Lecture 15
Long-run properties of DTMCs and MDPs

Dr. Dave Parker

Department of Computer Science
University of Oxford

Overview

- LTL – Linear temporal logic
- Repeated reachability and persistence
- Long-run properties of DTMCs
  - bottom strongly connected components (BSCCs)
- Long-run properties of MDPs
  - end components (E.C.s)

Limitations of PCTL

- PCTL, although useful in practice, has limited expressivity
  - essentially: probability of reaching states in X, passing only through states in Y (and within k time-steps)
- More expressive logics can be used, for example:
  - LTL [Pnu77] – the non-probabilistic linear-time temporal logic
  - PCTL* [ASB+95,BdA95] – which subsumes both PCTL and LTL
  - both allow path operators to be combined
- In PCTL, temporal operators always appear inside $P_{\sim p}$ […]
  - (and, in CTL, they always appear inside A or E)
  - in LTL (and PCTL*), temporal operators can be combined

Review – CTL and PCTL

- CTL:
  - ϕ ::= true | a | $\phi \wedge \phi$ | $\neg\phi$ | A ψ | E ψ
  - ψ ::= X ϕ | ϕ U ϕ

- PCTL
  - ϕ ::= true | a | $\phi \wedge \phi$ | $\neg\phi$ | $P_{\sim p}$ [ψ]
  - ψ ::= X ϕ | ϕ $U^{\leq k}$ ϕ | ϕ U ϕ

- Notation for paths: $\omega = s_0 s_1 s_2 \ldots$
  - Path(s) = set of all (infinite) paths with $s_0 = s$
  - $\omega(i)$ denotes the (i+1)th state, i.e. $\omega(i) = s_i$
  - $\omega[i\ldots]$ is the suffix starting from s_i, i.e. $\omega[i\ldots] = s_i s_{i+1} s_{i+2} \ldots$

LTL – Linear temporal logic

- LTL syntax
  - path formulae only
  - $\psi ::= \text{true} \mid a \mid \psi \wedge \psi \mid \neg\psi \mid X\ \psi \mid \psi\ U\ \psi$
  - where $a \in AP$ is an atomic proposition

- LTL semantics (for a path ω)
  - $\omega \vDash \text{true}$ always
  - $\omega \vDash a \Leftrightarrow a \in L(\omega(0))$
  - $\omega \vDash \psi_1 \wedge \psi_2 \Leftrightarrow \omega \vDash \psi_1$ and $\omega \vDash \psi_2$
  - $\omega \vDash \neg\psi \Leftrightarrow \omega \nvDash \psi$
  - $\omega \vDash X\ \psi \Leftrightarrow \omega[1\ldots] \vDash \psi$
  - $\omega \vDash \psi_1\ U\ \psi_2 \Leftrightarrow \exists k \geq 0$ s.t. $\omega[k\ldots] \vDash \psi_2$ and $\forall i < k\ \omega[i\ldots] \vDash \psi_1$

LTL – Linear temporal logic

- Derived operators like CTL, for example:
  - $F\ \psi \equiv \text{true}\ U\ \psi$
  - $G\ \psi \equiv \neg F(\neg \psi)$

- LTL semantics (non-probabilistic)
  - implicit universal quantification over paths
  - i.e. for an LTS $M = (S, s_{init}, \rightarrow, L)$ and LTL formula ψ
  - $s \models \psi$ iff $\omega \models \psi$ for all paths $\omega \in Path(s)$
  - $M \models \psi$ iff $s_{init} \models \psi$
- e.g:
  - $A\ F\ (req \wedge X\ ack)$
  - “it is always possible that a request, followed immediately by an acknowledgement, can occur”

More LTL examples

- $(\mathrm{F}\ tmp\_fail_1) \wedge (\mathrm{F}\ tmp\_fail_2)$
  - "both servers suffer temporary failures at some point"
- GF ready
  - "the server always eventually returns to a ready-state"
- $\mathrm{G}\ (req \rightarrow \mathrm{F}\ ack)$
  - "requests are always followed by an acknowledgement"
- FG stable
  - "the system reaches and stays in a 'stable' state"

Branching vs. Linear time

- LTL but not CTL:
  - FG stable
  - “the system reaches and stays in a ‘stable’ state”
  - e.g. A FG stable $\not\equiv$ AF AG stable
- CTL but not LTL:
  - AG EF init
  - e.g. “for every computation, it is always possible to return to the initial state”

