Probabilistic Models and Their Verification

David N. Jansen
Informatics for Technical Applications
Radboud University Nijmegen

September 18, 2007

Overview

Notation

$P(A)$	probability that A happens
$P(A, B)$	probability that both A and B happen
$P(A\|B)$	probability that A happens under the condition that B has happened

Notation

$P(A)$	probability that A happens
$P(A, B)$	probability that both A and B happen
$P(A\|B)$	probability that A happens under the condition that B has happened

Conditional Probability

$$P(A|B) = \frac{P(A, B)}{P(B)}$$

σ-Algebra

Let Ω be a set, the sample space. We assign probabilities to subsets of Ω in a systematic way.

Definition

A σ-algebra $\mathcal{A}$ is a set of subsets:

- $\Omega \in \mathcal{A}$
- $A \in \mathcal{A} \rightarrow \Omega \setminus A \in \mathcal{A}$
- $A_i \in \mathcal{A}$ for all $i = 1, 2, \ldots \rightarrow \bigcup_{i=1}^{\infty} A_i \in \mathcal{A}$

Definition

A measurable space is a pair $(\Omega, \mathcal{A})$ where $\mathcal{A}$ is a σ-algebra over Ω.

Example: Borel-σ-algebra

- $\Omega = \mathbb{R}$
- $\mathcal{B}$ = the smallest σ-algebra that contains all intervals $[r, s)$ for $r, s \in \mathbb{R}$
- The standard σ-algebra for the real numbers
- Émile Borel, French mathematician, 1871–1956, wrote *Le Hasard*

Measure Space

Definition

A measure is a function $\mu : \mathcal{A} \to [0, \infty]$ with the properties:

- $\mu(\emptyset) = 0$
- σ-additivity: If $A_i \in \mathcal{A}$ for all $i = 1, 2, \ldots$ are pairwise disjoint sets, then

$$\mu\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} \mu(A_i)$$

Definition

A measure space is a triple $(\Omega, \mathcal{A}, \mu)$ where $\mathcal{A}$ is a σ-algebra over Ω and $\mu : \mathcal{A} \to [0, \infty]$ is a measure.

Probability Space

Definition

A probability measure is a measure μ with

$$\mu(\Omega) = 1$$

A probability measure is often written P or $\mathbf{P}$.

Definition

A probability space is a measure space $(\Omega, \mathcal{A}, P)$ where P is a probability measure.

Overview

Markov Chains

- A model of the behaviour of a system with discrete states.
- Behaviour := development over time, including the probabilities to move from one state to another.
- Two variants: *discrete* time or *continuous* time
- Special cases of more general stochastic processes.

Discrete Time Markov Chain

Definition

A discrete-time Markov chain consists of

- a set of states S. Often, $S = \{1, 2, \ldots, n\}$.
- a transition probability matrix $\mathbf{P} : S \times S \to [0, 1]$ satisfying, for all $s \in S$,

$$1 = \sum_{s' \in S} \mathbf{P}\left(s, s'\right)$$

- Sometimes, an initial probability distribution $\pi_0 : S \to [0, 1]$ satisfying

$$1 = \sum_{s' \in S} \pi_0(s')$$

Drawing a DTMC

- Draw states as (numbered) circles
- Draw an arrow from i to j is $\mathbf{P}(i,j) > 0$
- Similar to a labelled transition system
- Example, to be drawn on the board:

$$\mathbf{P} = \begin{pmatrix} 0 & 0.2 & 0.3 & 0.5 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

The Behaviour of a DTMC

- The system starts in one of the initial states, chosen based on π_0
- When the system leaves state i, the next state is j with probability $\mathbf{P}(i, j)$.

The Probability Space of a DTMC

Definition

A run is a sequence $(s_0, s_1, \ldots)$.

...meaning: begin in s_0 and proceed from s_i to s_{i+1}.

