Model Checking Markov Chains

Lecture 1: Probabilistic CTL

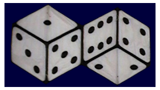
Joost-Pieter Katoen

Software Modeling and Verification Group

RWTH Aachen University

affiliated to University of Twente, Formal Methods and Tools

Lecture at Model Checking Summerschool, October 11, 2010



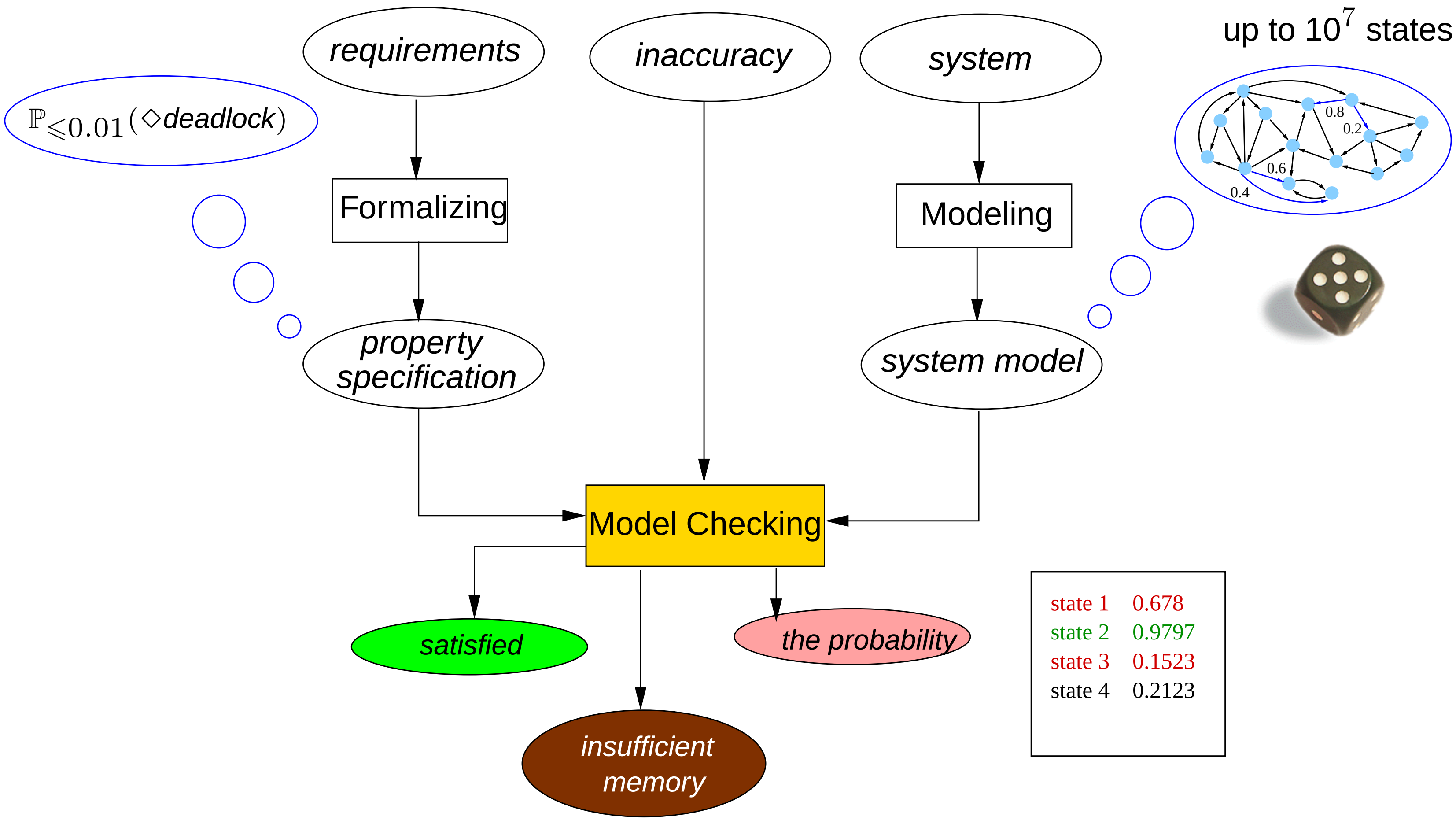
Probabilities help

- When analysing system performance and dependability
  - to quantify arrivals, waiting times, time between failure, QoS, ...
- When modelling uncertainty in the environment
  - to quantify imprecisions in system inputs
  - to quantify unpredictable delays, express soft deadlines, ...
- When building protocols for networked embedded systems
  - randomized algorithms
- When problems are undecidable deterministically
  - repeated reachability of channel systems, ...