LTL + probabilities

- Same idea as PCTL: probabilities of sets of path formulae
  - for a state s of a DTMC and an LTL formula ψ:
  - Prob(s, ψ) = Pr_s { ω ∈ Path(s) | ω ⊨ ψ }
  - all such path sets are measurable (see later lecture)

- For MDPs, we can again consider lower/upper bounds
  - $p_{min}(s, \psi) = \inf_{\sigma \in Adv} Prob^{\sigma}(s, \psi)$
  - $p_{max}(s, \psi) = \sup_{\sigma \in Adv} Prob^{\sigma}(s, \psi)$
  - (for LTL formula ψ)

- For DTMCs or MDPs, an LTL specification often comprises an LTL (path) formula and a probability bound
  - e.g. $P_{>0.99}$ [F (req ∧ X ack)]

PCTL*

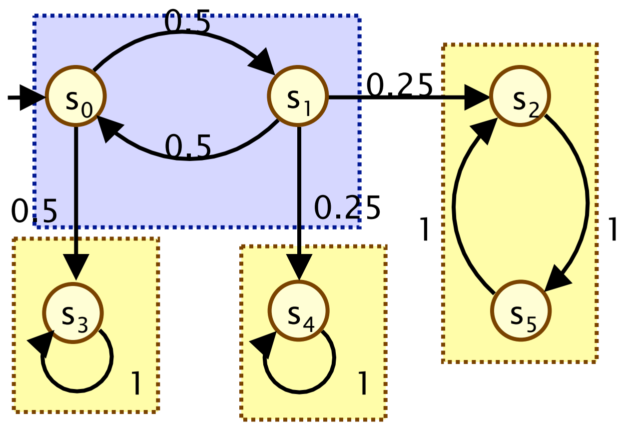
- PCTL* subsumes both (probabilistic) LTL and PCTL

- State formulae:
  - $\phi ::= \text{true} \mid a \mid \phi \wedge \phi \mid \neg\phi \mid P_{\sim p} [\ \psi\ ]$
  - where $a \in AP$, $\sim \in \{<,>,\leq,\geq\}$, $p \in [0,1]$ and ψ a path formula
- Path formulae:
  - $\psi ::= \phi \mid \psi \wedge \psi \mid \neg\psi \mid X\ \psi \mid \psi\ U\ \psi$
  - where ϕ is a state formula

- A PCTL* formula is a state formula ϕ
  - e.g. $P_{>0.99} [\ GF\ crit_1\ ] \wedge P_{>0.99} [\ GF\ crit_2\ ]$
  - e.g. $P_{\geq 0.75} [\ GF\ P_{>0} [\ F\ init\ ]\ ]$

Fundamental property of DTMCs

- Strongly connected component (SCC)
  - maximally strongly connected set of states
- Bottom strongly connected component (BSCC)
  - SCC T from which no state outside T is reachable from T



- With probability 1, a BSCC will be reached and all of its states visited infinitely often

- Formally:
  - $\text{Pr}_s\{\ \omega \in \text{Path}(s) \mid \exists\ i\geq 0,\ \exists\ \text{BSCC T such that}$
    $\forall\ j\geq i\ \omega(i) \in \text{T and}$
    $\forall\ s'\in T\ \omega(k) = s' \text{ for infinitely many k } \} = 1$

Repeated reachability – DTMCs

- Repeated reachability:
  - "always eventually…" or "infinitely often…"

- e.g. "what is the probability that the protocol successfully sends a message infinitely often?"

- Using LTL notation:
  - $\omega \vDash \mathbf{GF}\ a$

    $\Leftrightarrow$

  - $\forall\ i \geq 0\ .\ \exists\ j \geq i\ .\ \omega(j) \in Sat(a)$

- Prob(s, GF a)

  $= Pr_s \{ \omega \in Path(s) \mid \forall\ i \geq 0\ .\ \exists\ j \geq i\ .\ \omega(j) \in Sat(a) \}$