Definition

A cylinder set $C(s_1, s_2, \ldots, s_n)$ (for $n \geq 0$) is the set of runs:

$$\{(r_1, r_2, \ldots) \mid \forall i \leq n : r_i = s_i\}$$

The cylinder sets generate a σ-algebra.
Cylinder set $C(s_1, s_2, \ldots, s_n)$ has probability:

$$\pi_0(s_1)\mathbf{P}(s_1, s_2)\,\mathbf{P}(s_2, s_3)\cdots\mathbf{P}(s_{n-1}, s_n)$$

DTMC Example: Gambler's ruin

- A gambler plays a game repeatedly
- Each time, he either wins € 1 with probability p or he loses € 1 with probability $1 - p$.
- Plays until he is bankrupt

DTMC Example: Gambler's ruin

- A gambler plays a game repeatedly
- Each time, he either wins € 1 with probability p or he loses € 1 with probability $1 - p$.
- Plays until he is bankrupt or until he is millionaire.

Draw the Markov chain on the board!

Standard Properties of Discrete-Time Markov Chains

Definition

A DTMC is irreducible if every state is reachable from every other state.

Definition

A state s of a DTMC is periodic with period k if any return to state s occurs in some multiple of k steps.
A DTMC is aperiodic if all its states have period 1.
If an aperiodic DTMC is finite, it is also called ergodic.

Analysis of a Markov Chain

Interesting measures:

- Transient state distribution:
  What is the probability to be in state i at time t?

Analysis of a Markov Chain

Interesting measures:

- Transient state distribution:
  What is the probability to be in state i at time t?

- Steady-state distribution:
  What is the probability to be in state i in equilibrium / after a long time ($t \to \infty$)?

Analysis of a Markov Chain

Interesting measures:

- Transient state distribution:
  What is the probability to be in state i at time t?
  $p_i(t)$ and $\pi(t) = (p_1(t), p_2(t), \ldots)$
- Steady-state distribution:
  What is the probability to be in state i in equilibrium / after a long time ($t \to \infty$)?
  p_i and $\pi = (p_1, p_2, \ldots)$

DTMC: Transient State Distribution

- Given: Initial distribution $\pi(0)$ and $\mathbf{P} = \mathbf{P}(1)$
- Requested: Transient probabilities $\pi(t)$, for $t \in \mathbb{N}$

DTMC: Transient State Distribution

- Given: Initial distribution $\pi(0)$ and $\mathbf{P} = \mathbf{P}(1)$
- Requested: Transient probabilities $\pi(t)$, for $t \in \mathbb{N}$
- $\pi(t) = \pi(0) \cdot \mathbf{P}(t) = \pi(0) \cdot \mathbf{P}^t$

DTMC: Steady State Distribution

- Given: Initial distribution $\pi(0)$ and $\mathbf{P} = \mathbf{P}(1)$
- Requested: Steady-state probabilities π

DTMC: Steady State Distribution

- Given: Initial distribution $\pi(0)$ and $\mathbf{P} = \mathbf{P}(1)$
- Requested: Steady-state probabilities π

Theorem

If a DTMC is irreducible and ergodic, it has a steady-state distribution, which does not depend on the initial distribution.

The steady-state distribution is the solution of the equation system:

$$\pi = \pi \cdot \mathbf{P}$$

$$\sum_{s \in S} p_s = 1$$

Labelled Markov Chain

Definition

A labelled DTMC (S, P, L) consists of

- a set of states S
- a transition probability matrix $\mathbf{P}$
- a labelling $L : S \to 2^{AP}$
  where AP are the atomic propositions

Probabilistic Computation Tree Logic

Syntax	**Name**	**Semantics**
a	atomic proposition	$a \in L(s)$
$\neg\varphi$	negation	$s \not\models \varphi$
$\varphi \wedge \psi$	conjunction	both $s \models \varphi$ and $s \models \psi$
$\mathcal{P}_{\geq p}(X\,\varphi)$	next	$\sum_{s' \models \varphi} P(s \to s') \geq p$
$\mathcal{P}_{\geq p}(\varphi\,\mathcal{U}^{\leq k}\,\psi)$	bounded until	see picture
$\mathcal{P}_{\geq p}(\varphi\,\mathcal{U}\,\psi)$	unbounded until	see picture

