Probabilistic Computation Tree Logic

Lecture #21 of Advanced Model Checking

Joost-Pieter Katoen

Lehrstuhl 2: Software Modeling & Verification

E-mail: katoen@cs.rwth-aachen.de

February 1, 2007

Discrete-time Markov chains

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

- S is a countable nonempty set of states
- $\mathbf{P} : S \times S \rightarrow [0, 1]$, transition probability function s.t. $\sum_{s'} \mathbf{P}(s, s') = 1$
  - $\mathbf{P}(s, s')$ is the probability to jump from s to s' in one step
  - s is absorbing if $\mathbf{P}(s, s) = 1$
- $\iota_{init} : S \rightarrow [0, 1]$, the initial distribution with $\sum\limits_{s \in S} \iota_{init}(s) = 1$
  - $\iota_{init}(s)$ is the probability that system starts in state s
  - state s for which $\iota_{init}(s) > 0$ is an initial state
- $L : S \rightarrow 2^{AP}$, the labelling function

PCTL Syntax

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

$$\Phi \ ::= \ \text{true} \ \big| \ a \ \big| \ \Phi \wedge \Phi \ \big| \ \neg \Phi \ \big| \ \mathbb{P}_J(\varphi)$$

$$\varphi \ ::= \ \bigcirc \Phi \ \big| \ \Phi_1 \, \mathsf{U} \, \Phi_2 \ \big| \ \Phi_1 \, \mathsf{U}^{\leqslant n} \, \Phi_2$$

- $s_0 s_1 s_2 \ldots \models \Phi \, \mathsf{U}^{\leqslant n} \, \Psi$ 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 $\mathbb{P}_{>0}(\varphi)$

Derived operators

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

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

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

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

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

Example properties

- Transient probabilities: $\mathbb{P}_{\geqslant 0.92}\,(\Diamond^{=137}\, \mathit{goal})$
- With probability $\geqslant$ 0.92, a goal state is reached legally:

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

- ... 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)

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

Relation $\models$ is defined by:

$$
\begin{array}{lll}
s \models a & \text{iff} & a \in L(s) \\
s \models \neg \Phi & \text{iff} & \text{not } (s \models \Phi) \\
s \models \Phi \lor \Psi & \text{iff} & (s \models \Phi) \text{ or } (s \models \Psi) \\
s \models \mathbb{P}_J(\varphi) & \text{iff} & \Pr(s \models \varphi) \in J
\end{array}
$$

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

PCTL semantics (2)

A *path* in $\mathcal{M}$ 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 $\mathcal{M}$

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

PCTL model checking

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

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

- For the propositional fragment: as for CTL

- How to compute $Sat(\Phi)$ for the probabilistic operators?

PCTL model checking

- Alternative formulation: $s \models \mathbb{P}_J(\bigcirc \Phi)$ if and only if $Prob(s, \bigcirc \Phi) \in J$
- Next: $Prob(s, \bigcirc \Phi)$ equals $\sum_{s' \in Sat(\Phi)} \mathbf{P}(s, s')$
- Matrix-vector multiplication:

$$\big(Prob(s, \bigcirc \Phi)\big)_{s \in S} = \mathbf{P} \cdot \iota_\Phi$$

where ι_Φ is the characteristic vector of *Sat*(Φ), i.e.,
$\iota_\Phi(s) = 1$ if and only if $s \in Sat(\Phi)$

Checking probabilistic reachability

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

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

  - 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 $\mathcal{M}$
- Check $\Diamond^{=h}\,\Psi$ in the obtained DTMC $\mathcal{M}'$
- This is a standard transient analysis in $\mathcal{M}'$:

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

  - 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 $\mathcal{M}$ and PCTL formula Φ, $\mathcal{M} \models \Phi$ can be solved in time

$$\mathcal{O}\Big(poly(\textit{size}(\mathcal{M})) \cdot n_{\max} \cdot |\Phi| \Big)$$

- $n_{\max} = \max\{ n \mid \Psi_1 \, \mathsf{U}^{\leqslant n} \Psi_2$ occurs in $\Phi \}$
- and $n_{\max} = 1$ if Φ does not contain the bounded until-operator

The qualitative fragment of PCTL

- For $a \in AP$ and natural n:

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

$$\varphi \ ::= \ \bigcirc\Phi \ \Big| \ \Phi_1 \, \mathsf{U} \, \Phi_2$$

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

$\mathbb{P}_{=1}$ versus $\forall$ and $\mathbb{P}_{>0}$ versus $\exists$

- PCTL-formula Φ is *equivalent* to CTL-formula Ψ:
  - $\Phi \equiv \Psi$ if and only if $Sat_{\mathcal{M}}(\Phi) = Sat_{TS(\mathcal{M})}(\Psi)$ for each DTMC $\mathcal{M}$
- $\exists\varphi$ requires φ on some paths, $\mathbb{P}_{>0}(\varphi)$ with positive probability
  - $\mathbb{P}_{>0}(\bigcirc a) \equiv \exists \bigcirc a$ and $\mathbb{P}_{>0}(\Diamond a) \equiv \exists\Diamond a$
  - and $\mathbb{P}_{>0}(a \,\mathsf{U}\, b) \;\equiv\; \exists a \,\mathsf{U}\, b$
  - but: $\mathbb{P}_{>0}(\Box a) \;\not\equiv\; \exists\Box a$
- $\forall\varphi$ requires φ to hold for all paths, $\mathbb{P}_{=1}(\varphi)$ for almost all
  - $\mathbb{P}_{=1}(\bigcirc a) \equiv \forall \bigcirc a$ and $\mathbb{P}_{=1}(\Box a) \equiv \forall\Box a$
  - but: $\mathbb{P}_{=1}(\Diamond a) \;\not\equiv\; \forall\Diamond a$ whereas $s \models \forall\Diamond a$ implies $s \models \mathbb{P}_{=1}(\Diamond a)$
  - and $\mathbb{P}_{=1}(a \,\mathsf{U}\, b) \;\not\equiv\; \forall a \,\mathsf{U}\, b$

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

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 $\exists \Box a$

Proofs

Strong fairness

For finite $\mathcal{M}$ is finite and $s \in \mathit{AP}$ to characterize uniquely state s:

$$sfair \;=\; \bigwedge_{s \in S} \;\; \bigwedge_{t \,\in\, \mathit{Post}(s)} \left(\Box\Diamond s \rightarrow \Box\Diamond t \right).$$

Using earlier results (see previous lecture) we obtain:

$$\begin{array}{lll} s \models \mathbb{P}_{=1}(a \,\mathsf{U}\, b) & \text{iff} & s \models_{sfair} \forall a \,\mathsf{U}\, b \\ s \models \mathbb{P}_{>0}(\Box a) & \text{iff} & s \models_{sfair} \exists \Box a \end{array}$$

As $sfair$ is a *realizable* fairness constraint on obtains:

$$s \models_{sfair} \exists(a \,\mathsf{U}\, b) \quad \text{iff} \quad s \models \exists(a \,\mathsf{U}\, b) \quad \text{iff} \quad s \models \mathbb{P}_{>0}(a \,\mathsf{U}\, b)$$

$$s \models_{sfair} \forall \bigcirc a \quad \text{iff} \quad s \models \forall \bigcirc a \quad \text{iff} \quad s \models \mathbb{P}_{=1}(\bigcirc a)$$

$$s \models_{sfair} \exists \bigcirc a \quad \text{iff} \quad s \models \exists \bigcirc a \quad \text{iff} \quad s \models \mathbb{P}_{>0}(\bigcirc a)$$

for finite DTMCs the qualitative fragment of PCTL can be viewed as a variant of CTL with some special kind of strong fairness

Almost sure repeated reachability

Let $\mathcal{M}$ be a finite Markov chain and s a state of $\mathcal{M}$. Then:

$$s \models \mathbb{P}_{=1}\big(\Box\, \mathbb{P}_{=1}(\Diamond a)\big) \quad \text{iff} \quad \Pr_s\{\pi \in \textit{Paths}(s) \mid \pi \models \Box\Diamond a\} = 1$$

this resembles $s \models \forall\Box\forall\Diamond a$ iff for all paths π: $\pi \models \Box\Diamond a$

Repeated reachability probabilities

For finite Markov chain, s a state of $\mathcal{M}$ and interval $J \subseteq [0,1]$:

$$s \models \underbrace{\mathbb{P}_J(\Diamond \mathbb{P}_{=1}(\Box \mathbb{P}_{=1}(\Diamond a)))}_{=\mathbb{P}_J(\Box\Diamond a)} \quad \text{iff} \quad \Pr(s \models \Box\Diamond a) \in J$$

the probabilities for $\Box\Diamond a$ agree with the probability to reach

a BSCC that contains at least one a-state

Persistence probabilities

For finite Markov chain, s a state of $\mathcal{M}$ and interval $J \subseteq [0,1]$:

$$s \models \mathbb{P}_J(\Diamond \mathbb{P}_{=1}(\Box a)) \quad \text{iff} \quad \Pr(s \models \Diamond\Box a) \in J$$

Traditional model checking

- Bisimulation: (Fisler & Vardi, 1998)
  - preserves μ-calculus
  - . . . obtains significant state space reductions
  - . . . minimization effort significantly exceeds model checking time
- Advantages:
  - fully automated and efficient abstraction technique
  - may be tailored to properties-of-interest
  - enables compositional minimisation
- Does bisimulation in probabilistic model checking pay off?