Illustrative examples

- Security: Crowds protocol
  - analysis of probability of anonymity
- IEEE 1394 Firewire protocol
  - proof that biased delay is optimal
- Systems biology
  - probability that enzymes are absent within the deadline
- Software in next generation of satellites
  - mission time probability (ESA project)

What is probabilistic model checking?

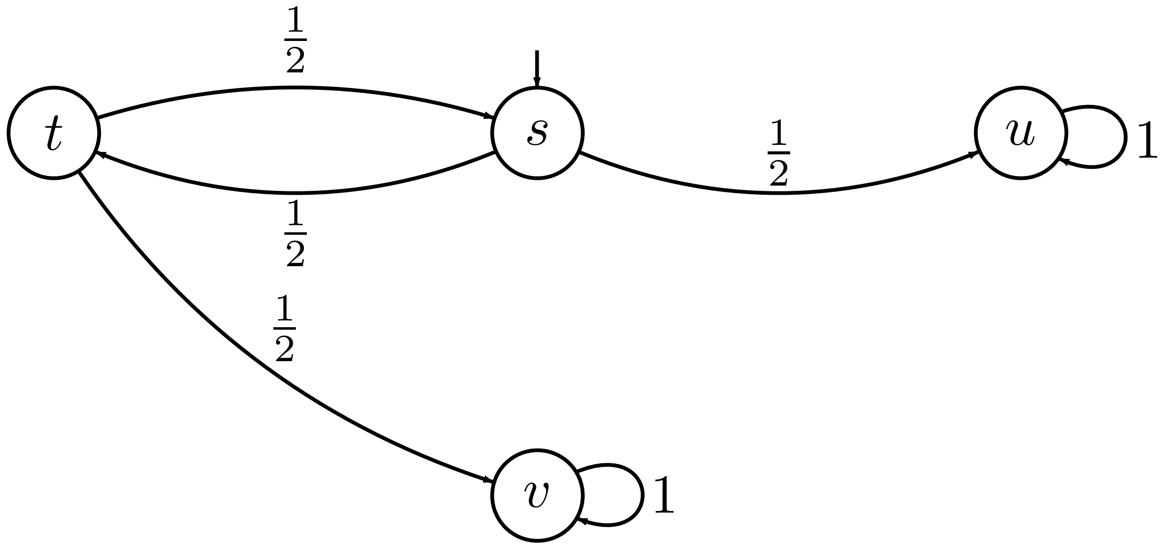


Probabilistic models

	Nondeterminism no	Nondeterminism yes
Discrete time	discrete-time Markov chain (DTMC)	Markov decision process (MDP)
Continuous time	CTMC	CTMDP

Other models: probabilistic variants of (priced) timed automata, or hybrid automata