Example formulas

- $\neg red$
- $\mathcal{P}_{\geq 0.3}\left(red \land green\ \mathcal{U}^{\leq k}\ blue\right)$

Example formulas

- $\neg red$
- $\mathcal{P}_{\geq 0.3}\left(red \wedge green\, \mathcal{U}^{\leq k}\ blue\right)$
- $\mathcal{P}_{\geq 1}\left(true\, \mathcal{U}\ red\right)$

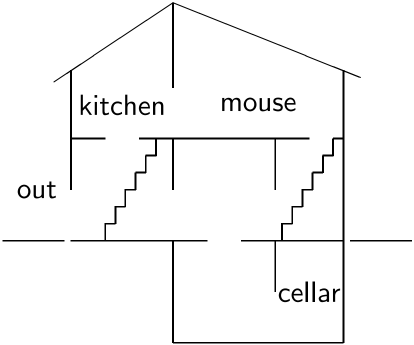
Example formulas

- $\neg \mathit{red}$
- $\mathcal{P}_{\geq 0.3}\left(\mathit{red} \wedge \mathit{green}\ \mathcal{U}^{\leq k}\ \mathit{blue}\right)$
- $\mathcal{P}_{\geq 1}\left(\mathit{true}\ \mathcal{U}\ \mathit{red}\right)$
- $\mathcal{P}_{\geq 0.5}\left(X\ \mathit{green}\right) \wedge \mathit{red}$

Example formulas

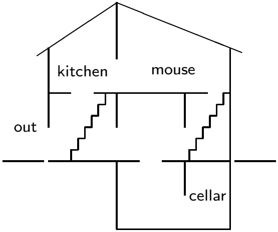
- $\neg \mathit{red}$
- $\mathcal{P}_{\geq 0.3}\left(\mathit{red} \land \mathit{green}\,\mathcal{U}^{\leq k}\ \mathit{blue}\right)$
- $\mathcal{P}_{\geq 1}\left(\mathit{true}\,\mathcal{U}\ \mathit{red}\right)$
- $\mathcal{P}_{\geq 0.5}\left(X\ \mathit{green}\right) \land \mathit{red}$
- $\mathcal{P}_{\geq 0.6}\left(\mathcal{P}_{\geq 0.3}\left(\mathit{true}\,\mathcal{U}\ \mathit{blue}\right)\mathcal{U}^{\leq 10}\ \mathit{blue}\right)$

Mouse Catching



A mouse walks through the house at random. It cannot climb where there are no stairs.
Let's think about the probability that the mouse gets out.
What happens if we place a mouse trap in the kitchen?

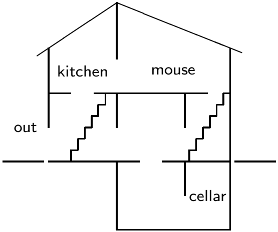
Mouse Catching: Example Formulas



Is the probability that the mouse gets out within 5 steps ≥ 0.2?

$$\mathcal{P}_{\geq 0.2}\left(\mathit{true}\ \mathcal{U}^{\leq 5}\ \mathit{out}\right)$$

Mouse Catching: Example Formulas



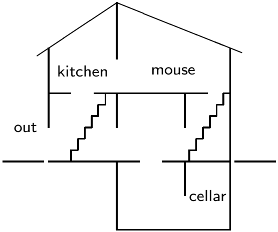
Is the probability that the mouse gets out within 5 steps ≥ 0.2?

$$\mathcal{P}_{\geq 0.2}\left(\mathit{true}\,\mathcal{U}^{\leq 5}\ \mathit{out}\right)$$

Is the probability that the mouse gets out within 5 steps while there is a mouse trap in the kitchen ≥ 0.2?