Qualitative repeated reachability

- $Pr_s\{ \omega \in Path(s) \mid \forall\ i \geq 0\ .\ \exists\ j \geq i\ .\ \omega(j) \in Sat(a) \} = 1$
- $P_{\geq 1}$ [GF a] ← PCTL*

if and only if

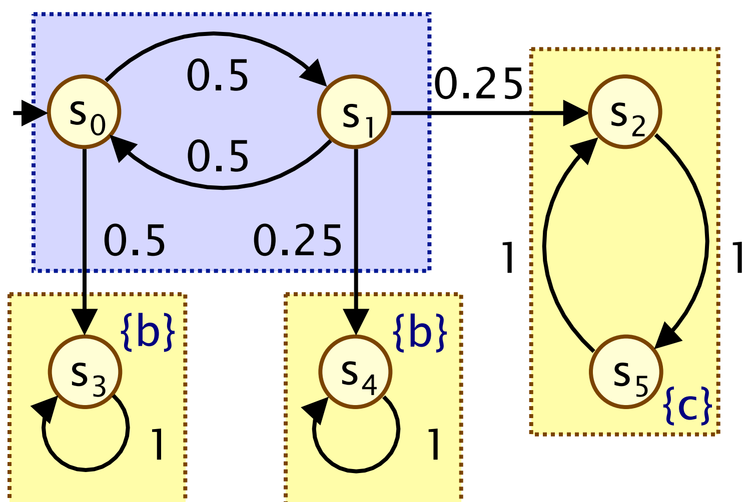
- $T \cap Sat(a) \neq \varnothing$ for all BSCCs T reachable from s

Examples:

$s_0 \vDash P_{\geq 1}$ [GF (b∨c)]

$s_0 \nvDash P_{\geq 1}$ [GF b]

$s_2 \vDash P_{\geq 1}$ [GF c]



Quantitative repeated reachability

- Prob(s, GF a) = Prob(s, F T_{GFa})
  - where T_{GFa} = union of all BSCCs T with $T \cap Sat(a) \neq \emptyset$

Example:

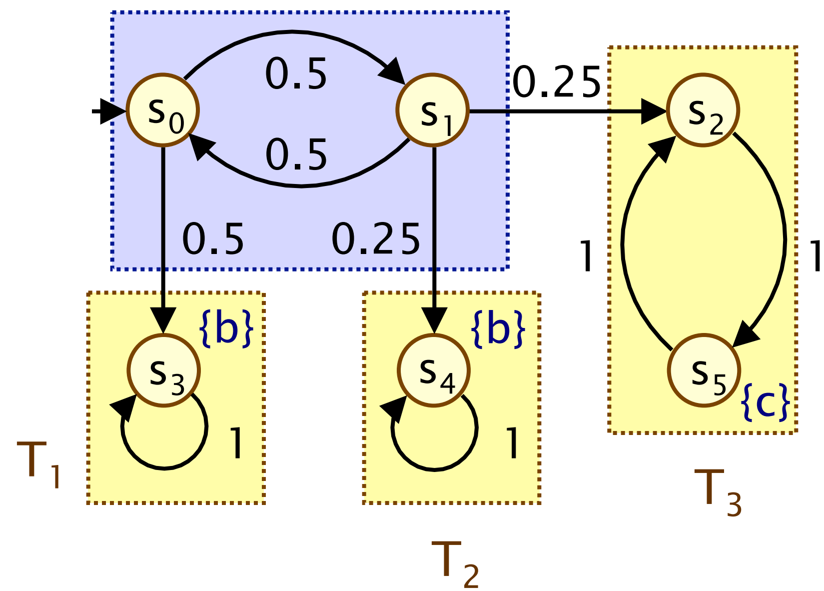
Prob(s_0, GF b)

= Prob(s_0, F T_{GFb})

= Prob(s_0, F ($T_1 \cup T_2$))

= Prob(s_0, F {s_3,s_4})

= 2/3 + 1/6 = 5/6



- From the above, we also have:
  - $P_{>0}$ [GF a] $\Leftrightarrow$ $T \cap Sat(a) \neq \emptyset$ for some reachable BSCC T

Persistence – DTMCs

- Persistence properties: “eventually always…”
  - e.g. “what is the probability of the leader election algorithm reaching, and staying in, a stable state?”
  - e.g. “what is the probability that an irrecoverable error occurs?”

- Using LTL notation:
  - $\omega \vDash \mathrm{FG}\ a$

    $\Leftrightarrow$
  - $\exists\ i \geq 0\ .\ \forall\ j \geq i\ .\ \omega(j) \in \mathrm{Sat}(a)$

- Prob(s, FG a)

  $= \mathrm{Pr}_s \{\ \omega \in \mathrm{Path}(s)\ |\ \exists\ i \geq 0\ .\ \forall\ j \geq i\ .\ \omega(j) \in \mathrm{Sat}(a)\ \}$