Probabilistic bisimulation

- Let $\mathcal{M} = (S, \mathbf{P}, AP, L)$ be a DTMC and R an equivalence on S
- R is a *probabilistic bisimulation* on S if for any $(s, s') \in R$:

$$L(s) = L(s') \text{ and } \mathbf{P}(s, C) = \mathbf{P}(s', C) \quad \text{for all} \quad C \text{ in } S/R$$

where $\mathbf{P}(s, C) = \sum_{s' \in C} \mathbf{P}(s, s')$ (Larsen & Shou, 1989)

- $s \sim s'$ if $\exists$ a probabilistic bisimulation R on S with $(s, s') \in R$

$$s \sim s' \Leftrightarrow (\forall \Phi \in \mathit{PCTL} : s \models \Phi \text{ if and only if } s' \models \Phi)$$

Proof

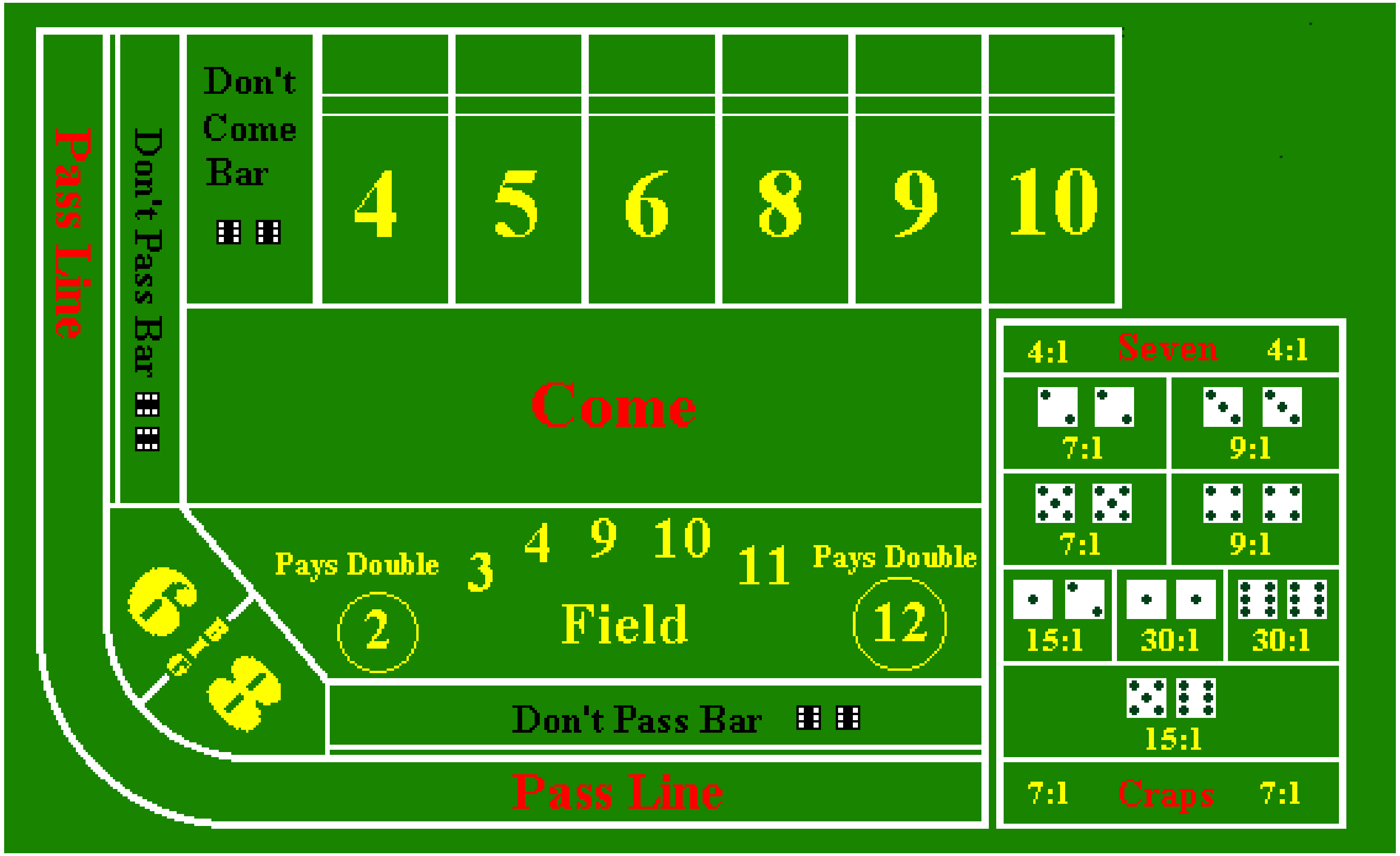
Quotient DTMC under $\sim$

$\mathcal{M}/\sim \; = \; (S', \mathbf{P}', AP, L')$, the quotient of $\mathcal{M} = (S, \mathbf{P}, AP, L)$ under $\sim$:

- $S' = S/\sim = \; \{ \, [s]_\sim \mid s \in S \, \}$
- $\mathbf{P}'([s]_\sim, C) = \mathbf{P}(s, C)$
- $L'([s]_\sim) = L(s)$

get $\mathcal{M}/\sim$ by partition-refinement in time $\mathcal{O}(M \cdot \log N + |AP| \cdot N)$ (Derisavi et al., 2001)

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
Field
12
6
8
Don't Pass Bar
Pass Line