$$\mathcal{P}_{\geq 0.2}\left(\neg \mathit{kitchen}\,\mathcal{U}^{\leq 5}\ \mathit{out}\right)$$

Mouse Catching: Example Formulas



Is the probability that the mouse gets out within 5 steps ≥ 0.2?

$$\mathcal{P}_{\geq 0.2}\left(\mathit{true}\ \mathcal{U}^{\leq 5}\ \mathit{out}\right)$$

Is the probability that the mouse gets out within 5 steps while there is a mouse trap in the kitchen ≥ 0.2?

$$\mathcal{P}_{\geq 0.2}\left(\neg \mathit{kitchen}\ \mathcal{U}^{\leq 5}\ \mathit{out}\right)$$

Is the probability that the mouse gets out at all ≥ 0.2?

$$\mathcal{P}_{\geq 0.2}\left(\mathit{true}\ \mathcal{U}\ \mathit{out}\right)$$

General Principle of Model Checking

- Input: model (e. g., DTMC)
  and desired property (e. g., PCTL formula)
- Output: “Yes” or “No” (or a probability)

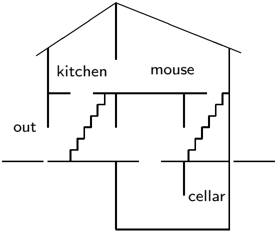
PCTL Model Checking

- Recursion over subformulas!
- For formula φ, we need an algorithm like:
  - Given: satisfaction sets of subformulas of φ
  - Requested: satisfaction set of φ

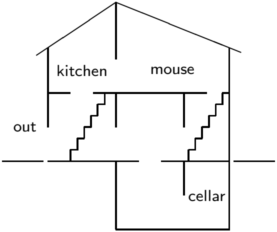
PCTL Model Checking: Example of Recursion

Let's look at the formula:

$$\mathcal{P}_{\geq 0.2}\left(\neg kitchen\ \mathcal{U}^{\leq 5}\ out\right)$$



PCTL Model Checking: Example of Recursion

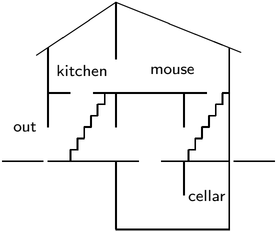


Let's look at the formula:

$$\mathcal{P}_{\geq 0.2}\left(\neg \mathit{kitchen}\, \mathcal{U}^{\leq 5}\ \mathit{out}\right)$$

1. Calculate $\textsc{Sat}\,(\mathit{kitchen})$

PCTL Model Checking: Example of Recursion

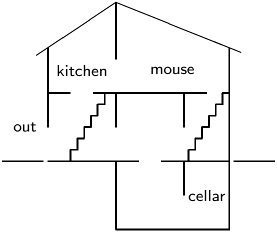


Let's look at the formula:

$$\mathcal{P}_{\geq 0.2}\left(\neg kitchen\,\mathcal{U}^{\leq 5}\ out\right)$$

1. Calculate $\text{SAT}\,(kitchen)$
2. Calculate $\text{SAT}\,(\neg kitchen)$ using 1

PCTL Model Checking: Example of Recursion



Let's look at the formula:

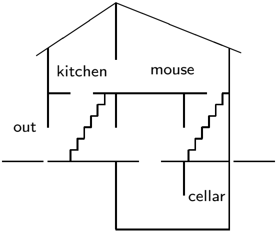
$$\mathcal{P}_{\geq 0.2}\left(\neg kitchen\, \mathcal{U}^{\leq 5}\ out\right)$$

1. Calculate $\textsc{Sat}\,(kitchen)$
2. Calculate $\textsc{Sat}\,(\neg kitchen)$ using 1
3. Calculate $\textsc{Sat}\,(out)$