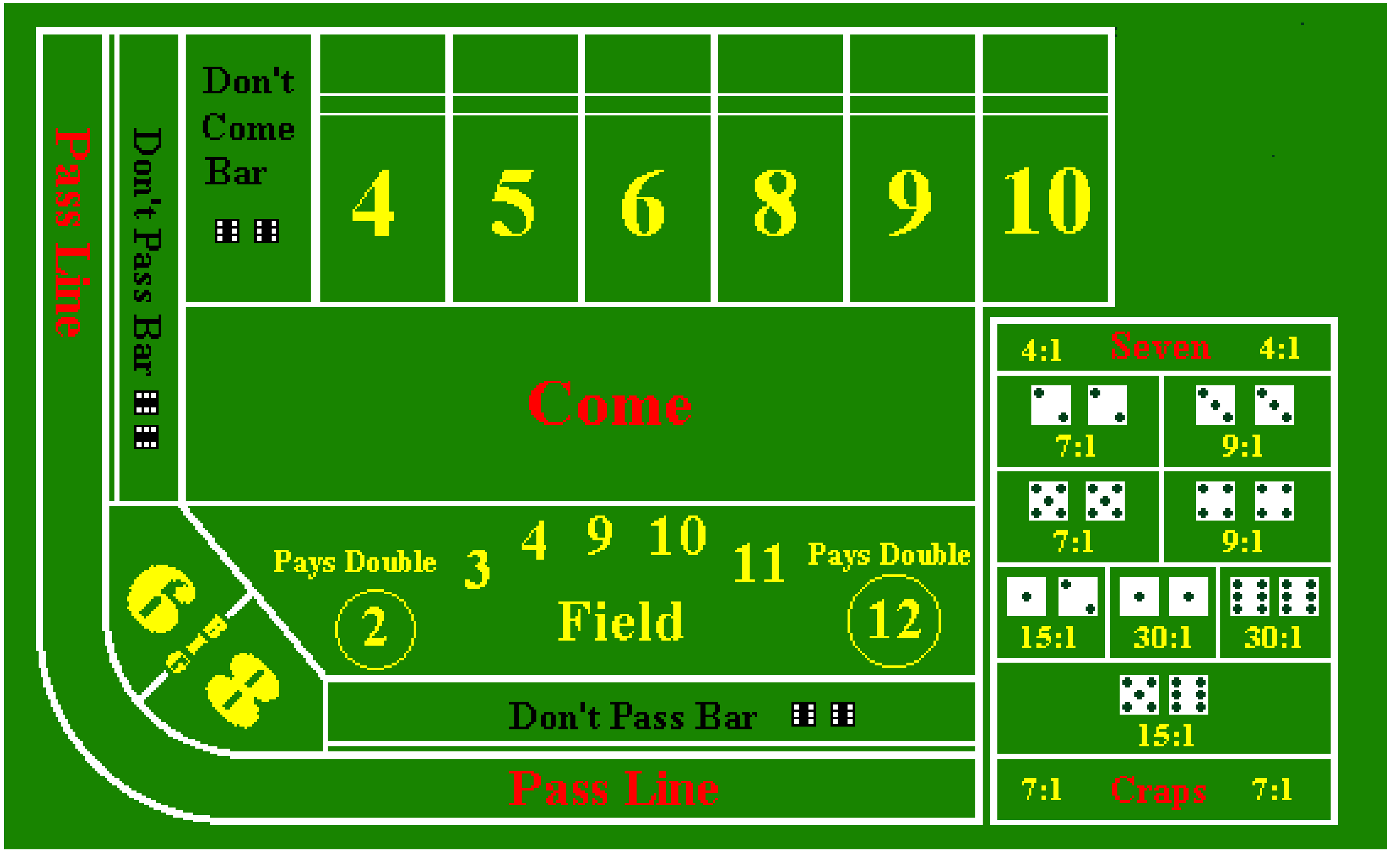
Discrete-time Markov chain



a DTMC $\mathcal{D}$ is a triple $(S, \mathbf{P}, L)$ with state space S and state-labelling L

and $\mathbf{P}$ a stochastic matrix with $\mathbf{P}(s, s') =$ one-step probability to jump from s to s'

Craps



Pass Line
Don't Pass Bar
Don't Come Bar
4
5
6
8
9
10
Come
4:1 Seven 4:1
7:1
9:1
7:1
9:1
15:1
30:1
30:1
15:1
7:1 Craps 7:1
Pays Double
3
4 9 10
11
Pays Double
2
12
Field
6
8
Don't Pass Bar
Pass Line