Qualitative persistence

- $Pr_s \{ \omega \in Path(s) \mid \exists\, i \geq 0 \,.\, \forall\, j \geq i \,.\, \omega(j) \in Sat(a) \} = 1$
- $P_{\geq 1}$ [FG a]

if and only if

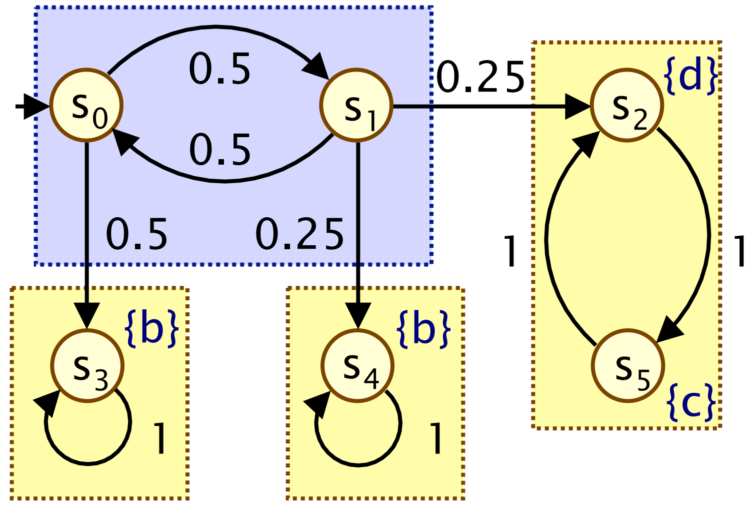
- $T \subseteq Sat(a)$ for all BSCCs T reachable from s

Examples:

$s_0 \not\models P_{\geq 1}$ [FG (b∨c)]

$s_0 \models P_{\geq 1}$ [FG (b∨c∨d)]

$s_2 \models P_{\geq 1}$ [FG (c∨d)]

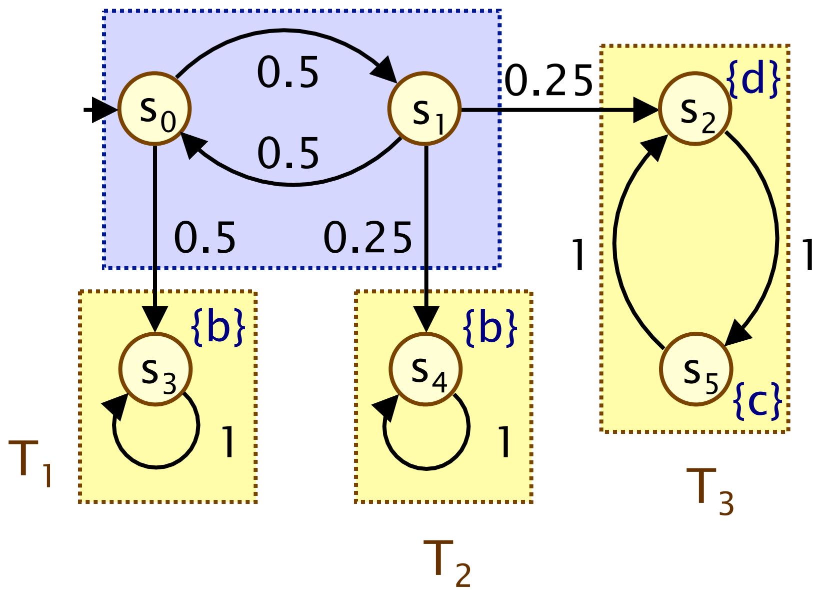


Quantitative persistence

- Prob(s, FG a) = Prob(s, F T_{FGa})
  - where T_{FGa} = union of all BSCCs T with $T \subseteq Sat(a)$

Example:

Prob(s_0, FG ($b \vee c$))
= Prob(s_0, F $T_{FG(b \vee c)}$)
= Prob(s_0, F ($T_1 \cup T_2$))
= Prob(s_0, F {s_3,s_4})
= 2/3 + 1/6 = 5/6



Success sets

- The sets T_P for property P are called success sets
  - T_{GFa} = union of all BSCCs T with $T \cap Sat(a) \neq \varnothing$
  - T_{FGa} = union of all BSCCs T with $T \subseteq Sat(a)$
- Sometimes denoted U_P
  - e.g. U_{GFa}
  - we use T_p here (to avoid confusion with the until operator)

Repeated reachability + persistence

- Repeated reachability and persistence are dual properties
  - GF a ≡ ¬(FG ¬a)
  - FG a ≡ ¬(GF ¬a)
- Hence, for example:
  - Prob(s, GF a) = 1 – Prob(s, FG ¬a)

- Can show this through LTL equivalences, or…

- Prob(s, GF a) + Prob(s, FG ¬a)

