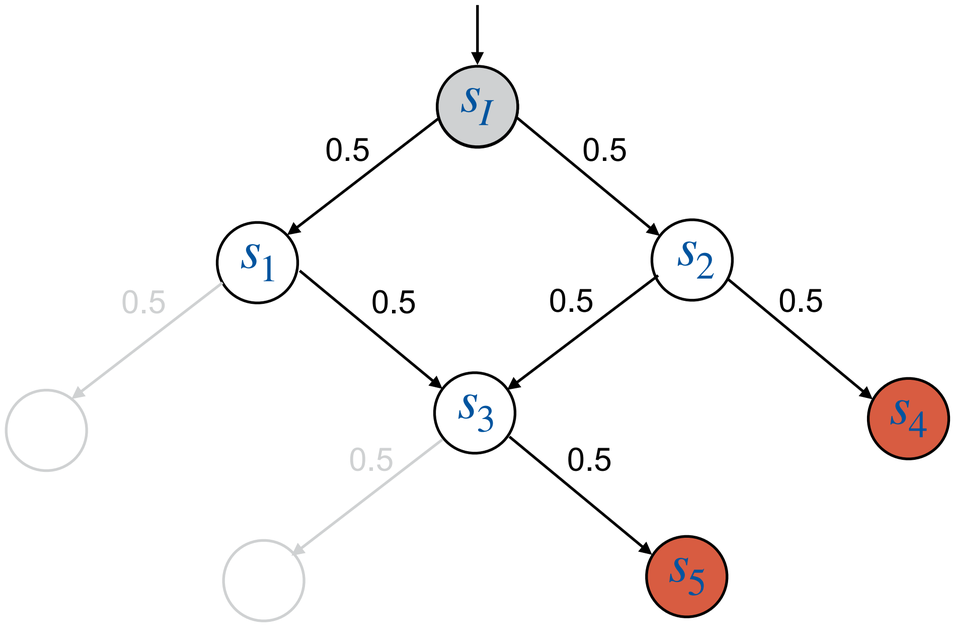
$$F_1 = (\ \underset{s_I}{0.7}\ ,\ \underset{s_1}{0.4}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

$$F_0(s) = \begin{cases} 0, & \text{if } s \notin \text{Bad} \\ 1, & \text{if } s \in \text{Bad} \end{cases}$$

PrIC3

$\text{MC} = (S, s_I, P)$ $\quad \text{Bad} \subseteq S \quad$ $\lambda = 0.7$

1. Initiality: $F_0 = [\text{Bad}] = \Phi(\mathbf{0})$
2. Chain-Property: $\forall 0 \leq i < k : F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k : F_i[s_I] \leq 0.7$
4. Relative inductivity: $\forall 0 \leq i < k : \Phi(F_i) \leq F_{i+1}$



$$F_3 = (\ \underset{s_I}{1}\ ,\ \underset{s_1}{1}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

$$F_2 = (\ \underset{s_I}{0.7}\ ,\ \underset{s_1}{1}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