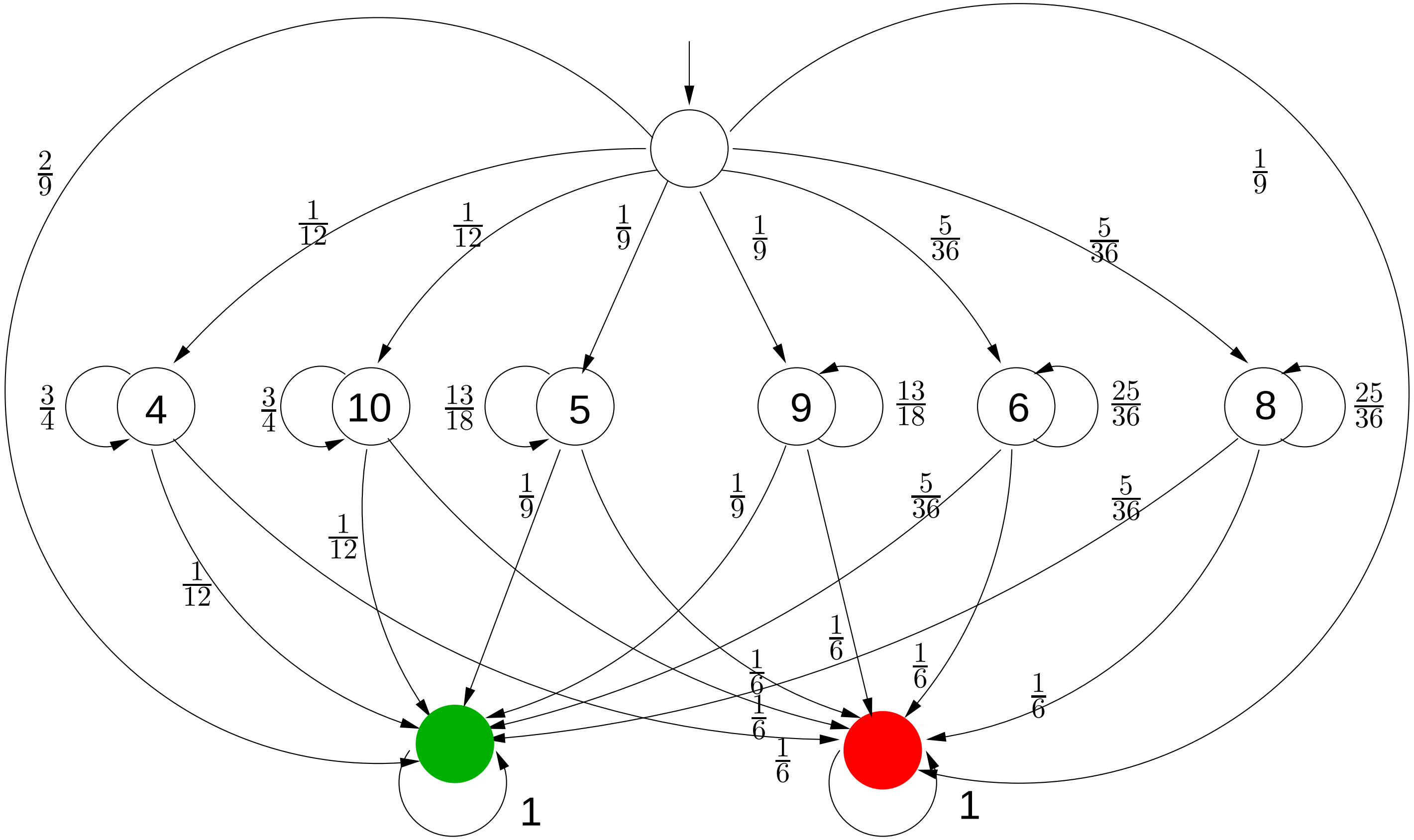
Craps

- Roll two dice and bet on outcome

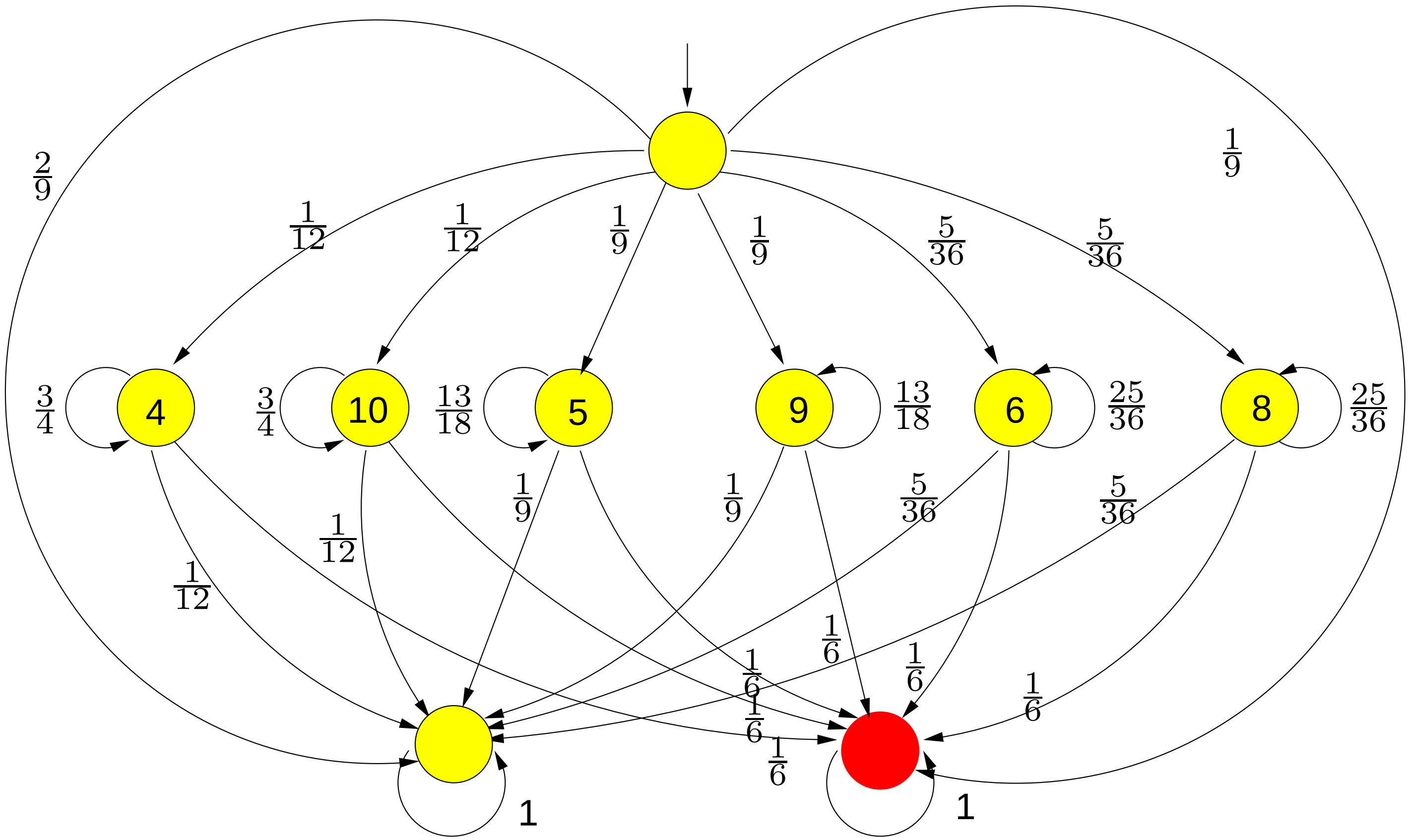
- Come-out roll ("pass line" wager):
  - outcome 7 or 11: win
  - outcome 2, 3, and 12: loss ("craps")
  - any other outcome: roll again (outcome is "point")