Craps

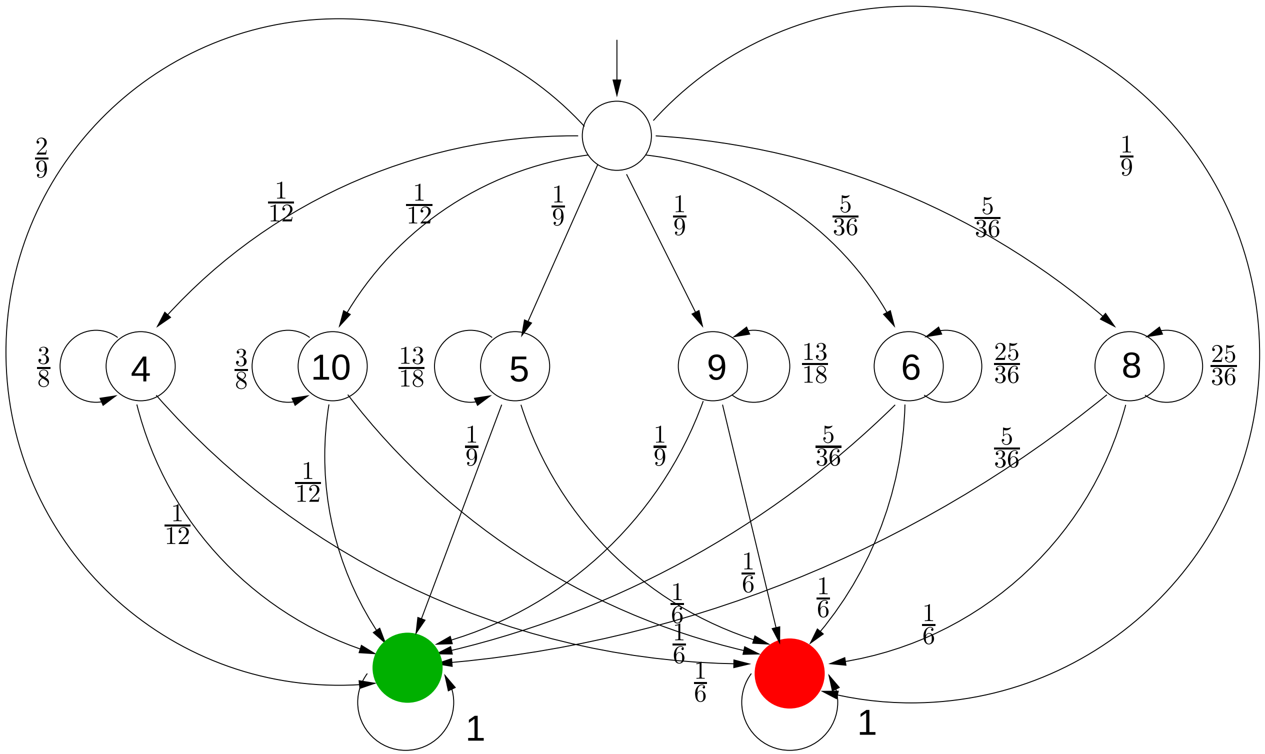
- Roll two dice and bet on outcome

- Come-out roll ("pass line" wager):
  - outcome 7 or 11: win
  - outcome 2, 3, or 12: loss ("craps")
  - any other outcome: roll again (outcome is "point")

- Repeat until 7 or the "point" is thrown:
  - outcome 7: loss ("seven-out")
  - outcome the point: win
  - any other outcome: roll again

A DTMC model of Craps

- Come-out roll:
  - 7 or 11: win
  - 2, 3, or 12: loss
  - else: roll again
- Next roll(s):
  - 7: loss
  - point: win
  - else: roll again



Probability measure on DTMCs

- Events are *infinite paths* in the DTMC $\mathcal{D}$, i.e., $\Omega = \mathit{Paths}(\mathcal{D})$
  - a path in a DTMC is just a sequence of states
- A σ-algebra on $\mathcal{D}$ is generated by *cylinder sets* of finite paths $\hat{\pi}$:

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

  - cylinder sets serve as basis events of the smallest σ-algebra on $\mathit{Paths}(\mathcal{D})$
- $\Pr$ is the *probability measure* on the σ-algebra on $\mathit{Paths}(\mathcal{D})$:

$$\Pr\big(\mathit{Cyl}(s_0 \ldots s_n)\big) \;=\; \iota_{init}(s_0) \cdot \mathbf{P}(s_0 \ldots s_n)$$

  - where $\mathbf{P}(s_0\, s_1 \ldots s_n) \;=\; \prod_{0 \leqslant i < n} \mathbf{P}(s_i, s_{i+1})$ and $\mathbf{P}(s_0) = 1$, and
  - $\iota_{init}(s_0)$ is the initial probability to start in state s_0