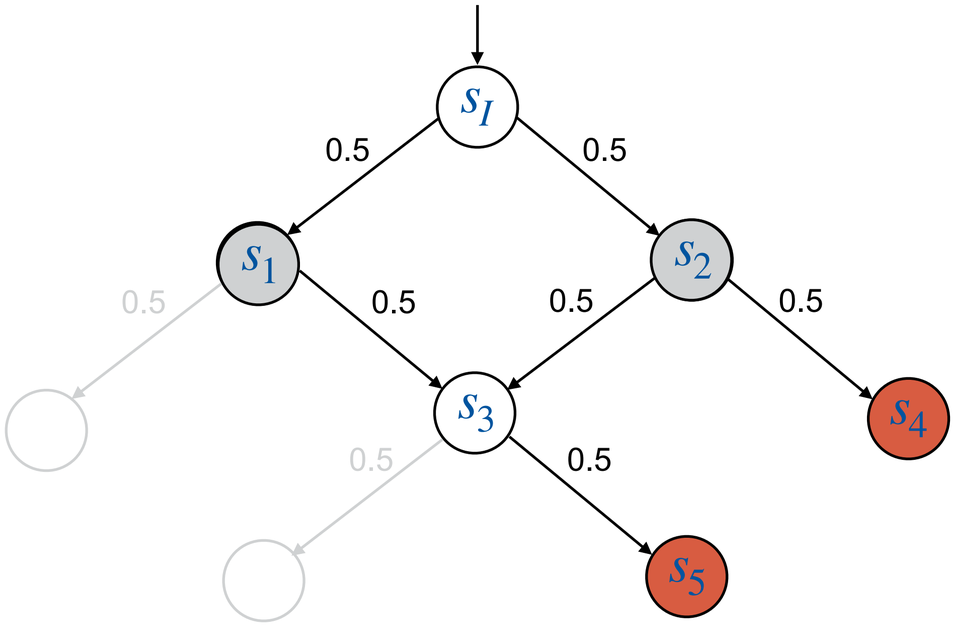
$$F_1 = (\ \underset{s_I}{0.7}\ ,\ \underset{s_1}{0.4}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

$$F_0(s) = \begin{cases} 0, & \text{if } s \notin \text{Bad} \\ 1, & \text{if } s \in \text{Bad} \end{cases}$$

PrIC3

$\text{MC} = (S, s_I, P)$ $\quad \text{Bad} \subseteq S \quad \lambda = 0.7$

1. Initiality: $F_0 = [\text{Bad}] = \Phi(\mathbf{0})$
2. Chain-Property: $\forall 0 \leq i < k : F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k : F_i[s_I] \leq 0.7$
4. Relative inductivity: $\forall 0 \leq i < k : \Phi(F_i) \leq F_{i+1}$



$$F_3 = (\ \underset{s_I}{1}\ ,\ \underset{s_1}{1}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

$$F_2 = (\ \underset{s_I}{0.7}\ ,\ \underset{s_1}{1}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

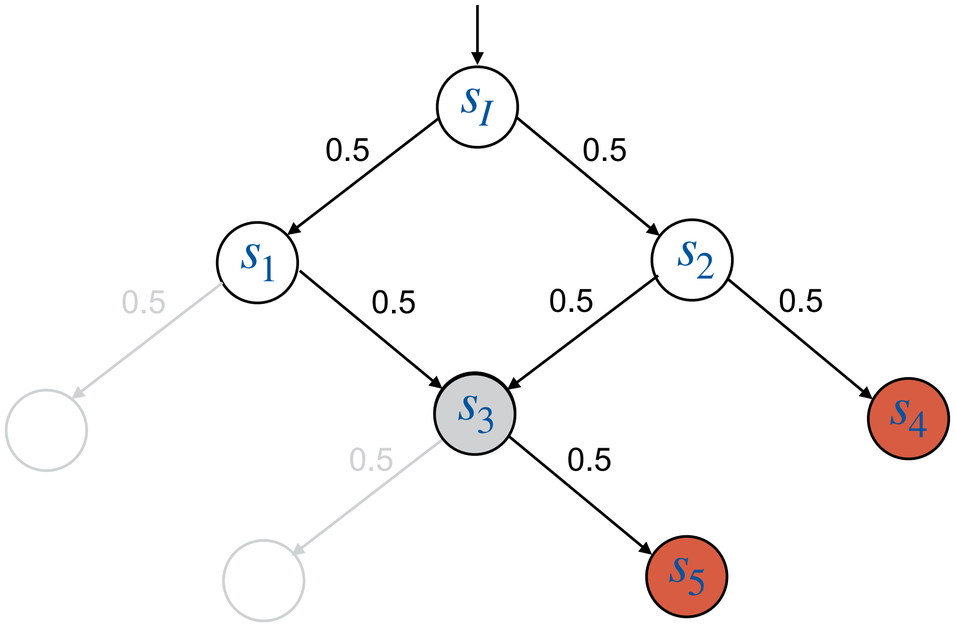
$$F_1 = (\ \underset{s_I}{0.7}\ ,\ \underset{s_1}{0.4}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

$$F_0(s) = \begin{cases} 0, & \text{if } s \notin \text{Bad} \\ 1, & \text{if } s \in \text{Bad} \end{cases}$$