- 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

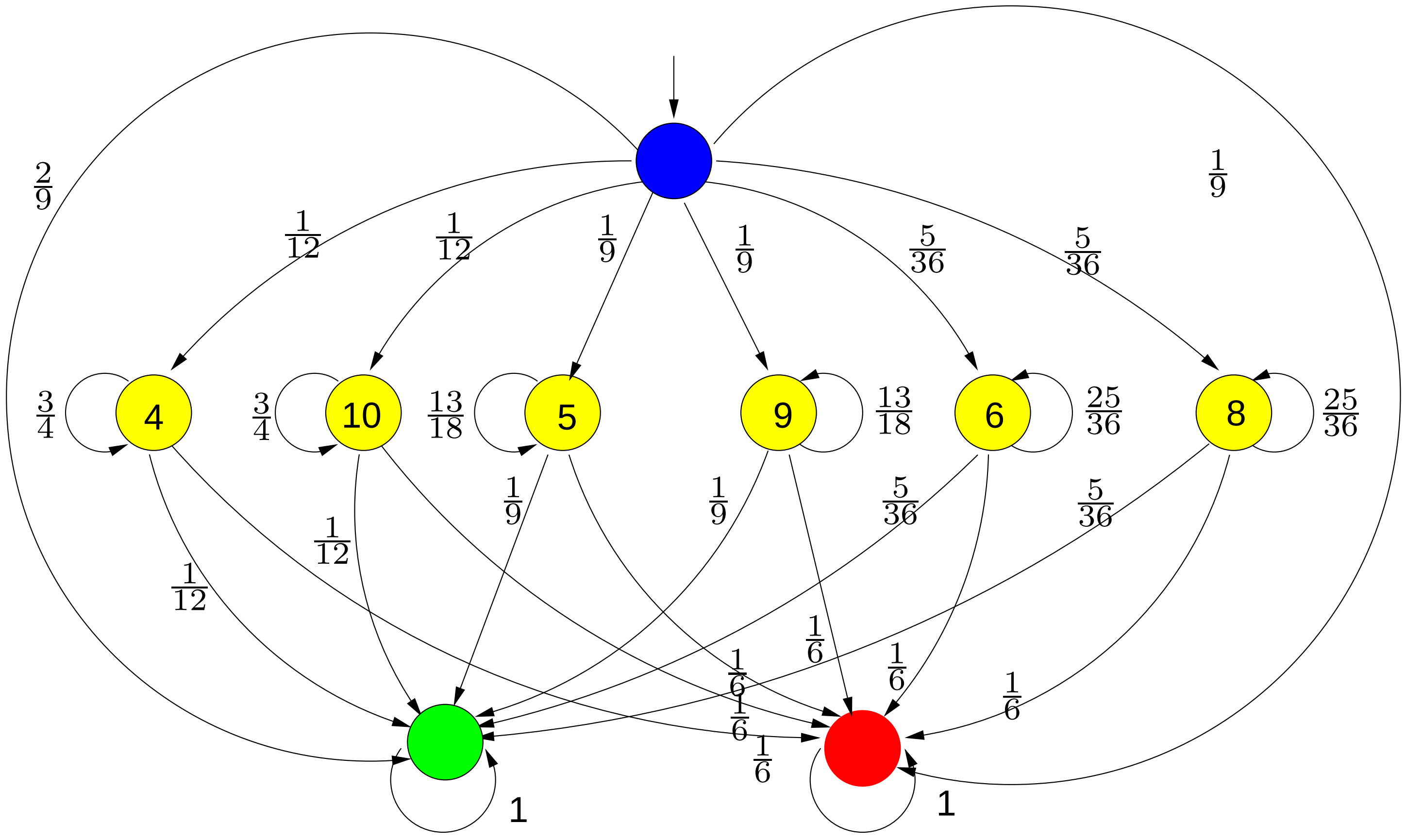


Minimizing Craps