= Prob(s, F T_{GFa}) + Prob(s, F $T_{FG\neg a}$)
  - T_{GFa} = union of BSCCs T with $T \cap Sat(a) \neq \emptyset$ (T intersects Sat(a))
  - $T_{FG\neg a}$ = union of BSCCs T with $T \subseteq (S \setminus Sat(a))$ (no intersection)

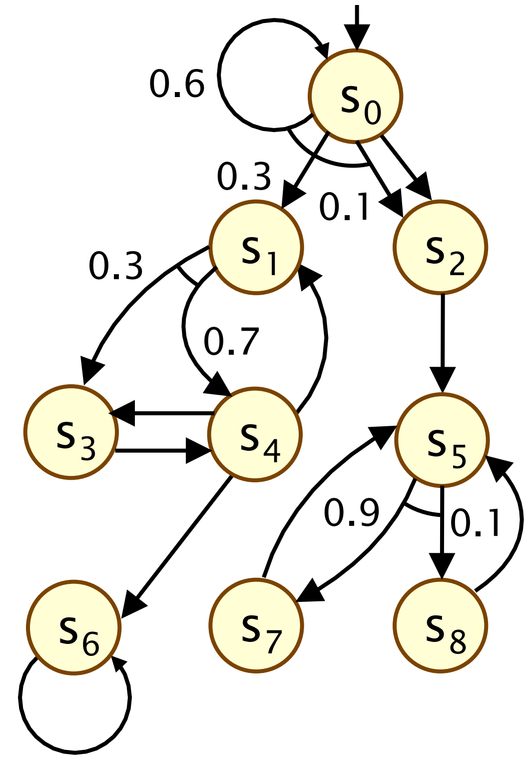
= Prob(s, F ($T_{GFa} \cup T_{FG\neg a}$)) = 1 (fundamental DTMC property)

End components of MDPs

- Consider an MDP M = (S,s_{init},**Steps**,L)

- A sub-MDP of M is a pair (T,**Steps**') where:
  - T ⊆ S is a (non-empty) subset of M's states
  - **Steps**'(s) ⊆ **Steps**(s) for each s ∈ T
  - (T,**Steps**') is closed under probabilistic branching, i.e. the set of states { s' | μ(s')>0 for some (a,μ)∈**Steps**'(s) } is a subset of T

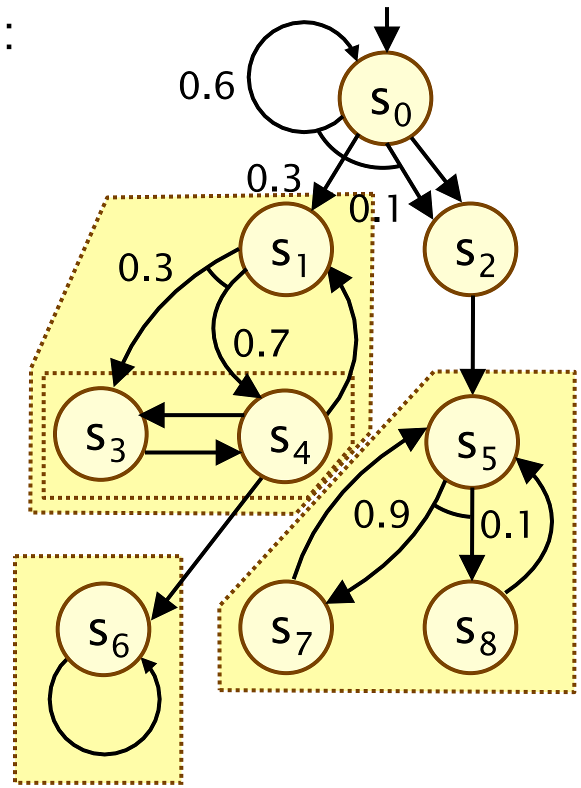
- An end component of M is a strongly connected sub-MDP



Note:
- action labels omitted
- probabilities omitted where =1

End components – Examples

- Sub-MDPs
  - can be formed from state sets such as:
  - $\{s_2,s_5,s_7,s_8\}$, $\{s_0,s_2,s_5,s_7,s_8\}$, $\{s_5,s_7,s_8\}$,
  - $\{s_1,s_3,s_4\}$, $\{s_1,s_3,s_4,s_6\}$, $\{s_3,s_4\}$, …



- End components
  - can be formed from state sets:
  - $\{s_3,s_4\}$, $\{s_1,s_3,s_4\}$, $\{s_6\}$, $\{s_5,s_7,s_8\}$