PrIC3

$\text{MC} = (S, s_I, P)$ $\quad \text{Bad} \subseteq S \quad$ $\lambda = 0.7$

1. Initiality: $F_0 = [\text{Bad}] = \Phi(\mathbf{0})$
2. Chain-Property: $\forall 0 \leq i < k \colon F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k \colon F_i[s_I] \leq 0.7$
4. Relative inductivity: $\forall 0 \leq i < k \colon \Phi(F_i) \leq F_{i+1}$



$$F_3 = (\ \underset{s_I}{1}\ ,\ \underset{s_1}{1}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

$$F_2 = (\ \underset{s_I}{0.7}\ ,\ \underset{s_1}{1}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

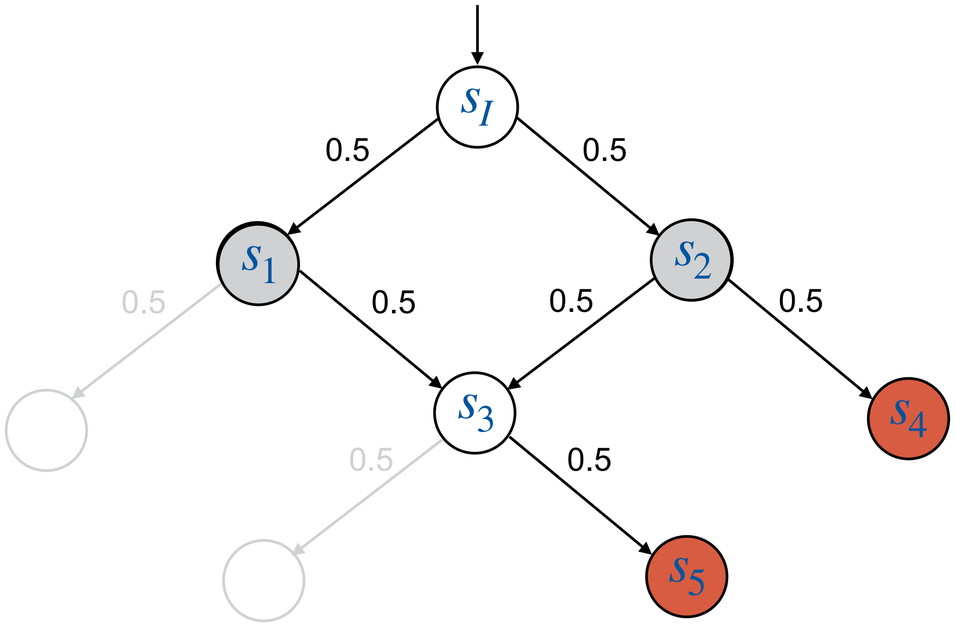
$$F_1 = (\ \underset{s_I}{0.7}\ ,\ \underset{s_1}{0.4}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

$$F_0(s) = \begin{cases} 0, & \text{if } s \notin \text{Bad} \\ 1, & \text{if } s \in \text{Bad} \end{cases}$$

PrIC3

$\text{MC} = (S, s_I, P)$ $\quad \text{Bad} \subseteq S \quad \lambda = 0.7$

1. Initiality: $F_0 = [\text{Bad}] = \Phi(\mathbf{0})$
2. Chain-Property: $\forall 0 \leq i < k\colon F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k\colon F_i[s_I] \leq 0.7$
4. Relative inductivity: $\forall 0 \leq i < k\colon \Phi(F_i) \leq F_{i+1}$



$$F_3 = (\ \underset{s_I}{1}\ ,\ \underset{s_1}{1}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

$$F_2 = (\ \underset{s_I}{0.7}\ ,\ \underset{s_1}{1}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

