Modeling and Verification of Probabilistic Systems

Lecture 3: Reachability Probabilities

Joost-Pieter Katoen

Lehrstuhl für Informatik 2
Software Modeling and Verification Group

http://www-i2.informatik.rwth-aachen.de/i2/mvps11/

April 12, 2011

Overview

Overview

DTMCs — A transition system perspective

Discrete-time Markov chain

A DTMC $\mathcal{D}$ is a tuple $(S, \mathbf{P}, \iota_{\text{init}}, AP, L)$ with:

- S is a countable nonempty set of states
- $\mathbf{P} : S \times S \rightarrow [0, 1]$, transition probability function s.t. $\sum_{s'} \mathbf{P}(s, s') = 1$
- $\iota_{\text{init}} : S \rightarrow [0, 1]$, the initial distribution with $\sum_{s \in S} \iota_{\text{init}}(s) = 1$
- AP is a set of atomic propositions.
- $L : S \rightarrow 2^{AP}$, the labeling function, assigning to state s, the set $L(s)$ of atomic propositions that are valid in s.

Initial states

- $\iota_{\text{init}}(s)$ is the probability that DTMC $\mathcal{D}$ starts in state s
- the set $\{ s \in S \mid \iota_{\text{init}}(s) > 0 \}$ are the possible initial states.

Paths in a DTMC

State graph

The *state graph* of DTMC $\mathcal{D}$ is a digraph $G = (V, E)$ with V are the states of $\mathcal{D}$, and $(s, s') \in E$ iff $\mathbf{P}(s, s') > 0$.

Paths

Paths in $\mathcal{D}$ are maximal (i.e., infinite) paths in its state graph. Thus, a path is an infinite sequence of states $s_0 s_1 s_2 \ldots\ldots$ with $\mathbf{P}(s_i, s_{i+1}) > 0$ for all i. Let $\pi[i] = s_i$.

Let $Paths(\mathcal{D})$ denote the set of paths in $\mathcal{D}$, and $Paths^*(\mathcal{D})$ the set of finite prefixes thereof.

Direct successors and predecessors

$Post(s) = \{ s' \in S \mid \mathbf{P}(s, s') > 0 \}$ and $Pre(s) = \{ s' \in S \mid \mathbf{P}(s', s) > 0 \}$ are the set of direct successors and predecessors of s respectively. $Post^*(s)$ and $Pre^*(s)$ are the reflexive and transitive closure of *Post* and *Pre*.

Paths and probabilities

To reason quantitatively about the behavior of a DTMC, we need to define a probability space over its paths.

Intuition

For a given state s in DTMC $\mathcal{D}$:

- Sample space := set of all infinite paths starting in s
- Events := sets of infinite paths starting in s
- Basic events := cylinder sets
- Cylinder set of finite path $\hat{\pi}$:= set of all infinite continuations of $\hat{\pi}$

Probability measure on DTMCs

Cylinder set

The *cylinder set* of finite path $\hat{\pi} = s_0\, s_1 \ldots s_n \in Paths^*(\mathcal{D})$ is defined by:

$$Cyl(\hat{\pi}) \;=\; \{ \pi \in Paths(\mathcal{D}) \mid \hat{\pi} \text{ is a prefix of } \pi \}$$

The cylinder set spanned by finite path $\hat{\pi}$ thus consists of all infinite paths that have prefix $\hat{\pi}$. Cylinder sets serve as basic events of the smallest σ-algebra on $Paths(\mathcal{D})$.

σ-algebra of a DTMC

The σ-algebra associated with DTMC $\mathcal{D}$ is the smallest σ-algebra that contains all cylinder sets $Cyl(\hat{\pi})$ where $\hat{\pi}$ ranges over all finite path fragments in $\mathcal{D}$.

Probability measure on DTMCs

Cylinder set

The cylinder set of finite path $\hat{\pi} = s_0\, s_1 \ldots s_n \in Paths^*(\mathcal{D})$ is defined by:

$$Cyl(\hat{\pi}) \;=\; \{ \pi \in Paths(\mathcal{D}) \mid \hat{\pi} \text{ is a prefix of } \pi \}$$

Probability measure

Pr is the unique *probability measure* on the σ-algebra on $Paths(\mathcal{D})$ defined by:

$$Pr(Cyl(s_0 \ldots s_n)) \;=\; \iota_{\text{init}}(s_0) \cdot \mathbf{P}(s_0\, s_1 \ldots s_n)$$

where $\mathbf{P}(s_0\, s_1 \ldots s_n) \;=\; \prod_{0 \leqslant i < n} \mathbf{P}(s_i, s_{i+1})$ for $n > 0$ and $\mathbf{P}(s_0) = 1$.