PCTL Model Checking: Example of Recursion

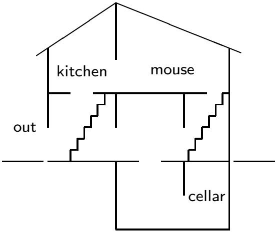
Let's look at the formula:

$$\mathcal{P}_{\geq 0.2}\left(\neg kitchen\,\mathcal{U}^{\leq 5}\ out\right)$$



1. Calculate $\mathrm{SAT}(kitchen)$
2. Calculate $\mathrm{SAT}(\neg kitchen)$ using 1
3. Calculate $\mathrm{SAT}(out)$
4. Calculate the probabilities of $\neg kitchen\,\mathcal{U}^{\leq 5}\ out$ using 2 and 3

PCTL Model Checking: Example of Recursion



Let's look at the formula:

$$\mathcal{P}_{\geq 0.2}\left(\neg kitchen\,\mathcal{U}^{\leq 5}\ out\right)$$

1. Calculate $\mathrm{SAT}\,(kitchen)$
2. Calculate $\mathrm{SAT}\,(\neg kitchen)$ using 1
3. Calculate $\mathrm{SAT}\,(out)$
4. Calculate the probabilities of $\neg kitchen\,\mathcal{U}^{\leq 5}\ out$ using 2 and 3
5. Calculate $\mathrm{SAT}\left(\mathcal{P}_{\geq 0.2}\left(\neg kitchen\,\mathcal{U}^{\leq 5}\ out\right)\right)$ using 4

Checking Simple Operators

- Atomic proposition: $\textsc{Sat}(a) = \{s \in S \mid a \in L(s)\}$
- Negation: $\textsc{Sat}(\neg\varphi) = S \setminus \textsc{Sat}(\varphi)$
- Conjunction: $\textsc{Sat}(\varphi \wedge \psi) = \textsc{Sat}(\varphi) \cap \textsc{Sat}(\psi)$

Next Operator

- For all $s \in S$, let

$$i_{\varphi}(s) := \begin{cases} 1 & \text{if } s \in \textsc{Sat}(\varphi) \\ 0 & \text{otherwise} \end{cases}$$

- $P(X\,\varphi) = \mathbf{P} \cdot i_{\varphi}$
- $\textsc{Sat}(\mathcal{P}_{\geq p}(X\,\varphi)) = \{s \mid P(X\,\varphi)_i \geq p\}$

Bounded Until Operator

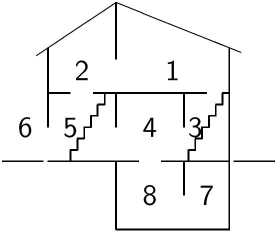
$$\mathrm{Sat}\left(\mathcal{P}_{\geq p}\left(\varphi\,\mathcal{U}^{\leq k}\,\psi\right)\right) = \left\{s \mid P\left(\varphi\,\mathcal{U}^{\leq k}\,\psi\right)_s \geq p\right\}$$

To calculate $P\left(\varphi\,\mathcal{U}^{\leq k}\,\psi\right)$:

- Make all states in $\mathrm{Sat}\left(\psi\right)$ absorbing
  because they satisfy the formula trivially
- Make all states $\notin \mathrm{Sat}\left(\varphi\right) \cup \mathrm{Sat}\left(\psi\right)$ absorbing
  because they falsify the formula trivially
- Let $\tilde{\mathbf{P}}$ be the resulting matrix
- $P\left(\varphi\,\mathcal{U}^{\leq k}\,\psi\right) = \tilde{\mathbf{P}}^k \cdot i_\psi$

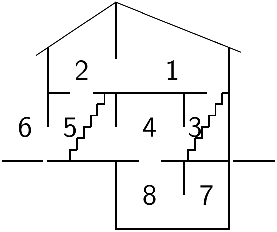
Mouse Catching: Bounded Until Example

$$\mathcal{P}_{\geq 0.2}\left(true\ \mathcal{U}^{\leq 5}\ out\right)$$



Mouse Catching: Bounded Until Example

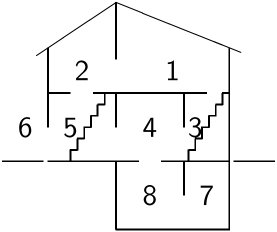
$$\mathcal{P}_{\geq 0.2}\left(\mathit{true}\ \mathcal{U}^{\leq 5}\ \mathit{out}\right)$$



$$\mathbf{P} = \begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & 0 & \frac{1}{3} \\ 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Mouse Catching: Bounded Until Example