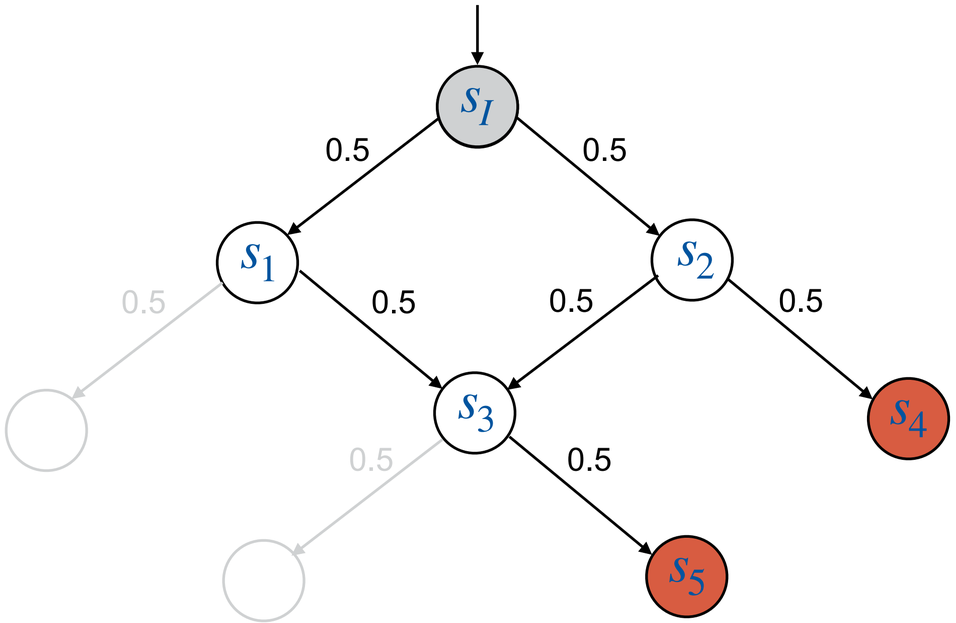
$$F_1 = (\ \underset{s_I}{0.7}\ ,\ \underset{s_1}{0.4}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{0.8}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

$$F_0(s) = \begin{cases} 0, & \text{if } s \notin \text{Bad} \\ 1, & \text{if } s \in \text{Bad} \end{cases}$$

PrIC3

$\text{MC} = (S, s_I, P)$ $\quad \text{Bad} \subseteq S \quad$ $\lambda = 0.7$

1. Initiality: $F_0 = [\text{Bad}] = \Phi(\mathbf{0})$
2. Chain-Property: $\forall 0 \leq i < k : F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k : F_i[s_I] \leq 0.7$
4. Relative inductivity: $\forall 0 \leq i < k : \Phi(F_i) \leq F_{i+1}$



$$F_3 = (\ \underset{1}{s_I}\ ,\ \underset{1}{s_1}\ ,\ \underset{1}{s_2}\ ,\ \underset{1}{s_3}\ ,\ \underset{1}{s_4}\ ,\ \underset{1}{s_5}\ )$$

$$F_2 = (\ \underset{0.7}{s_I}\ ,\ \underset{0.4}{s_1}\ ,\ \underset{1}{s_2}\ ,\ \underset{1}{s_3}\ ,\ \underset{1}{s_4}\ ,\ \underset{1}{s_5}\ )$$