Example

Overview

Some events of interest

Let DTMC $\mathcal{D}$ with (possibly infinite) state space S.

(Simple) reachability

Eventually reach a state in $G \subseteq S$. Formally:

$$\Diamond G \;=\; \{ \pi \in Paths(\mathcal{D}) \mid \exists i \in \mathbb{N}.\, \pi[i] \in G \}$$

Invariance, i.e., always stay in state in G:

$$\Box G \;=\; \{ \pi \in Paths(\mathcal{D}) \mid \forall i \in \mathbb{N}.\, \pi[i] \in G \} \;=\; \overline{\Diamond \overline{G}}.$$

Constrained reachability

Or "reach-avoid" properties where states in $F \subseteq S$ are forbidden:

$$\overline{F} \,\mathsf{U}\, G \;=\; \{ \pi \in Paths(\mathcal{D}) \mid \exists i \in \mathbb{N}.\, \pi[i] \in G \wedge \forall j < i.\, \pi[j] \notin F \}$$

More events of interest

Repeated reachability

Repeatedly visit a state in G; formally:

$$\Box\Diamond G \;=\; \{ \pi \in Paths(\mathcal{D}) \mid \forall i \in \mathbb{N}.\, \exists j \geqslant i.\, \pi[j] \in G \}$$

Persistence

Eventually reach in a state in G and always stay there; formally:

$$\Diamond\Box G \;=\; \{ \pi \in Paths(\mathcal{D}) \mid \exists i \in \mathbb{N}.\, \forall j \geqslant i.\, \pi[j] \in G \}$$

Measurability

Measurability theorem

Events $\Diamond G$, $\Box G$, $\overline{F} \, \mathrm{U} \, G$, $\Box\Diamond G$ and $\Diamond\Box G$ are measurable on any DTMC.

Proof:

To show this, every event will be expressed as allowed operations (complement and/or countable unions) of the events — our cylinder sets!— in the σ-algebra on infinite paths in a DTMC.

Note that $\Box G = \overline{\Diamond \overline{G}}$ and $\Diamond\Box G = \overline{\Box\Diamond\overline{G}}$.

It remains to prove the measurability for the remaining three cases.

Proof for $\Diamond G$

Which event (in our σ-algebra) does $\Diamond G$ formally mean?

the union of all cylinders $Cyl(s_0 \ldots s_n)$ where

$s_0 \ldots s_n$ is a finite path in $\mathcal{D}$ with $s_0, \ldots, s_{n-1} \notin G$ and $s_n \in G$, i.e.,

$$\Diamond G = \bigcup_{s_0 \ldots s_n \in Paths^*(\mathcal{D}) \cap (S \setminus G)^* G} Cyl(s_0 \ldots s_n)$$

Thus $\Diamond G$ is measurable.

As all cylinder sets are pairwise disjoint, its probability is defined by:

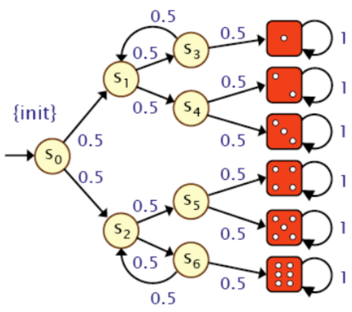
$$Pr(\Diamond G) = \sum_{s_0 \ldots s_n \in Paths^*(\mathcal{D}) \cap (S \setminus G)^* G} Pr(Cyl(s_0 \ldots s_n))$$

$$= \sum_{s_0 \ldots s_n \in Paths^*(\mathcal{D}) \cap (S \setminus G)^* G} \iota_{\text{init}}(s_0) \cdot \mathbf{P}(s_0 \ldots s_n)$$

A similar proof strategy applies to the case $\overline{F} \, \mathrm{U} \, G$.