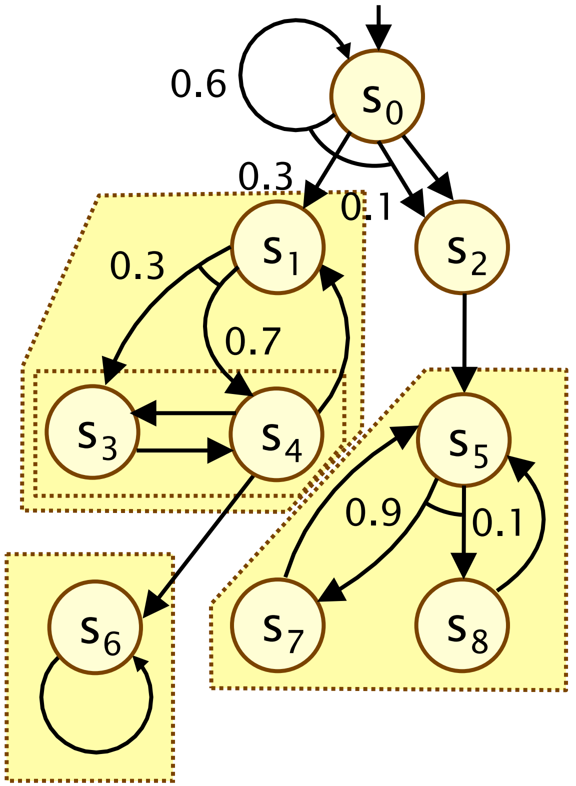
- Note that
  - state sets do not necessarily uniquely identify end components
  - e.g. $\{s_1,s_3,s_4\}$

End components of MDPs

- For finite MDPs…
  - (analogue of fundamental property of finite DTMCs)

- For every end component, there is an adversary which, with probability 1, forces the MDP to remain in the end component, and visit all its states infinitely often

- Under every adversary σ, with probability 1 an end component will be reached and all of its states visited infinitely often



Repeated reachability – MDPs (max)

- Repeated reachability (GF) for MDPs
  - consider first the case of maximum probabilities…
  - $p_{max}(s, GF\ a)$

- First, a simple qualitative property:
  - $Prob^{\sigma}(s, GF\ a) > 0$ for some adversary σ, i.e. $p_{max}(s, GF\ a) > 0$

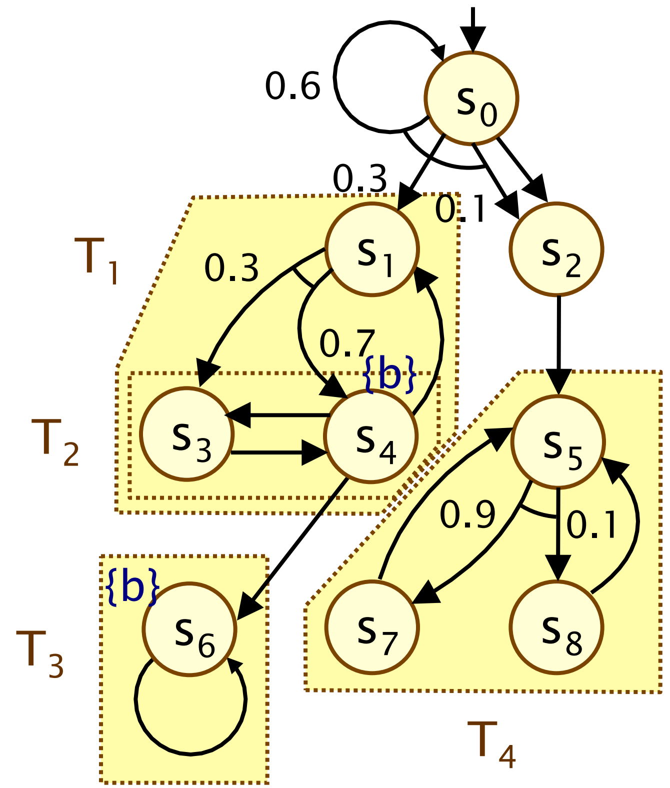
    $\Leftrightarrow$
  - $T \cap Sat(a) \neq \varnothing$ for some end component T reachable from s

- The quantitative case (for maximum probabilities):
  - $p_{max}(s, GF\ a) = p_{max}(s, F\ T_{GFa})$
  - where T_{GFa} is the union of sets T for all end components (T,**Steps'**) with $T \cap Sat(a) \neq \varnothing$ (i.e. at least one a-state in T)