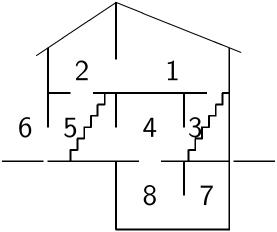
$$\mathcal{P}_{\geq 0.2}\left(\mathit{true}\ \mathcal{U}^{\leq 5}\ \mathit{out}\right)$$



$$\tilde{\mathbf{P}} = \begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & 0 & \frac{1}{3} \\ 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & 0 \\ \color{red}{0} & \color{red}{0} & \color{red}{0} & \color{red}{0} & \color{red}{0} & \color{red}{1} & \color{red}{0} & \color{red}{0} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

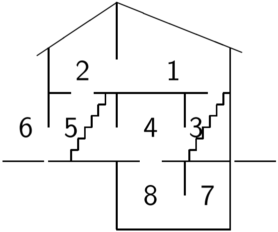
Mouse Catching: Bounded Until Example

$$\mathcal{P}_{\geq 0.2}\left(true\ \mathcal{U}^{\leq 5}\ out\right)$$



$$\tilde{\mathbf{P}}^5 \cdot i_{out} =$$
$$= (0.18, 0.27, 0.14, 0.17, 0.47, 1, 0, 0)$$

Mouse Catching: Bounded Until Example



$$\mathcal{P}_{\geq 0.2}\left(true\,\mathcal{U}^{\leq 5}\ out\right)$$

$$\tilde{\mathbf{P}}^5 \cdot i_{out} =$$
$$= (0.18, 0.27, 0.14, 0.17, 0.47, 1, 0, 0)$$

$$\textsc{Sat}\left(\mathcal{P}_{\geq 0.2}\left(true\,\mathcal{U}^{\leq 5}\ out\right)\right) = \{2, 5, 6\}$$

Unbounded Until Operator

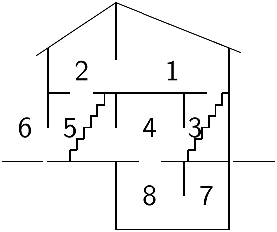
$$\text{Sat}\left(\mathcal{P}_{\geq p}\left(\varphi\, \mathcal{U}\ \psi\right)\right) = \left\{s \mid P\left(\varphi\, \mathcal{U}\ \psi\right)_s \geq p\right\}$$

$P\left(\varphi\, \mathcal{U}\ \psi\right)$ satisfies the equation system:

$$P\left(\varphi\, \mathcal{U}\ \psi\right)_s = \begin{cases} 1 & \text{if } s \in \text{Sat}\left(\psi\right) \\ 0 & \text{if } s \notin \text{Sat}\left(\varphi\right) \cup \text{Sat}\left(\psi\right) \\ \sum_{s' \in S} \mathbf{P}\left(s, s'\right) P\left(\varphi\, \mathcal{U}\ \psi\right)_{s'} & \text{otherwise} \end{cases}$$

- Equation system is ambiguous if $\varphi \wedge \neg\psi$-traps (BSCCs) exist
- Can be repaired by:
  - Take the minimal solution; or
  - Change the equation system: $P\left(\varphi\, \mathcal{U}\ \psi\right)_s = 0$ also if s is in such a trap