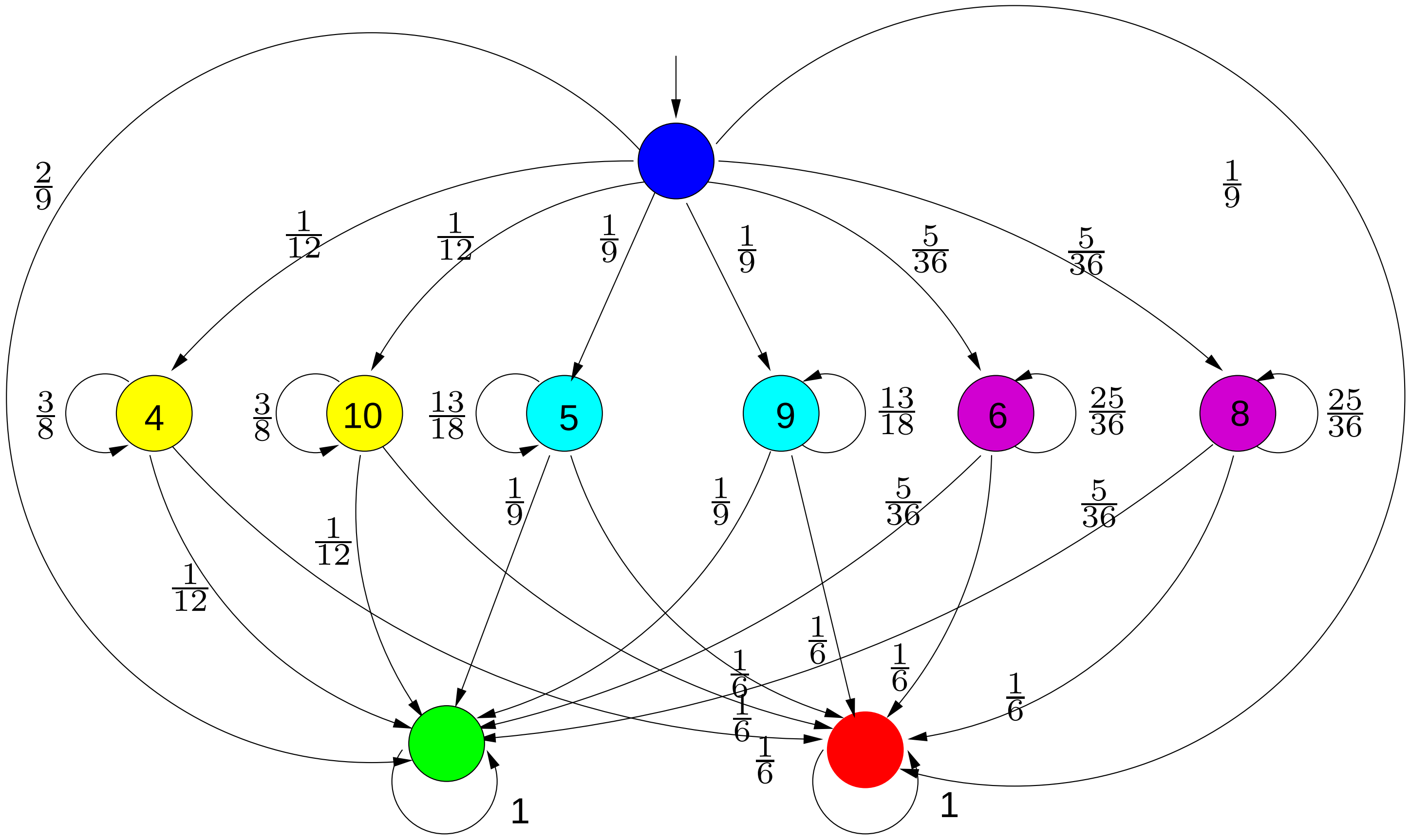
initial partitioning for the atomic propositions $AP = \{ \textit{loss} \}$