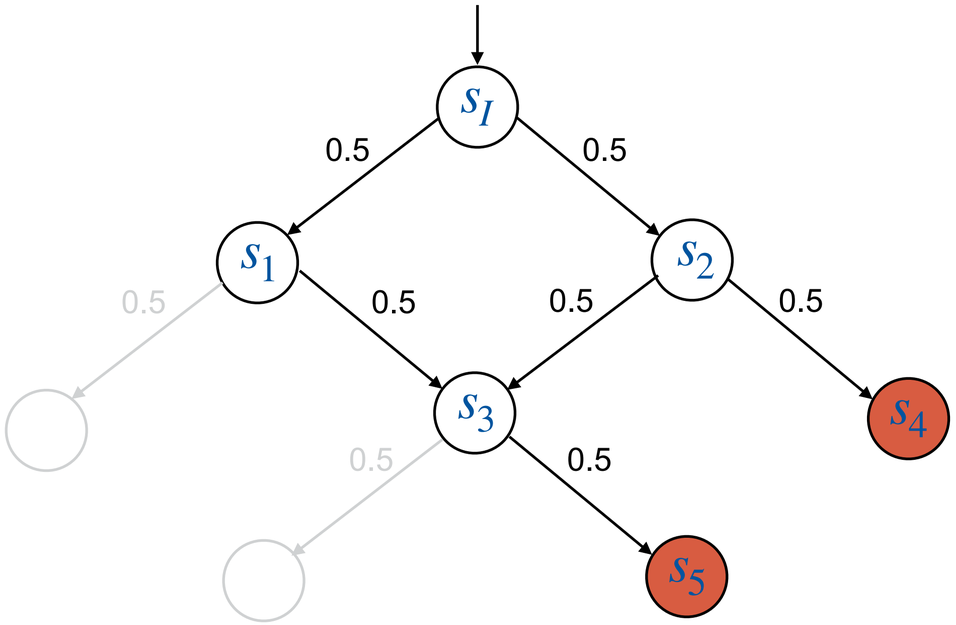
$$F_1 = (\ \underset{0.7}{s_I}\ ,\ \underset{0.4}{s_1}\ ,\ \underset{1}{s_2}\ ,\ \underset{0.8}{s_3}\ ,\ \underset{1}{s_4}\ ,\ \underset{1}{s_5}\ )$$

$$F_0(s) = \begin{cases} 0, & \text{if } s \notin \text{Bad} \\ 1, & \text{if } s \in \text{Bad} \end{cases}$$

PrIC3

$\text{MC} = (S, s_I, P)$ $\quad \text{Bad} \subseteq S \quad$ $\lambda = 0.7$

1. Initiality: $F_0 = [\text{Bad}] = \Phi(\mathbf{0})$
2. Chain-Property: $\forall 0 \leq i < k \colon F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k \colon F_i[s_I] \leq 0.7$
4. Relative inductivity: $\forall 0 \leq i < k \colon \Phi(F_i) \leq F_{i+1}$



$$F_3 = (\ \underset{0.7}{s_I}\ ,\ \underset{1}{s_1}\ ,\ \underset{1}{s_2}\ ,\ \underset{1}{s_3}\ ,\ \underset{1}{s_4}\ ,\ \underset{1}{s_5}\ )$$

$$F_2 = (\ \underset{0.7}{s_I}\ ,\ \underset{0.4}{s_1}\ ,\ \underset{1}{s_2}\ ,\ \underset{1}{s_3}\ ,\ \underset{1}{s_4}\ ,\ \underset{1}{s_5}\ )$$

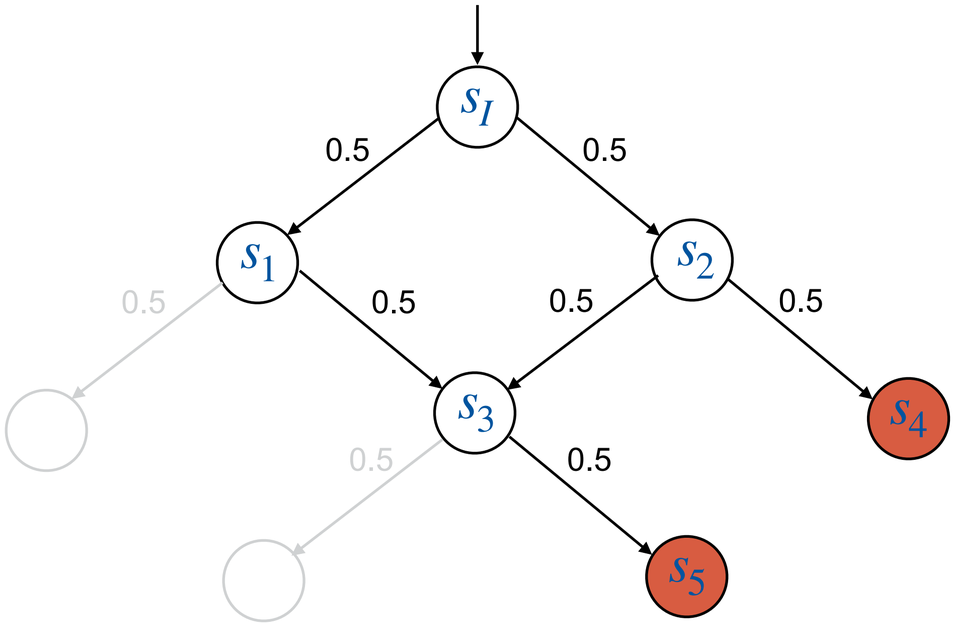
$$F_1 = (\ \underset{0.7}{s_I}\ ,\ \underset{0.4}{s_1}\ ,\ \underset{1}{s_2}\ ,\ \underset{0.8}{s_3}\ ,\ \underset{1}{s_4}\ ,\ \underset{1}{s_5}\ )$$