Reachability probabilities

- What is the probability to reach a set of states $B \subseteq S$ in DTMC $\mathcal{D}$?
- Which event does $\Diamond B$ mean formally?
  - the union of all cylinders *Cyl*$(s_0 \ldots s_n)$ where
  - $s_0 \ldots s_n$ is an initial path fragment in $\mathcal{D}$ with $s_0, \ldots, s_{n-1} \notin B$ and $s_n \in B$

$$
\begin{aligned}
\Pr(\Diamond B) &= \sum_{s_0 \ldots s_n \in \textit{Paths}_{\mathit{fin}}(\mathcal{D}) \cap (S \setminus B)^* B} \Pr\big(\textit{Cyl}(s_0 \ldots s_n)\big) \\
&= \sum_{s_0 \ldots s_n \in \textit{Paths}_{\mathit{fin}}(\mathcal{D}) \cap (S \setminus B)^* B} \iota_{\mathit{init}}(s_0) \cdot \mathbf{P}(s_0 \ldots s_n)
\end{aligned}
$$

Reachability probabilities in finite DTMCs

- Let $\Pr(s \models \Diamond B) = \Pr_s(\Diamond B) = \Pr_s\{\pi \in \textit{Paths}(s) \mid \pi \models \Diamond B\}$
  - where $\Pr_s$ is the probability measure in $\mathcal{D}$ with single initial state s
- Let variable $x_s = \Pr(s \models \Diamond B)$ for any state s
  - if B is not reachable from s then $x_s = 0$
  - if $s \in B$ then $x_s = 1$
- For any state $s \in \textit{Pre}^*(B) \setminus B$:

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

Unique solution

Let $\mathcal{D}$ be a finite DTMC with state space S partitioned into:

- $S_{=0} \ = \ Sat(\neg\exists(C \,\mathsf{U}\, B))$
- $B \ \subseteq S_{=1} \ \subseteq \{s \in S \mid \Pr(s \models C \,\mathsf{U}\, B) = 1\}$
- $S_? \ = \ S \setminus (S_{=0} \cup S_{=1})$

The vector $\big(\Pr(s \models C \,\mathsf{U}\, B)\big)_{s \in S_?}$

is the *unique* solution of the linear equation system:

$\mathbf{x} \ = \ \mathbf{A}\mathbf{x} + \mathbf{b}$ where $\mathbf{A} \ = \ \big(\mathbf{P}(s,t)\big)_{s,t \in S_?}$ and $\mathbf{b} \ = \ \big(\mathbf{P}(s, S_{=1})\big)_{s \in S_?}$

Computing reachability probabilities

- The probabilities of the events $C \,\mathsf{U}^{\leqslant n}\, B$ can be obtained iteratively:

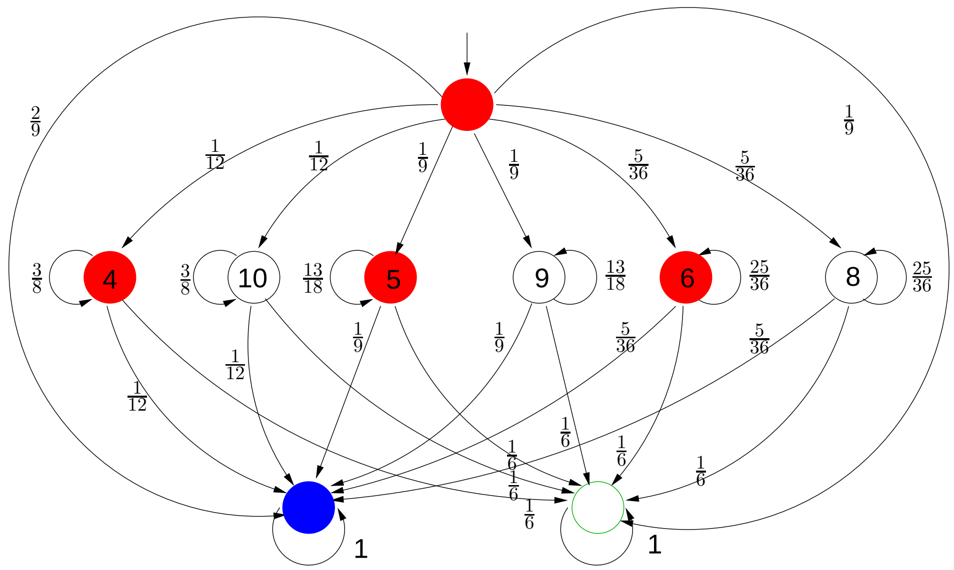
$$\mathbf{x}^{(0)} = \mathbf{0} \quad \text{and} \quad \mathbf{x}^{(i+1)} = \mathbf{A}\mathbf{x}^{(i)} + \mathbf{b} \text{ for } 0 \leqslant i < n$$