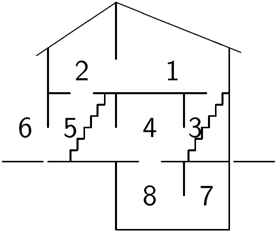
Mouse Catching: Unbounded Until Example



$$\mathcal{P}_{\geq 0.2}\,(\neg kitchen\,\mathcal{U}\;\; out)$$

Mouse Catching: Unbounded Until Example

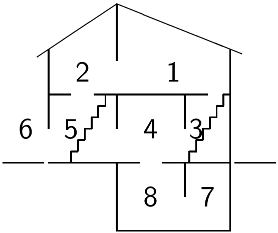
$$\mathcal{P}_{\geq 0.2}\,(\neg kitchen\;\mathcal{U}\;\,out)$$



$$x_1 = \tfrac{1}{2}x_2 + \tfrac{1}{2}x_3$$
$$x_2 = 0$$
$$x_3 = \tfrac{1}{2}x_1 + \tfrac{1}{2}x_4$$
$$x_4 = \tfrac{1}{3}x_3 + \tfrac{1}{3}x_5 + \tfrac{1}{3}x_8$$
$$x_5 = \tfrac{1}{3}x_2 + \tfrac{1}{3}x_4 + \tfrac{1}{3}x_6$$
$$x_6 = 1$$
$$x_7 = x_8$$
$$x_8 = x_7$$

Mouse Catching: Unbounded Until Example

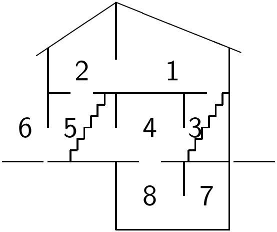
$$\mathcal{P}_{\geq 0.2}\,(\neg kitchen\;\mathcal{U}\;out)$$



$$x_1 = \tfrac{1}{2}x_2 + \tfrac{1}{2}x_3$$
$$x_2 = 0$$
$$x_3 = \tfrac{1}{2}x_1 + \tfrac{1}{2}x_4$$
$$x_4 = \tfrac{1}{3}x_3 + \tfrac{1}{3}x_5 + \tfrac{1}{3}x_8$$
$$x_5 = \tfrac{1}{3}x_2 + \tfrac{1}{3}x_4 + \tfrac{1}{3}x_6$$
$$x_6 = 1$$
$$x_7 = 0$$
$$x_8 = 0$$

Mouse Catching: Unbounded Until Example

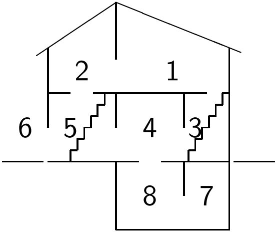
$$\mathcal{P}_{\geq 0.2}\left(\neg kitchen\ \mathcal{U}\ out\right)$$



$$(x_1, \ldots, x_8) = \left(\frac{1}{18}, 0, \frac{1}{9}, \frac{1}{6}, \frac{7}{18}, 1, 0, 0\right)$$

Mouse Catching: Unbounded Until Example

$$\mathcal{P}_{\geq 0.2}\,(\neg kitchen\,\mathcal{U}\;out)$$



$$(x_1, \ldots, x_8) = \left(\tfrac{1}{18}, 0, \tfrac{1}{9}, \tfrac{1}{6}, \tfrac{7}{18}, 1, 0, 0\right)$$

$$\textsc{Sat}\,(\mathcal{P}_{\geq 0.2}\,(\neg kitchen\,\mathcal{U}\;out)) = \{5, 6\}$$

Steady-state Operator?

- Steady-state probabilities are undefined for non-aperiodic DTMCs
- It is, however, possible to define a long-run operator (seldom used)

Recapitulation

- A Markov chain describes the (probabilistic) behaviour of a discrete-state system.
- Transient state and steady state analysis calculate state probabilities.
- Probabilistic CTL expresses properties of discrete-time Markov chains.
- There are model checking algorithms for PCTL (using transient state analysis).

Coming Soon

1. Continuous-Time Markov Chains
2. Markov Decision Processes
3. Further Extensions: MRM, HMM, ...
4. Tool: MRMC