Proof for $\Box\Diamond G$

Reachability probabilities: Knuth's die



- Consider the event $\Diamond 4$
- Using the previous theorem we obtain:

$$Pr(\Diamond 4) = \sum_{s_0 \ldots s_n \in (S \setminus 4^*)4} \mathbf{P}(s_0 \ldots s_n)$$

- This yields: $\mathbf{P}(s_0 s_2 s_5 4) + \mathbf{P}(s_0 s_2 s_6 s_2 s_5 4) + \ldots\ldots$
- Or: $\sum_{k=0}^{\infty} \mathbf{P}(s_0 s_2 (s_6 s_2)^k s_5 4)$
- Or: $\frac{1}{8} \sum_{k=0}^{\infty} \left(\frac{1}{4}\right)^k$
- Geometric series: $\frac{1}{8} \cdot \frac{1}{1 - \frac{1}{4}} = \frac{1}{8} \cdot \frac{4}{3} = \frac{1}{6}$

There is however an simpler way to obtain reachability probabilities!

Reachability probabilities in finite DTMCs

Problem statement

Let $\mathcal{D}$ be a DTMC with finite state space S, $s \in S$ and $G \subseteq S$.

Aim: determine $Pr(s \models \Diamond G) = Pr_s(\Diamond G) = Pr_s\{\, \pi \in Paths(s) \mid \pi \models \Diamond G \,\}$

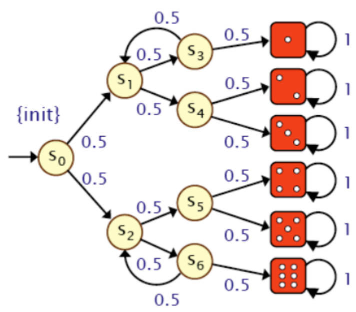
where Pr_s is the probability measure in $\mathcal{D}$ with single initial state s.

Characterisation of reachability probabilities

- Let variable $x_s = Pr(s \models \Diamond G)$ for any state s
  - if G is not reachable from s, then $x_s = 0$
  - if $s \in G$ then $x_s = 1$
- For any state $s \in Pre^*(G) \setminus G$:

$$x_s = \underbrace{\sum_{t \in S \setminus G} \mathbf{P}(s,t) \cdot x_t}_{\text{reach } G \text{ via } t \in S \setminus G} + \underbrace{\sum_{u \in G} \mathbf{P}(s,u)}_{\text{reach } G \text{ in one step}}$$

Reachability probabilities: Knuth's die



- Consider the event $\Diamond 4$
- Using the previous characterisation we obtain:

$x_1 = x_2 = x_3 = x_5 = x_6 = 0$ and $x_4 = 1$

$x_{s_1} = x_{s_3} = x_{s_4} = 0$

$x_{s_0} = \frac{1}{2} x_{s_1} + \frac{1}{2} x_{s_2}$

$x_{s_2} = \frac{1}{2} x_{s_5} + \frac{1}{2} x_{s_6}$

$x_{s_5} = \frac{1}{2} x_5 + \frac{1}{2} x_4$

$x_{s_6} = \frac{1}{2} x_{s_2} + \frac{1}{2} x_6$

- Gaussian elimination yields:

$x_{s_5} = \frac{1}{2}$, $x_{s_2} = \frac{1}{3}$, $x_{s_6} = \frac{1}{6}$, and $\boxed{x_{s_0} = \frac{1}{6}}$

Linear equation system

Reachability probabilities as linear equation system

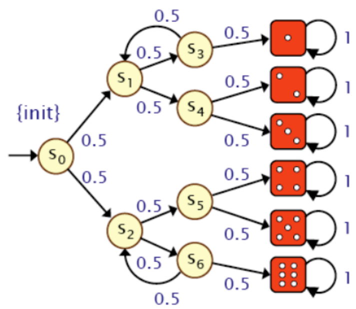
- Let $S_? = Pre^*(G) \setminus G$, the states that can reach G by > 0 steps
- $\mathbf{A} = \big(\mathbf{P}(s,t)\big)_{s,t \in \tilde{S}}$, the transition probabilities in $S_?$
- $\mathbf{b} = (b_s)_{s \in S_?}$, the probs to reach G in 1 step, i.e., $b_s = \sum_{u \in G} \mathbf{P}(s,u)$

Then: $\mathbf{x} = (x_s)_{s \in S_?}$ with $x_s = Pr(s \models \Diamond G)$ is the unique solution of:

$$\mathbf{x} = \mathbf{A} \cdot \mathbf{x} + \mathbf{b} \quad \text{or} \quad (\mathbf{I} - \mathbf{A}) \cdot \mathbf{x} = \mathbf{b}$$

where $\mathbf{I}$ is the identity matrix of cardinality $|S_?| \times |S_?|$.