A first refinement



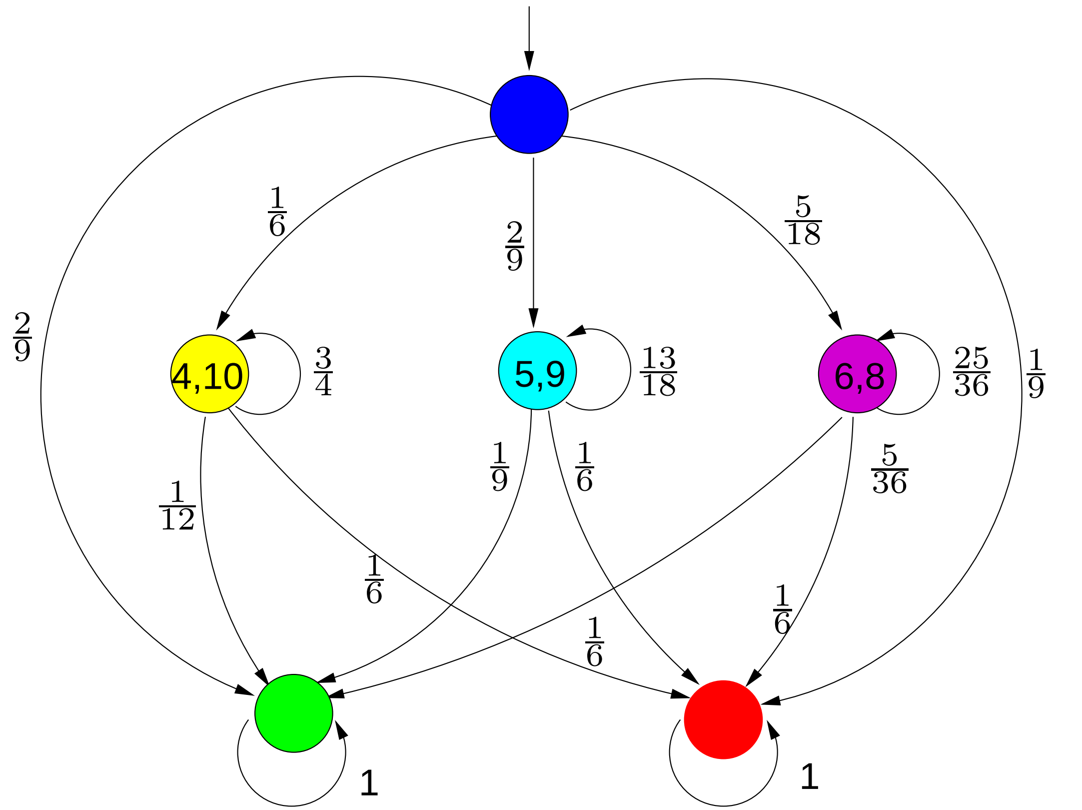
refine ("split") with respect to the set of red states

A second refinement



refine ("split") with respect to the set of green states

Quotient DTMC



Property-driven bisimulation

- For DTMC $\mathcal{M}$, set F of PCTL-formulas, and equivalence R on S
- R is a probabilistic F-bisimulation on S if for any $(s, s') \in R$:

$$L_F(s) = L_F(s') \text{ and } \mathbf{P}(s, C) = \mathbf{P}(s', C) \quad \text{for all} \quad C \text{ in } S/R$$

  where $L_F(s) = \{ \Phi \in F \mid s \models \Phi \}$ (Baier et al., 2000)

- $s \sim_F s'$ if $\exists$ a probabilistic F-bisimulation R on S with $(s, s') \in R$

$$s \sim_F s' \Leftrightarrow (\forall \Phi \in \mathit{PCTL}_F : s \models \Phi \text{ if and only if } s' \models \Phi)$$

Minimization for Φ until Ψ

- Initial partition for $\sim$: $s_\Pi = \{ s' \mid L(s') = L(s) \}$
  - independent of the formula to be checked

- Now: exploit the structure of the formula to be checked

- Bounded until:
  - take $F = \{ \Psi, \neg\Phi \wedge \neg\Psi, \Phi \wedge \neg\Psi \}$
  - initial partition $\Pi = \{ s_\Psi, s_{\neg\Phi\wedge\neg\Psi}, \mathit{Sat}(\Phi \wedge \neg\Psi) \}$
  - or, for non-recurrent DTMCs: $\mathcal{P}_{\leqslant 0}(\Phi \,\mathsf{U}\, \Psi)$ instead of $\neg\Phi \wedge \neg\Psi$

- Standard until:
  - take $F = \{ \underbrace{\mathcal{P}_{\geqslant 1}(\Phi \,\mathsf{U}\, \Psi)}_{\text{single state in } \Pi}, \underbrace{\mathcal{P}_{\leqslant 0}(\Phi \,\mathsf{U}\, \Psi)}_{\text{single state in } \Pi}, \mathcal{P}_{>0}(\Phi \,\mathsf{U}\, \Psi) \wedge \mathcal{P}_{<1}(\Phi \,\mathsf{U}\, \Psi) \}$