Example

- Check: $P_{<0.8}$ [GF b] for s_0

- Compute p_{max}(GF b)
  - $p_{max}(GF\ b) = p_{max}(s, F\ T_{GFb})$
  - T_{GFb} is the union of sets T for all end components with $T \cap Sat(b) \neq \varnothing$
  - $Sat(b) = \{ s_4, s_6 \}$
  - $T_{GFb} = T_1 \cup T_2 \cup T_3 = \{ s_1, s_3\ s_4, s_6 \}$
  - $p_{max}(s, F\ T_{GFb}) = 0.75$
  - $p_{max}(GF\ b) = 0.75$



- Result: $s_0 \vDash P_{<0.8}$ [GF b]

Repeated reachability – MDPs (max)

- Quantitative case:
  - $p_{max}(s, GF\ a) = p_{max}(s, F\ T_{GFa})$
- This yields the qualitative property given earlier:
  - $Prob^{\sigma}(s, GF\ a) > 0$ for some adversary σ

    $\Leftrightarrow\ p_{max}(s, GF\ a) > 0$

    $\Leftrightarrow\ p_{max}(s, F\ T_{GFa}) > 0$

    $\Leftrightarrow\ Prob^{\sigma}(s, F\ T_{GFa}) > 0$ for some adversary σ

    $\Leftrightarrow\ s \vDash EF\ T_{GFa}$

    $\Leftrightarrow\ T \cap Sat(a) \neq \varnothing$ for some E.C. T reachable from s
- Another qualitative property:
  - $Prob^{\sigma}(s, GF\ a) = 1$ for some adversary σ

    $\Leftrightarrow\ p_{max}(s, GF\ a) = 1$

    $\Leftrightarrow\ p_{max}(s, F\ T_{GFa}) = 1$

Compute with Prob1E

Repeated reachability – MDPs (min)

- Repeated reachability for MDPs – minimum probabilities
  - p_{min}(s, GF a)

- First, a useful qualitative property:
  - $Prob^{\sigma}$(s, GF a) = 1 for all adversaries σ

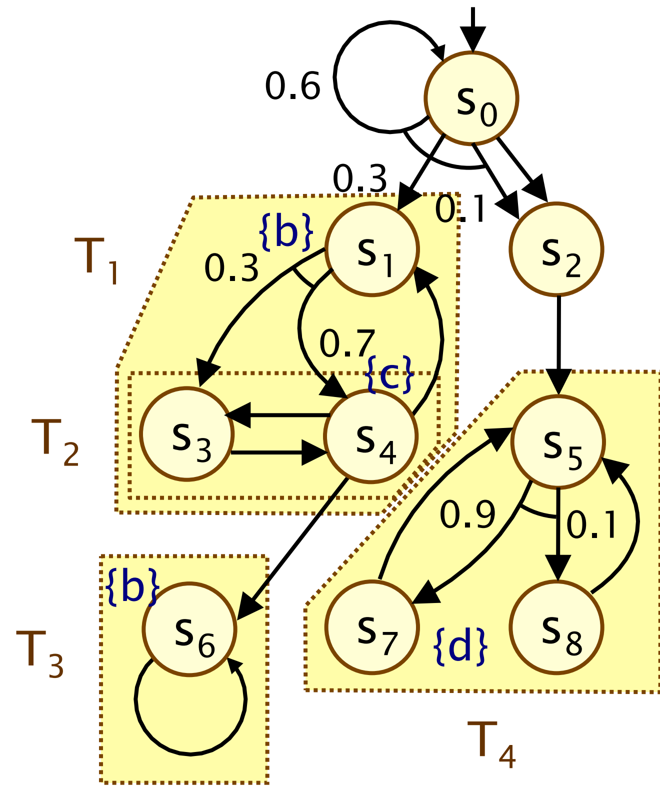
    ⇔
  - s ⊨ $P_{\geq 1}$ [GF a] ← PCTL*

    ⇔
  - T ∩ Sat(a) ≠ ∅ for all end components T reachable from s

Examples

- $s_0 \vDash P_{\geq 1}$ [GF ($b \vee c \vee d$)] ?

- $s_0 \vDash P_{\geq 1}$ [GF ($b \vee d$)] ?