Reachability probabilities: Knuth's die



- Consider the event $\Diamond 4$
- $S_? = \{\, s_0, s_2, s_5, s_6 \,\}$

$$\begin{pmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 1 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 1 & 0 \\ 0 & -\frac{1}{2} & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_{s_0} \\ x_{s_2} \\ x_{s_5} \\ x_{s_6} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \frac{1}{2} \\ 0 \end{pmatrix}$$

- Gaussian elimination yields:

$x_{s_5} = \frac{1}{2}$, $x_{s_2} = \frac{1}{3}$, $x_{s_6} = \frac{1}{6}$, and $\boxed{x_{s_0} = \frac{1}{6}}$

Constrained reachability probabilities

Problem statement

Let $\mathcal{D}$ be a DTMC with finite state space S, $s \in S$ and $\overline{F}, G \subseteq S$.

Aim: $Pr(s \models \overline{F} \,\mathsf{U}\, G) \;=\; Pr_s(\overline{F} \,\mathsf{U}\, G) \;=\; Pr_s\{\, \pi \in Paths(s) \mid \pi \models \overline{F} \,\mathsf{U}\, G \,\}$

where Pr_s is the probability measure in $\mathcal{D}$ with single initial state s.

Characterisation of constrained reachability probabilities

- Let variable $x_s = Pr(s \models \overline{F} \,\mathsf{U}\, G)$ for any state s
  - if G is not reachable from s via $\overline{F}$, then $x_s = 0$
  - if $s \in G$ then $x_s = 1$
- For any state $s \in (Pre^*(G) \cap \overline{F}) \setminus G$:

$$x_s \;=\; \sum_{t \in S \setminus G} \mathbf{P}(s,t) \cdot x_t \;+\; \sum_{u \in G} \mathbf{P}(s,u)$$

Remark

In the previous characterisation we basically set:

- $S_{=1} \;=\; G$
- $S_{=0} \;=\; \{\, s \in S \mid Pr(\overline{F} \,\mathsf{U}\, G) = 0 \,\}$
- $S_? \;=\; S \setminus (S_{=0} \cup S_{=1})$

In fact any partition of S satisfying the following constraints will do:

- $G \subseteq S_{=1} \subseteq \{\, s \in S \mid Pr(\overline{F} \,\mathsf{U}\, G) = 1 \,\}$
- $F \setminus G \subseteq S_{=0} \subseteq \{\, s \in S \mid Pr(\overline{F} \,\mathsf{U}\, G) = 0 \,\}$
- $S_? \;=\; S \setminus (S_{=0} \cup S_{=1})$

In practice, $S_{=0}$ and $S_{=1}$ should be chosen as large as possible, as then $S_?$ is of minimal size, and the smallest linear equation system needs to be solved.

Thus $S_{=0} \;=\; \{\, s \in S \mid Pr(\overline{F} \,\mathsf{U}\, G) = 0 \,\}$ and $S_{=1} \;=\; \{\, s \in S \mid Pr(\overline{F} \,\mathsf{U}\, G) = 1 \,\}$.

These sets can easily be determined in linear time by a graph analysis.

Iteratively computing reachability probabilities

Theorem

The vector $\mathbf{x} = \big(Pr(s \models \overline{F} \,\mathsf{U}\, G)\big)_{s \in S_?}$ is the *unique* solution of:

$$\mathbf{y} \;=\; \mathbf{A} \cdot \mathbf{y} + \mathbf{b}$$

with $\mathbf{A}$ and $\mathbf{b}$ as defined before.

Furthermore, let:

$$\mathbf{x}^{(0)} = \mathbf{0} \quad \text{and} \quad \mathbf{x}^{(i+1)} \;=\; \mathbf{A} \cdot \mathbf{x}^{(i)} + \mathbf{b} \text{ for } 0 \leqslant i.$$

Then:

1. $\mathbf{x}^{(n)}(s) \;=\; Pr(s \models \overline{F} \,\mathsf{U}^{\leqslant n}\, G)$ for $s \in S_?$
2. $\mathbf{x}^{(0)} \leqslant \mathbf{x}^{(1)} \leqslant \mathbf{x}^{(2)} \leqslant \ldots \leqslant \mathbf{x}$
3. $\mathbf{x} = \lim_{n \to \infty} \mathbf{x}^{(n)}$

where $\overline{F} \,\mathsf{U}^{\leqslant n} G$ contains those paths that reach G via $\overline{F}$ within n steps.