- where $\mathbf{A} = \big(\mathbf{P}(s,t)\big)_{s,t \in C \setminus B}$ and $\mathbf{b} = \big(\mathbf{P}(s,B)\big)_{s \in C \setminus B}$

- Then: $\mathbf{x}^{(n)}(s) = \Pr(s \models C \,\mathsf{U}^{\leqslant n} B)$ for $s \in C \setminus B$

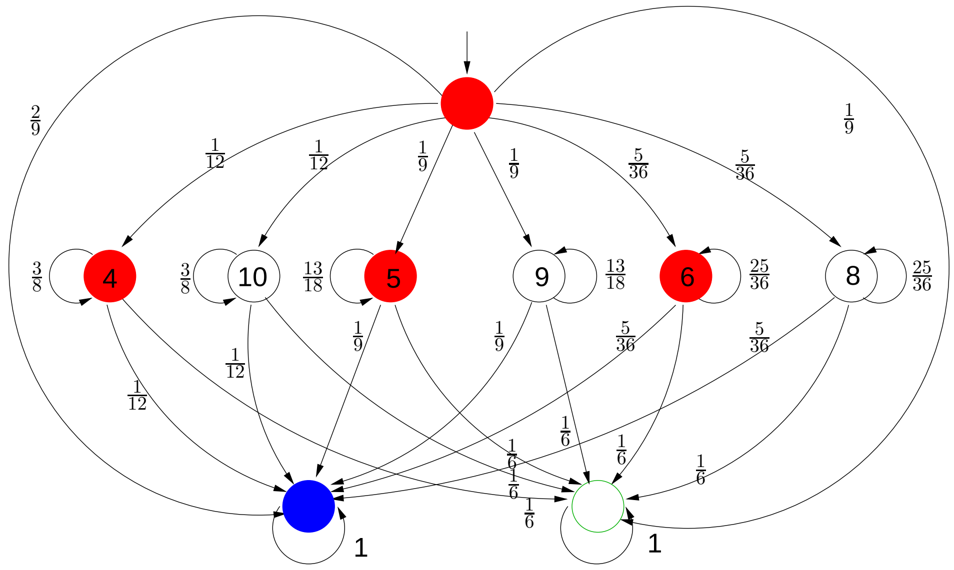
Example: Craps game

- $\Pr(start \models {\color{red}C} \,\mathsf{U}^{\leqslant n}\, {\color{blue}B})$
- $S_{=0} = \{\, 8, 9, 10, lost \,\}$
- $S_{=1} = \{\, {\color{blue}won} \,\}$
- $S_{?} = \{\, {\color{red}start}, 4, 5, 6 \,\}$



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

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

PCTL Syntax

- For $a \in AP$, $J \subseteq [0,1]$ an interval with rational bounds, and natural n:

$$\boxed{\begin{aligned} \Phi \; &::= \; \text{true} \;\Big|\; a \;\Big|\; \Phi \wedge \Phi \;\Big|\; \neg\Phi \;\Big|\; \mathbb{P}_J(\varphi) \\ \varphi \; &::= \; \mathsf{X}\,\Phi \;\Big|\; \Phi_1 \,\mathsf{U}\, \Phi_2 \;\Big|\; \Phi_1 \,\mathsf{U}^{\leqslant n}\, \Phi_2 \end{aligned}}$$

- $s_0 s_1 s_2 \ldots \models \Phi \,\mathsf{U}^{\leqslant n}\, \Psi$ if Φ holds until Ψ holds within n steps