Repeated reachability – MDPs (min)

- Repeated reachability for MDPs – minimum probabilities
  - $p_{min}(s, GF\ a)$

- Quantitative case
  - use duality of min/max probabilities for MDPs
  - $p_{min}(s, \psi) = 1 - p_{max}(s, \neg\psi)$
  - e.g. $p_{min}(s, GF\ a) = 1 - p_{max}(s, FG\neg a)$

- So min probabilities for repeated reachability (GF)
  - can be computed as max probabilities for persistence (FG)

Persistence – MDPs

- Persistence for MDPs
  - $p_{min}(s, FG\ a)$ or $p_{max}(s, FG\ a)$

- Quantitative case – maximum probabilities
  - $p_{max}(s, FG\ a) = p_{max}(s, F\ T_{FGa})$
  - where T_{FGa} is the union of sets T for all end components (T,**Steps'**) with $T \subseteq Sat(a)$ (i.e. all states in T satisfy a)

Repeated reachability (again)

- We now have way a of computing minimum probabilities for repeated reachability (GF)
  - $p_{min}(s, GF\ a) = 1 - p_{max}(s, FG\neg a)$
    $= 1 - p_{max}(s, F\ T_{FG\neg a})$
  - where $T_{FG\neg a}$ is the union of sets T for all end components (T,**Steps'**) with $T \subseteq S \backslash Sat(a)$
  - ie. $T_{FG\neg a}$ is the union of sets T for all end components (T,**Steps'**) with $T \cap Sat(a) = \varnothing$

Opposite of condition for GFa

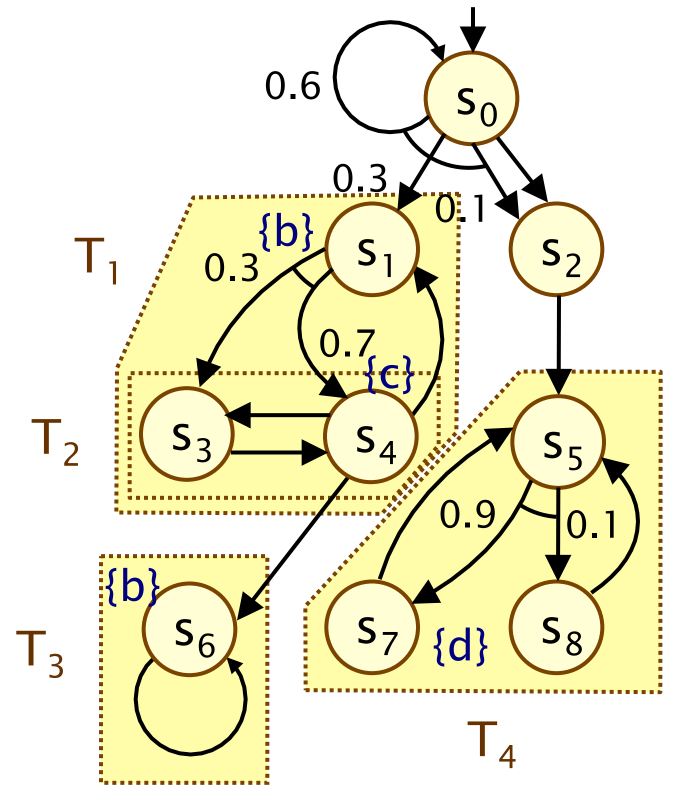
- Can also now show why:
  - $s \vDash P_{\geq 1}$ [GF a]

    $\Leftrightarrow$
  - $T \cap Sat(a) \neq \varnothing$ for all end components T reachable from s

Examples

- $s_0 \models P_{>0}$ [GF d] ?

- $s_0 \models P_{>0.3}$ [GF d] ?



Summing up… I

- LTL: path-based, path operators can be combined
- PCTL*: subsumes PCTL and LTL

CTL LTL	Φ ψ	non-probabilistic (LTSs)
PCTL LTL + prob. PCTL*	Φ Prob(s, ψ) Φ	probabilistic (DTMCs, MDPs)

Summing up… II

- 2 useful instances of LTL formulae:
  - repeated reachability: GF a
  - persistence: FG a
- DTMCs
  - qualitative: properties of reachable BSCCs
  - quantitative: probability of reaching success set (BSCC set)
- MDPs
  - end components: MDP analogue of BSCCs
  - p_{max}(s, GF a) – max. reachability of success set ($T \cap Sat(a) \neq \emptyset$)
  - $P_{\geq 1}$ [GF a] – reachability of end components
  - p_{min}(s, GF a) – one minus max. prob. for dual property
  - p_{max}(s, FG a) – max. reachability of success set ($T \subseteq Sat(a)$)
  - p_{min}(s, FG a) – again, via dual property