Proof

Remark

Iterative algorithms to compute x

There are various algorithms to compute $\mathbf{x} = \lim_{n\to\infty} \mathbf{x}^{(n)}$ where:

$$\mathbf{x}^{(0)} = \mathbf{0} \quad \text{and} \quad \mathbf{x}^{(i+1)} \;=\; \mathbf{A}{\cdot}\mathbf{x}^{(i)} + \mathbf{b} \text{ for } 0 \leqslant i.$$

The Power method computes vectors $\mathbf{x}^{(0)}, \mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots$ and aborts if:

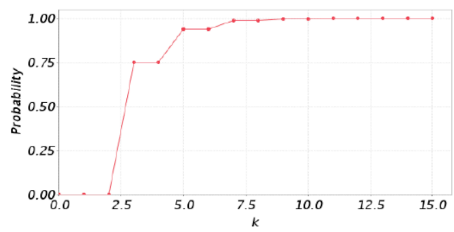
$$\max_{s\in S_?} \left| x_s^{(n+1)} - x_s^{(n)} \right| \; < \; \varepsilon \quad \text{for some small tolerance } \varepsilon$$

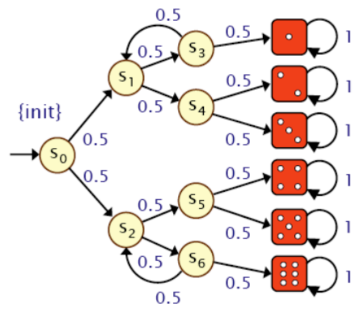
This technique guarantees convergence.

Alternative iterative techniques: e.g., Jacobi or Gauss-Seidel, successive overrelaxation (SOR). Details of these techniques fall outside the scope of these lecture series.

Example: Knuth's die

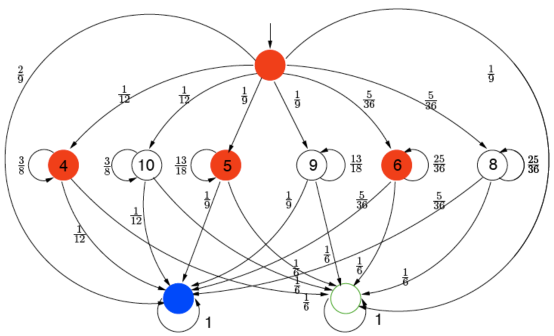
- Let $G = \{1, 2, 3, 4, 5, 6\}$
- Then $Pr(s_0 \models \Diamond G) = 1$
- And $Pr(s_0 \models \Diamond^{\leqslant k} G)$ for $k \in \mathbb{N}$ is given by:





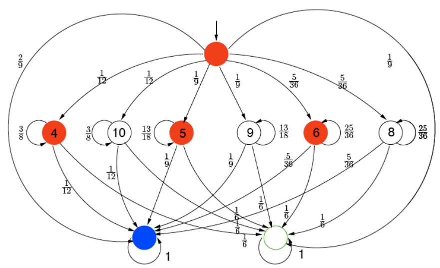
Example: Craps game

- $Pr(start \models R \, \mathrm{U}^{\leqslant n} \, G)$
- $S_{=0} = \{8, 9, 10, lost\}$
- $S_{=1} = \{won\}$
- $S_? = \{start, 4, 5, 6\}$



Example: Craps game

- $start < 4 < 5 < 6$
- $\mathbf{A} = \frac{1}{36}\begin{pmatrix} 0 & 3 & 4 & 5 \\ 0 & 27 & 0 & 0 \\ 0 & 0 & 26 & 0 \\ 0 & 0 & 0 & 25 \end{pmatrix}$
- $\mathbf{b} = \frac{1}{36}\begin{pmatrix} 8 \\ 3 \\ 4 \\ 5 \end{pmatrix}$



$$\mathbf{x}^{(0)} = \mathbf{0} \quad \text{and} \quad \mathbf{x}^{(i+1)} \;=\; \mathbf{A}\mathbf{x}^{(i)} + \mathbf{b} \text{ for } 0 \leqslant i < n.$$