- $s \models \mathbb{P}_J(\varphi)$ if probability that paths starting in s fulfill φ lies in J

abbreviate $\mathbb{P}_{[0,0.5]}(\varphi)$ by $\mathbb{P}_{\leqslant 0.5}(\varphi)$ and $\mathbb{P}_{]0,1]}(\varphi)$ by $\mathbb{P}_{>0}(\varphi)$ and so on

Derived operators

$$\Diamond\Phi \;=\; \text{true}\,\mathsf{U}\,\Phi$$

$$\Diamond^{\leqslant n}\Phi \;=\; \text{true}\,\mathsf{U}^{\leqslant n}\,\Phi$$

$$\mathbb{P}_{\leqslant p}(\Box\Phi) \;=\; \mathbb{P}_{\geqslant 1-p}(\Diamond\neg\Phi)$$

$$\mathbb{P}_{]p,q]}(\Box^{\leqslant n}\,\Phi) \;=\; \mathbb{P}_{[1-q,1-p[}(\Diamond^{\leqslant n}\,\neg\Phi)$$

operators like weak until W or release R can be derived analogously

Example properties

- With probability $\geqslant 0.92$, a goal state is reached via legal ones:

$$\mathbb{P}_{\geqslant 0.92}\,(\neg\, \mathit{illegal}\ \mathsf{U}\ \mathit{goal})$$

- ... in maximally 137 steps: $\mathbb{P}_{\geqslant 0.92}\,(\neg\, \mathit{illegal}\ \mathsf{U}^{\leqslant 137}\ \mathit{goal})$

- ... once there, remain there almost surely for the next 31 steps:

$$\mathbb{P}_{\geqslant 0.92}\left(\neg\, \mathit{illegal}\ \mathsf{U}^{\leqslant 137}\ \mathbb{P}_{=1}(\Box^{[0,31]}\ \mathit{goal})\right)$$

PCTL semantics (1)

$\mathcal{D}, s \models \Phi$ if and only if formula Φ holds in state s of DTMC $\mathcal{D}$

Relation $\models$ is defined by:

$s \models a$	iff	$a \in L(s)$
$s \models \neg \Phi$	iff	not $(s \models \Phi)$
$s \models \Phi \vee \Psi$	iff	$(s \models \Phi)$ or $(s \models \Psi)$
$s \models \mathbb{P}_J(\varphi)$	iff	$\Pr(s \models \varphi) \in J$

where $\Pr(s \models \varphi) = \Pr_s\{\pi \in \mathit{Paths}(s) \mid \pi \models \varphi\}$

PCTL semantics (2)

A *path* in $\mathcal{D}$ is an infinite sequence $s_0\, s_1\, s_2 \ldots$ with $\mathbf{P}(s_i, s_{i+1}) > 0$

Semantics of path-formulas is defined as in CTL:

$$\begin{array}{lll}
\pi \models \bigcirc \Phi & \text{iff} & s_1 \models \Phi \\
\pi \models \Phi \,\mathsf{U}\, \Psi & \text{iff} & \exists n \geqslant 0. (\, s_n \models \Psi \,\wedge \forall 0 \leqslant i < n.\, s_i \models \Phi \,) \\
\pi \models \Phi \,\mathsf{U}^{\leqslant n}\, \Psi & \text{iff} & \exists k \geqslant 0. (\, k \leqslant n \,\wedge\, s_k \models \Psi \,\wedge \\
 & & \qquad \forall 0 \leqslant i < k.\, s_i \models \Phi \,)
\end{array}$$

Measurability

For any PCTL path formula φ and state s of DTMC $\mathcal{D}$

the set $\{ \pi \in \mathit{Paths}(s) \mid \pi \models \varphi \}$ is measurable

PCTL model checking

- Given a finite DTMC $\mathcal{D}$ and PCTL formula Φ, how to check $\mathcal{D} \models \Phi$?

- Check whether state s in a DTMC satisfies a PCTL formula:
  - compute recursively the set *Sat*(Φ) of states that satisfy Φ
  - check whether state s belongs to *Sat*(Φ)

  $\Rightarrow$ bottom-up traversal of the parse tree of Φ (like for CTL)

- For the propositional fragment: as for CTL

- How to compute *Sat*(Φ) for the probabilistic operators?