$$F_0(s) = \begin{cases} 0, & \text{if } s \notin \text{Bad} \\ 1, & \text{if } s \in \text{Bad} \end{cases}$$

PrIC3

$\text{MC} = (S, s_I, P)$ $\quad \text{Bad} \subseteq S \quad$ $\lambda = 0.7$

1. Initiality: $F_0 = [\text{Bad}] = \Phi(\mathbf{0})$
2. Chain-Property: $\forall 0 \leq i < k\colon F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k\colon F_i[s_I] \leq 0.7$
4. Relative inductivity: $\forall 0 \leq i < k\colon \Phi(F_i) \leq F_{i+1}$



$$F_4 = (\ \underset{1}{s_I}\ ,\ \underset{1}{s_1}\ ,\ \underset{1}{s_2}\ ,\ \underset{1}{s_3}\ ,\ \underset{1}{s_4}\ ,\ \underset{1}{s_5}\ )$$

$$F_3 = (\ \underset{0.7}{s_I}\ ,\ \underset{1}{s_1}\ ,\ \underset{1}{s_2}\ ,\ \underset{1}{s_3}\ ,\ \underset{1}{s_4}\ ,\ \underset{1}{s_5}\ )$$

$$F_2 = (\ \underset{0.7}{s_I}\ ,\ \underset{0.4}{s_1}\ ,\ \underset{1}{s_2}\ ,\ \underset{1}{s_3}\ ,\ \underset{1}{s_4}\ ,\ \underset{1}{s_5}\ )$$

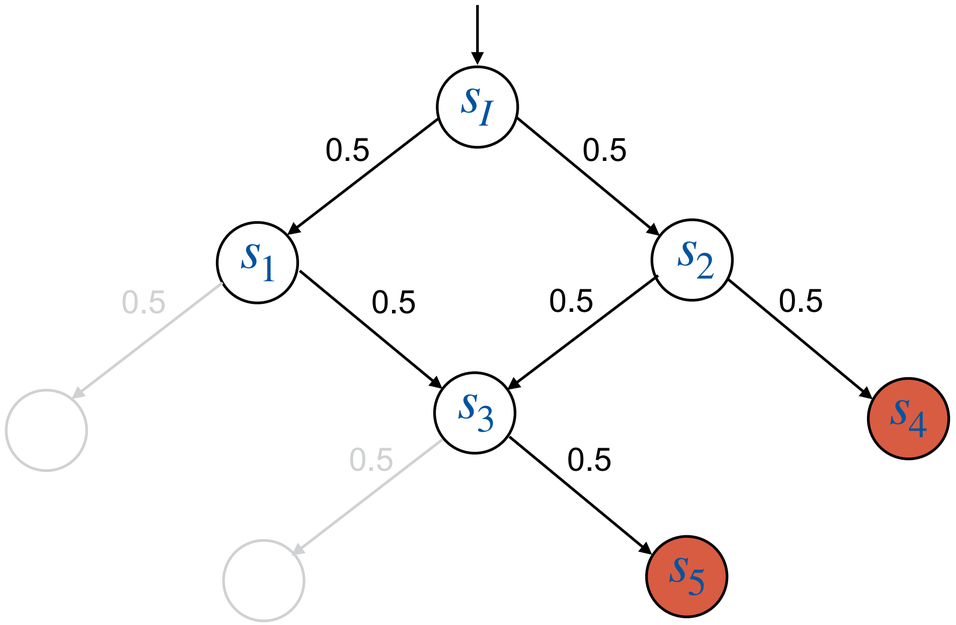
$$F_1 = (\ \underset{0.7}{s_I}\ ,\ \underset{0.4}{s_1}\ ,\ \underset{1}{s_2}\ ,\ \underset{0.8}{s_3}\ ,\ \underset{1}{s_4}\ ,\ \underset{1}{s_5}\ )$$