Example: Craps game

$$\mathbf{x}^{(2)} = \underbrace{\frac{1}{36}\begin{pmatrix}0&3&4&5\\0&27&0&0\\0&0&26&0\\0&0&0&25\end{pmatrix}}_{\mathbf{A}} \cdot \underbrace{\frac{1}{36}\begin{pmatrix}8\\3\\4\\5\end{pmatrix}}_{\mathbf{x}^{(1)}} + \underbrace{\frac{1}{36}\begin{pmatrix}8\\3\\4\\5\end{pmatrix}}_{\mathbf{b}} = \left(\frac{1}{36}\right)^2 \begin{pmatrix}338\\189\\248\\305\end{pmatrix}$$

Recall: transient probability distribution

Transient distribution

$\mathbf{P}^n(s,t)$ equals the probability of being in state t after n steps given that the computation starts in s.

The probability of DTMC $\mathcal{D}$ being in state t after exactly n transitions is:

$$\Theta_n^{\mathcal{D}}(t) \;=\; \sum_{s \in S} \iota_{\text{init}}(s) \cdot \mathbf{P}^n(s,t) \;=$$

The function $\Theta_n^{\mathcal{D}}$ is the *transient state distribution* at epoch n of DTMC $\mathcal{D}$.

When considering $\Theta_n^{\mathcal{D}}$ as vector $(\Theta_n^{\mathcal{D}})_{t \in S}$ we have:

$$\Theta_n^{\mathcal{D}} \;=\; \iota_{\text{init}} \cdot \underbrace{\mathbf{P} \cdot \mathbf{P} \cdot \ldots \cdot \mathbf{P}}_{n \text{ times}} \;=\; \iota_{\text{init}} \cdot \mathbf{P}^n.$$

Computation: $\Theta_0^{\mathcal{D}} = \iota_{\text{init}}$ and $\Theta_{n+1}^{\mathcal{D}} = \Theta_n^{\mathcal{D}} \cdot \mathbf{P}$ for $n \geqslant 0$.

Reachability probability = transient probabilities

Aim

Compute $Pr(\Diamond^{\leqslant n} G)$ in DTMC $\mathcal{D}$. Observe that once a path π reaches G, then the remaining behaviour along π is not important. This suggests to make all states in G absorbing.

Let DTMC $\mathcal{D} = (S, \mathbf{P}, \iota_{\text{init}}, AP, L)$ and $G \subseteq S$. The DTMC $\mathcal{D}[G] = (S, \mathbf{P}_G, \iota_{\text{init}}, AP, L)$ with $\mathbf{P}_G(s,t) = \mathbf{P}(s,t)$ if $s \notin G$ and $\mathbf{P}_G(s,s) = 1$ if $s \in G$.

All outgoing transitions of $s \in G$ are replaced by a single self-loop at s.

Lemma

$$\underbrace{Pr(\Diamond^{\leqslant n} G)}_{\text{reachability in } \mathcal{D}} \;=\; \underbrace{Pr(\Diamond^{= n} G)}_{\text{reachability in } \mathcal{D}[G]} \;=\; \underbrace{\iota_{\text{init}} \cdot \mathbf{P}_G^n}_{\text{in } \mathcal{D}[G]} \;=\; \Theta_n^{\mathcal{D}[G]}$$

Constrained reachability = transient probabilities

Aim

Compute $Pr(\overline{F} \, \mathsf{U}^{\leqslant n} \, G)$ in DTMC $\mathcal{D}$. Observe (as before) that once a path π reaches G, then the remaining behaviour along π is not important. Now also observe that once $s \in F \setminus G$ is reached, then the remaining behaviour along π is not important. This suggests to make all states in G and $F \setminus G$ absorbing.

Lemma

$$\underbrace{Pr(\overline{F} \, \mathsf{U}^{\leqslant n} \, G)}_{\text{reachability in } \mathcal{D}} \;=\; \underbrace{Pr(\Diamond^{= n} G)}_{\text{reachability in } \mathcal{D}[F \cup G]} \;=\; \underbrace{\iota_{\text{init}} \cdot \mathbf{P}_{F \cup G}^n}_{\text{in } \mathcal{D}[F \cup G]} \;=\; \Theta_n^{\mathcal{D}[F \cup G]}$$

Example: Craps game