Checking probabilistic reachability

- $s \models \mathbb{P}_J(\Phi \, \mathsf{U}^{\leqslant h} \, \Psi)$ if and only if $\Pr(s \models \Phi \, \mathsf{U}^{\leqslant h} \, \Psi) \; \in \; J$

- $\Pr(s \models \Phi \, \mathsf{U}^{\leqslant h} \, \Psi)$ is the least solution of: (Hansson & Jonsson, 1990)
  - 1 if $s \models \Psi$
  - for $h > 0$ and $s \models \Phi \wedge \neg \Psi$:

$$\sum_{s' \in S} \mathbf{P}(s, s') \cdot \Pr(s' \models \Phi \, \mathsf{U}^{\leqslant h-1} \, \Psi)$$

  - 0 otherwise

- Standard reachability for $\mathbb{P}_{>0}(\Phi \, \mathsf{U}^{\leqslant h} \, \Psi)$ and $\mathbb{P}_{\geqslant 1}(\Phi \, \mathsf{U}^{\leqslant h} \, \Psi)$
  - for efficiency reasons (avoiding solving system of linear equations)

Reduction to transient analysis

- Make all Ψ- and all $\neg(\Phi \vee \Psi)$-states absorbing in $\mathcal{D}$
- Check $\Diamond^{=h}\Psi$ in the obtained DTMC $\mathcal{D}'$
- This is a standard transient analysis in $\mathcal{D}'$:

$$\sum_{s' \models \Psi} \Pr_s\{\pi \in \mathit{Paths}(s) \mid \sigma[h] = s'\}$$

  – compute by $(\mathbf{P}')^h \cdot \iota_\Psi$ where ι_Ψ is the characteristic vector of $\mathit{Sat}(\Psi)$

$\Rightarrow$ Matrix-vector multiplication

Time complexity

For finite DTMC $\mathcal{D}$ and PCTL formula Φ, $\mathcal{D} \models \Phi$ can be solved in time

$$\mathcal{O}\big(\, poly(|\mathcal{D}|) \;\cdot\; n_{\max} \cdot |\Phi| \,\big)$$

where $n_{\max} \;=\; \max\{\, n \mid \Psi_1 \, \mathsf{U}^{\leqslant n} \, \Psi_2$ occurs in $\Phi \,\}$ with $\max \varnothing = 1$

The qualitative fragment of PCTL

- For $a \in AP$:

$$\Phi ::= \text{true} \mid a \mid \Phi \wedge \Phi \mid \neg \Phi \mid \mathbb{P}_{>0}(\varphi) \mid \mathbb{P}_{=1}(\varphi)$$

$$\varphi ::= \mathsf{X}\,\Phi \mid \Phi_1 \,\mathsf{U}\, \Phi_2$$

- The probability bounds $= 0$ and < 1 can be derived:

$$\mathbb{P}_{=0}(\varphi) \equiv \neg \mathbb{P}_{>0}(\varphi) \quad \text{and} \quad \mathbb{P}_{<1}(\varphi) \equiv \neg \mathbb{P}_{=1}(\varphi)$$

- No bounded until, and only > 0, $= 0$, > 1 and $= 1$ intervals

so: $\mathbb{P}_{=1}(\Diamond \mathbb{P}_{>0}(\mathsf{X}\, a))$ and $\mathbb{P}_{<1}(\mathbb{P}_{>0}(\Diamond a) \,\mathsf{U}\, b)$ are qualitative PCTL formulas

Qualitative PCTL versus CTL

- There is no CTL-formula that is equivalent to $\mathbb{P}_{=1}(\Diamond a)$
- There is no CTL-formula that is equivalent to $\mathbb{P}_{>0}(\Box a)$
- There is no qualitative PCTL-formula that is equivalent to $\forall\Diamond a$
- There is no qualitative PCTL-formula that is equivalent to $\exists\Box a$

$\Rightarrow$ PCTL with $\forall\varphi$ and $\exists\varphi$ is more expressive than PCTL

- For finite DTMCs, qualitative PCTL $\equiv$ CTL + strong fairness

谢谢大家！