$$F_0(s) = \begin{cases} 0, & \text{if } s \notin \text{Bad} \\ 1, & \text{if } s \in \text{Bad} \end{cases}$$

PrIC3

$\text{MC} = (S, s_I, P)$ $\quad \text{Bad} \subseteq S \quad \lambda = 0.7$

1. Initiality: $F_0 = [\text{Bad}] = \Phi(\mathbf{0})$
2. Chain-Property: $\forall 0 \leq i < k\colon F_i \leq F_{i+1}$
3. Frame-safety: $\forall 0 \leq i \leq k\colon F_i[s_I] \leq 0.7$
4. Relative inductivity: $\forall 0 \leq i < k\colon \Phi(F_i) \leq F_{i+1}$



$$F_4 = (\ \underset{s_I}{0.7}\ ,\ \underset{s_1}{1}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

$$F_3 = (\ \underset{s_I}{0.7}\ ,\ \underset{s_1}{0.4}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{1}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

$$F_2 = (\ \underset{s_I}{0.7}\ ,\ \underset{s_1}{0.4}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{0.8}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

$$F_1 = (\ \underset{s_I}{0.7}\ ,\ \underset{s_1}{0.4}\ ,\ \underset{s_2}{1}\ ,\ \underset{s_3}{0.8}\ ,\ \underset{s_4}{1}\ ,\ \underset{s_5}{1}\ )$$

$$F_0(s) = \begin{cases} 0, & \text{if } s \notin \text{Bad} \\ 1, & \text{if } s \in \text{Bad} \end{cases}$$

Empirical Results

Table 1. Empirical results. Run times are in seconds; time out = 15 minutes.

	$\lvert S\rvert$	$\Pr^{\max}(s_I \models \Diamond B)$	λ	w/o	$\lvert sub\rvert$	pol	$\lvert sub\rvert$	$\text{Storm}_{\text{sparse}}$	Storm_{dd}
BRP	10^3	0.035	0.01	**51.3**	324	TO	–	<0.1	0.18
			0.005	**10.9**	188	TO	–	<0.1	0.1
ZeroConf	10^9	~0.55	0.9	TO	–	**3.7**	0	MO	TO
			0.75	TO	–	**3.4**	0	MO	TO
			0.52	TO	–	TO	– -	MO	TO
			0.45	<**0.1**	1	<**0.1**	1	MO	TO
Chain	10^{12}	0.394	0.9	TO	–	**6.4**	0	MO	TO
			0.4	TO	–	**6.0**	0	MO	TO

http://www.stormchecker.org/ http://qcomp.org/

Advanced PrIC3 Challenges

- Refutation
  - Single paths from s_I to Bad do generally not suffice
- SMT Encoding
- How to find oracles?
  - Solve an abstraction of the state space
  - Compute Q-Table with deep RL
  - Explore part of the system
  - Do some iterations of Value iteration with BDDs

See paper for further reading.

Conclusion

- PrIC3: A truly quantitative extension of IC3
  - Probabilistic invariants
  - PrIC3 invariants
  - PrIC3 requires a heuristic

Thanks!

Future Work

- Finding good heuristics/oracles
- Generalization
- Infinite systems?